PRIVACY AND SECURITY ASSESSMENT OF BIOMETRIC TEMPLATE PROTECTION

vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

DISSERTATION

zur Erlangung des akademischen Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
von

周雪冰
Dipl.-Ing. Xuebing Zhou

geboren in Shenyang, China

Referenten der Arbeit:	Prof. Dr. techn. Dieter W. Fellner Technische Universität Darmstadt
	Prof. Dr. Ir. Raymond N. J. Veldhuis University of Twente
Tag der Einreichung:	04. August 2011
Tag der mündlichen Prüfung:	19. September 2011

Erscheinungsjahr 2012

Darmstädter Dissertation
D 17

谨以此献给我的父亲母亲

Dedicated to my dear parents

古今之成大事、大学问者，必经过三种之境界：“昨夜西风凋碧树，独上高楼，望尽天涯路。”此第一境也。“衣带渐宽终不悔，为伊消得人憔悴。”此第二境也。“众里寻他千百度，蓦然回首，那人却在灯火阑珊处。”此第三境也。

——王国维·人间词话

The Three Realms of Scholarship

– Wang, Guo-Wei, “Ren Jian Ci Hua”, 1908

Throughout the ages all those who have been highly successful in great ventures and in the pursuit of great learning must have successfully undergone three stages:

> “Last night the west wind shriveled the green-clad trees; alone I climb the high tower, to gaze at the road stretching to the horizon” represents the first stage.
>
> “I have no regrets as my girdle grows looser on my waist; with everlasting love I pine for you” represents the second stage.
>
> “I have sought her in the crowd a hundred, a thousand times; suddenly turning back my head, I see her under the dimming lanterns” represents the third stage.

Erklärung zur Dissertation

Hiermit versichere ich die vorliegende Dissertation selbständig nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 4. August 2011 Xuebing Zhou

Abstract

Biometrics enables convenient authentication based on a person's physical or behavioral characteristics. In comparison with knowledge- or token-based methods, it links an identity directly to its owner. Furthermore, it can not be forgotten or handed over easily. As biometric techniques have become more and more efficient and accurate, they are widely used in numerous areas. Among the most common application areas are physical and logical access controls, border control, authentication in banking applications and biometric identification in forensics.

In this growing field of biometric applications, concerns about privacy and security cannot be neglected. The advantages of biometrics can revert to the opposite easily. The potential misuse of biometric information is not limited to the endangerment of user privacy, since biometric data potentially contain sensitive information like gender, race, state of health, etc. Different applications can be linked through unique biometric data. Additionally, identity theft is a severe threat to identity management, if revocation and reissuing of biometric references are practically impossible. Therefore, template protection techniques are developed to overcome these drawbacks and limitations of biometrics. Their advantage is the creation of multiple secure references from biometric data. These secure references are supposed to be unlinkable and non-invertible in order to achieve the desired level of security and to fulfill privacy requirements.

The existing algorithms can be categorized into transformation-based approaches and biometric cryptosystems. The transformation-based approaches deploy different transformation or randomization functions, while the biometric cryptosystems construct secrets from biometric data. The integration in biometric systems is commonly accepted in research and their feasibility according to the recognition performance is proved. Despite of the success of biometric template protection techniques, their security and privacy properties are investigated only limitedly.

This predominant deficiency is addressed in this thesis and a systematic evaluation framework for biometric template protection techniques is proposed and demonstrated:

Firstly, three main protection goals are identified based on the review of the requirements on template protection techniques. The identified goals can be summarized as security, privacy protection ability and unlinkability. Furthermore, the definitions of privacy and security are given, which allow to quantify the computational complexity estimating a pre-image of a secure template and to measure the hardness of retrieving biometric data respectively.

Secondly, three threat models are identified as important prerequisites for the assessment. Threat models define the information about biometric data, system parameters and functions that can be accessed during the evaluation or an attack. The first threat model, so called naive model, assumes that an adversary has very limited information about a system. In the second threat model, the advanced model, we apply Kerckhoffs' principle and assume that essential details of algorithms as well as properties of biometric data are known. The last threat model assumes that an adversary owns large amount of biometric data and this allows him to exploit inaccuracy of biometric systems. It is called the collision threat model.

Finally, a *systematic* framework for privacy and security assessment is proposed. Before an evaluation process, protection goals and threat models need to be clarified. Based on these, the metrics measuring different protection goals as well as an evaluation process determining the metrics will be developed. Both theoretical evaluation with metrics such as entropy, mutual information and practical evaluation based on individual attacks can be used.

The framework for privacy and security assessment is applied on the biometric cryptosystems: fuzzy commitment for 3D face and iris recognition is assessed. I develop my own 3D face recognition algorithm based on the depth distribution of facial sub-surfaces and integrate it in the fuzzy commitment scheme. The iris recognition is based on an open source algorithm using Gabor filter. It is implemented in the fuzzy commitment scheme with the two layer coding method as proposed by Hao et al.

Both features, the 3D face features and the iris features, represent local characteristics of the modalities. Thus, strong dependency within these features is observed. The second order dependency tree is applied to describe the distribution of 3D face features. The Markov model is applied to characterize the statistical properties of iris features. Thus, security and privacy of these algorithms can be measured with theoretical metrics. Due to strong feature dependency, the achieved security is much smaller than the secret size, which is the assumed security in a perfect secure case with uniformly identically distributed features.

Moreover, the unlinkability is analyzed. The analysis shows that these protected systems are less vulnerable to leakage amplification. However, the secure templates contain much personal identifiable information. We demonstrate the attacks, which can identify a subject by linking auxiliary data stored in his secure templates. Cross matching is assessed with the performance of these attacks.

Additionally, the characteristic of iris features is exploited to perform an attack retrieving features from secure templates. The efficiency of the practical attack confirms the result of the theoretical assessment of privacy with conditional entropy.

The coding process plays a very important role for the security and privacy properties in the fuzzy commitment scheme. Designing a coding method should not only focus on the improvement of code rate. As shown in this thesis, security and privacy properties can be enhanced significantly by changing the dependency pattern in iris features and 3D face features. Therefore, the coding process should be adapted to properties of the underlying biometric features to increase the security and privacy performance.

The security and privacy assessment within this thesis is completed by a comparison of two fuzzy commitment algorithms with the fuzzy vault algorithm for fingerprint recognition. Here, different threat models as well as the corresponding protection goals are considered. The fuzzy vault system has the best performance regarding security and irreversibility of biometric features. However, all of these systems are vulnerable to cross matching. The comparison results show that the proposed evaluation framework provides the fundamental basis for benchmarking different template protection algorithms.

The proposed framework is also validated with the existing security analysis on transformation-based approaches. Unlike the analysis on biometric cryptosystems, the security is dependent on the hardness of transformation functions or randomization processes. Therefore, the presented analysis is based on efficiency of different kinds of attacks, which measure different protection goals in the appropriate threat models. The security of these approaches depends on the transformation parameters. The knowledge of these parameters allows generating a pre-image, while it is still hard to estimate the original biometric features practically. However, privacy leakage amplifications are still possible.

This thesis defines a systematic evaluation framework, which adheres to essential criteria and requirements of biometric template protection techniques. Its applicability is demonstrated with the analysis of template protection algorithms for different biometric modalities. The assessment presented in this thesis is fundamental for a thorough analysis. Furthermore, it provides provable evidence on security and privacy performance. Therefore, it is the fundamental tool for technical innovation and improvement and helps system designers in selecting a suitable template protection algorithm for their applications and needs. It creates a basis for certification and benchmarking of biometric template protection.

Zusammenfassung

Biometrie ist eine komfortable Authentifizierungsmethode basierend auf körperlichen oder verhaltenstypischen Charakteristiken. Im Gegensatz zu wissens- oder tokensbasierten Methoden, kann sie eine Identität direkt mit der zugehörigen Person verbinden. Darüber hinaus können biometrische Merkmale nicht vergessen oder einfach weitergegeben werden. Da biometrische Techniken immer effizienter und präziser werden, sind sie in vielen Bereichen weit verbreitet. Zu den häufigsten Anwendungsgebieten zählen physische und logische Zugangskontrolle, Grenzkontrolle, Authentifizierung in Bankengeschäften und biometrische Identifikation in der Forensik.

Durch die wachsende Zahl von Anwendungsbereichen ziehen Bedenken bezüglich der Privatsphäre und Sicherheit viel Aufmerksamkeit auf sich. Die Vorteile der Biometrie können sich leicht in das Gegenteil umkehren. Die Nutzung von biometrischen Daten gefährdet die Privatsphäre der Benutzer, da biometrische Daten möglicherweise vertrauliche Informationen wie Geschlecht, Rasse, den Gesundheitszustand usw. enthalten. Außerdem können verschiedene Anwendungen durch eindeutige biometrische Daten verknüpft werden. Zusätzlich ist Identitätsdiebstahl eine ernste Gefahr für Identitätsmanagement, weil Widerruf und Erneuerung von biometrischen Referenzen praktisch unmöglich sind. Deswegen werden Template-Protection-Techniken entwickelt, um diese Nachteile und Einschränkungen der Biometrie zu vermeiden. Deren Vorteil ist die Schaffung von mehreren sicheren Referenzen aus biometrischen Daten. Diese sicheren Referenzen dürfen nicht verknüpfbar und nicht umkehrbar sein, um das gewünschte Sicherheitsniveau zu erreichen und die Anforderungen an den Schutz der Privatsphäre zu erfüllen.

Die existierenden Template-Protection-Verfahren können in transformationsbasierte Verfahren und biometrische Kryptosysteme kategorisiert werden. Die transformationsbasierten Verfahren nutzen unterschiedliche Transformations- oder Randomisierungsfunktionen, während die biometrischen Kryptosysteme Geheimnisse aus biometrischen Daten generieren. Die Integration der Verfahren in biometrische Systeme ist allgemein im Forschungsbereich akzeptiert und deren Durchführbarkeit ist hinsichtlich der Erkennungsleistung bewiesen. Trotz des Erfolgs sind deren Sicherheits- und privatsphäreerhaltenden Eigenschaften nur bedingt untersucht.

Dieser wesentliche Mangel wird mit dieser Arbeit behoben. Ein systematisches Evaluierungsframework für Template-Prtoection-Verfahren wird vorgeschlagen und validiert:

Zunächst werden drei wesentliche Protection-Goals (Schutzziele) identifiziert, die sich aus den Anforderungen an Template-Protection ergeben. Die Protection-Goals können als Sicherheit, Schutzfähigkeit der Privatsphäre und Unverknüpfbarkeit zusammengefasst werden. Darüber hinaus sind die Definitionen für Schutzfähigkeit der Privatsphäre und Sicherheit gegeben. Diese quantifizieren den rechnerischen Aufwand bei Pre-Image-Abschätzung eines sicheren Templates und bei der Rekonstruktion biometrischer Daten.

Außerdem werden drei Bedrohungsmodelle als wichtige Voraussetzungen für die Evaluierung ermittelt. Die Bedrohungsmodelle definieren die Informationen, einschließlich System-Parameter und Funktionen, auf die bei einer Evaluierung oder einem Angriff zugegriffen werden kann. Das erste Bedrohungsmodell, das so genannte naive Modell, setzt voraus, dass einem Angreifer sehr begrenzte Informationen über ein System zur Verfügung stehen. In dem zweiten Bedrohungsmodell, dem erweiterten Modell, setzen wir das Kerckhoffs' Prinzip ein und gehen davon aus, dass wesentliche Details eines Algorithmus sowie Eigenschaften der biometrischen Daten bekannt sind. Das letzte Bedrohungsmodell nimmt an, dass ein Angreifer eine große Menge biometrischer Daten

besitzt und die Ungenauigkeit des biometrischen Systems ausnutzen kann. Deswegen wird es Kollisionsmodell genannt.

Schließlich wird ein systematisches Framework entwickelt, das genutzt werden kann, um die Schutzfähigkeit der Privatsphäre und die Sicherheit zu bewerten. Vor einem Evaluierungsprozess werden Protection-Goals und Bedrohungsmodelle festgelegt. Basierend auf diesen, werden die Metriken, die verschiedene Protection-Goals messen, sowie zugehörige Analyseprozesse hergeleitet. Sowohl die theoretische Analyse mit Metriken wie Entropie, bedingte Entropie, Transinformation als auch die praktische Analyse, die auf einzelnen Angriffen basiert, können genutzt werden.

Wir wenden das Framework auf die biometrische Kryptosysteme an: das Fuzzy-Commitment-Verfahren für 3-D-Gesichts- und Iriserkennung wird evaluiert. Wir entwickeln unseren eigenen 3-D-Gesichtserkennungsalgorithmus, der auf der Tiefenverteilung der Gesichtsoberflächen basiert. Das Fuzzy-Commitment-Verfahren wird erfolgreich integriert. Ein Gabor-Filter-basierter Open-Source-Algorithmus wird für die Iriserkennung verwendet und in dem geschützten System wird das zweistufige Kodierungsverfahren von Hao umgesetzt.

Beide Merkmale, die 3-D-Gesichtsmerkmale und die Irismerkmale, repräsentieren lokale Eigenschaften der Modalitäten. Deswegen wird eine starke Abhängigkeit in diesen Merkmalen beobachtet. Wir verwenden einen Abhängigkeitsbaum zweiter Ordnung, um die Verteilung von 3-D-Gesichtsmerkmale zu beschreiben. Das Markovmodell wird angewendet, um die statistischen Eigenschaften der Irismerkmale zu charakterisieren. Die Sicherheit und die Schutzfähigkeit der Privatsphäre werden mit informationstheoretischen Metriken gemessen. Wenn die Merkmale gleichmäßig identisch verteilt wären, wäre das System perfekt sicher und die Sicherheit könnte über die Geheimnislänge gemessen werden. Aufgrund der starken gegenseitigen Abhängigkeit der Merkmale ist die erreichte Sicherheit jedoch viel geringer als die Geheimnislänge.

Darüber hinaus analysieren wir die Unverknüpfbarkeit. Diese gestützten Systeme geben nicht viel mehr Informationen über die biometrischen Daten bei der Verknüpfung mehrerer sicherer Templates preis, als wenn nur ein sicheres Template zur Verfügung steht. Jedoch beinhalten die sicheren Templates viele personenbezogene Daten. Wir demonstrieren Angriffe, mit denen Personen anhand der Verknüpfung sicherer Templates verifiziert werden können. Die Verknüpfbarkeit wird mit den Erfolgswahrscheinlichkeiten der Angriffe bewertet.

Zusätzlich nutzen wir die statistischen Eigenschaften der Irismerkmale aus und führen einen Angriff durch, um Irismerkmale aus sicheren Templates zu rekonstruieren. Die Effizienz dieses praktischen Angriffs bestätigt das Ergebnis der theoretischen Analyse über die Schutzfähigkeit der Privatsphäre mit bedingter Entropie.

Der Kodierungsprozess spielt eine sehr wichtige Rolle für die Sicherheit und den Schutz der Privatsphäre in Fuzzy-Commitment-Systemen. Das Design eines Kodierungsverfahrens sollte sich nicht nur auf die Verbesserung der Coderate fokussieren. Wie in dieser Arbeit gezeigt, können sich die Sicherheit und der Schutz der Privatsphäre durch Änderungen der Abhängigkeitsmuster in Iris- und 3-D-Gesichtsmerkmale verbessern. Deswegen sollte der Kodierungsprozess an die Eigenschaften der zugrunde liegenden biometrischen Merkmale angepasst werden.

Die Evaluierungsarbeit wird mit einem Vergleich der beiden Fuzzy-Commitment-Systeme und des Fuzzy-Vault-Systems für Fingerabdruckerkennung abgeschlossen. Hier werden verschiedene Bedrohungsmodelle sowie die entsprechenden Protection-Goals betrachtet. Das Fuzzy-Vault-System hat die beste Leistung im Hinblick auf Sicherheit und Schutz der Privatsphäre. Doch alle Systeme sind anfällig für Verknüpfungsangriffe. Die Vergleichsergebnisse zeigen, dass das vorgeschlagene Framework eine Grundlage für das Benchmarking der Template-Protection-Techniken geschaffen hat.

Wir validieren das Framework mit den bestehenden Sicherheitsanalysen über die transformationsbasierten Verfahren. Im Gegensatz zu Analyse der biometrischen Kryptosysteme ist hier die Sicherheit von der Härte einer Transformationsfunktion oder eines Randomisierungsprozesses abhängig. Deshalb basiert die präsentierte Analyse auf der Effizienz der verschiedenen Angriffe. Die Angriffe messen verschiedene Protection-Goals in den

entsprechenden Bedrohungsmodellen. Die Sicherheit dieser Ansätze hängt von den Transformationsparametern ab. Die Kenntnis dieser Parameter ermöglicht die Erzeugung eines Pre-Image. Die Rekonstruktion der originalen biometrischen Daten kann jedoch sehr schwierig bleiben. Durch die Verknüpfung der sicheren Templates können mehr Informationen über die biometrische Daten erhalten werden.

In dieser Arbeit wird ein systematisches Evaluierungsframework entwickelt, das sich an die wesentlichen Kriterien und Anforderungen an biometrische Template-Protection-Verfahren festhält. Seine Anwendbarkeit wird durch die Analyse der verschiedenen Algorithmen demonstriert. Die in dieser Arbeit präsentierte Evaluierung ist grundlegend für eine vollständige Analyse. Darüber hinaus ermöglicht es einen Nachweis der Sicherheit und Einhaltung der Privatsphäre. Daher ist es ein unverzichtbares Werkzeug für technische Innovationen und Verbesserungen. Es hilft Systemdesignern bei der Auswahl eines geeigneten Algorithmus für ihre Anwendungen und Anforderungen. Es schafft eine Basis für Zertifizierung und Benchmark der Template-Protection-Verfahren.

Acknowledgements

I would like to express my gratitude to the following people for supporting my thesis: my adviser Prof. Dr. techn. Dieter W. Fellner, my second adviser Prof. Dr. Ir. Raymond N. J. Veldhuis, the research coach at Fraunhofer IGD Dr. Ir. Arjan Kuijper, and my additional advisers Prof. Dr. Christoph Busch and Prof. Dr. Stephen D. Wolthusen. I would like to thank Prof. Dr. Fellner for his requirement of scientific excellence and the valuable discussions on the topic. I would like to thank Prof. Dr. Veldhuis for being the second adviser and his scientific input and support. I would like to thank Arjan. He taught me how to work and write scientifically. He made a lot of effort to help me enhance the thesis. Christoph and Stephen have guided me from the very beginning not only with their professional competence but also their great personality. Christoph motivated me to finish the thesis step by step and showed me how to do project work. Even in hard time, his magic motto "Alles wird gut!" gives me power to face problems and to go forward. As a very strict professor, Stephen always asked complicated questions. I appreciate these questions very much, which really helped me to improve my work. I benefit a lot from his preciseness and perfection in research.

I am very grateful to Prof. Dr. Stefan Katzenbeisser who carefully reviewed my thesis. I would like to thank Dr. Tom Kevenaar. The discussions with him broadened my mind in this topic. Thanks for his advice on Chapter 3. My thanks go to Prof. Dr. Ir. Frans M. J. Willems and Dr. Tanya Ignatenko. They spent their time to discuss essential problems in this area with me. Thanks for their guidance and suggestions. I would like to thank Dr. Olaf Henniger for the detailed reviews of the whole thesis. Thank you for his valuable feedbacks and comments.

I would like to give a special thank to Dr. Marin Schmucker. Martin was the supervisor of my Diploma thesis. I joined the team at Fraunhofer IGD because of him. Although he left IGD already four years ago, he never stopped helping and encouraging me. He is the kindest person that I have ever known. I am happy and lucky to have him as a friend.

I would like to thank all my colleagues at Fraunhofer IGD, Jaime Corvera, Peter Ebinger, Elfriede Fitschen, Olga Kähm, Jaromir Likavec, Claudia Nickel, Alexander Nouak, M. Margarida P. C. Neves, Alexander Opel, Jan Peters, Dr. Ulrich Pinsdorf, Ute Rau, Frank Seibert, Helmut Seibert, and Dr. Wolfgang Funk. It was wonderful time working with them. Many thanks go to Claudia. We spent nice time together on discussions and sharing experiences. She did great work correcting my thesis. I also would like to thank Peter, who makes everything in our team go smoothly. He and his wife Julia are my best friends, who always offer their helps and kindness in my difficult moments. The 3D FACE was the first big project I have worked on. I would like to thank all members of this project, in particular Prof. Dr. Farzin Deravi, Dr. Michael Brauckmann, Dr. Emile Kelkboom and Prof. Dr. Ir. Luuk J. Spreeuwers not only for the great cooperation but also for encouragement and helps on my work.

At the end, I would like to thank my dear parents for their great spiritual support. They always show me what is the essential of life, when I am lost. They give me the power to face all difficulties. It was not easy to finish this thesis. I am very lucky to have some many supporters, colleagues and friends to help me. Thank you!

Contents

1. Introduction

The human perception system recognizes a person based on face, voice, gait information, etc. Similarly, biometric techniques automatize recognition process based on physical or behavioral traits of a person. Nowadays biometrics is not only exploited in forensics or high security areas but also is coming into everyday life. It is due to increasing requirements on security and concerns on safety of citizens. In on-line banking or accessing confidential documents in a company, it is necessary to authenticate whether a person with a claimed identity is really the owner of that identity. The knowledge- or token-based authentication cannot meet this challenge: A token or password can be stolen or handed over and they cannot provide a unique link between an identity and a person himself. Furthermore, biometrics is currently a very powerful tool against terrorists. In Europe, face photos and fingerprints are stored in e-Passports. In the US visit program, 10 fingers and face images are also acquired to support visa application and border control. Uniqueness of biometric features is helpful to cut down duplicate identities or identity fraud. This nice security property benefits e-commerce applications a lot. It can for instance prevent unauthorized access to buildings or cell phones and ensure that a session ticket is only used by its holder. Additionally, it has a big advantage of convenience. Biometric users do not need to remember long passwords or to worry about forgetting their ID-cards.

As biometrics plays a growing role in diverse application areas, their security and privacy concerns grab the attention of researchers, public sectors, government agencies and end users. Biometric information needs to be stored for the sake of authentication. However, if personal biometric data fall into hands of adversaries, serious security and privacy problems arise. An adversary can create a fake modality to spoof biometric systems. He can also track activities of a victim in other biometric applications. Unfortunately a biometric modality is hard or impossible to change. Compromise of biometric data is permanent. Renewing or revocation of biometric identities is infeasible. Additionally, biometric data are important private information and may contain sensitive information such as gender, race, genetic and disease information. Collection of biometric information is critical in many countries because of privacy legislation.

This has stimulated research on the protection of stored biometric data in recent years. Template protection techniques, also referred to as biometric encryption, untraceable biometrics, cancelable or revocable biometrics, have been developed. These techniques convert biometric data elements into multiple (ideally) uncorrelated secure templates, from which it is infeasible to retrieve the original information. Biometric information can be protected and creation of a fake modality from stored templates is impossible. Issuing distinct templates from one biometric data can stop cross matching between different applications. It also enables revocation and renewing of a template, which are crucial functionalities in identity management. Centralized storage of a reference as well as identification are feasible with consent of privacy law. With template protection, biometrics can be safely exploited in manifold applications associated with multiple secure templates. It minimizes data used in authentication, so that misuse or abuse of biometric information can be avoided. Users of such a system don't need to worry to expose or to loose control of their private information. System providers can popularize usage of biometrics with increasing user acceptance and without any limitation of privacy law. Template protection maintains the advantages of biometrics and vanquishes its security and privacy drawbacks. The developments of the techniques are quite successful. Some of them are already available on markets. In this work we will focus on security and privacy aspects of template protection.

1.1. Research Questions and Contributions

As an important supplement to biometrics, template protection techniques aim at enhancing privacy and security. Researchers have designed different kinds of template protection algorithms. Although integration of these algorithms to biometric systems is quite successful regarding recognition performance, the evaluation of security and privacy performance is still a weak point.

The current assessment cannot give convincing proofs on security and privacy. The existing theoretical works give the boundaries of security capacity (maximum secret rate) and privacy leakage. However, they are not able to represent the security and privacy in real systems. Some fundamental assumptions made in these work are hard to apply in practice, for instance, identically independently distributed input biometric features. Security analyses in the existing implementation papers propose different security metrics and come up with different evaluation results. It is not clear, according to which criteria these algorithms are really secure and whether these metrics are proper in security measurement. Other security analyses propose attacks on template protection. All of these works address only a part of security and privacy requirements and lack the determination at a general level.

The main research question addressed in this thesis is:

> ***How can we make a comprehensive and systematic assessment of the privacy and security performance of biometric template protection algorithms?***

We solve this main question step by step through the following sub problems:

1. What are the *criteria* to evaluate privacy and security of these algorithms?
2. How can we *define* the security and privacy of these algorithms?
3. How can we *measure* the security and privacy of these algorithms quantitatively?
4. How can we *rank* these algorithms regarding security and privacy?

In this work we propose *protection goals* as evaluation criteria, which cover different security and privacy requirements on template protection. The protection goals include security of templates, privacy protection ability and unlinkability. Moreover, we show the metrics and methods to quantify protection goals. The *definitions* of security and privacy are given regarding the computational complexity to break an authentication and to retrieve biometric data. In order to enable rigorous assessment, we need to know the adversaries' ability. We define three *threat models*, which give realistic assumptions on the resource and information available to potential adversaries. In the *naive* model, we assume that an adversary has no information about the system; in the *advanced* model we suppose that an adversary has full knowledge of the algorithm and properties of the biometric data; in the *collision* model, we presume that an adversary owns a large amount of biometric data and can exploit inaccuracies of the biometric system. These threat models are the prerequisites for an evaluation.

Based upon these, we propose a *generalized evaluation framework*, from which we design rigorous security and privacy assessment for different template protection systems. The framework considers all security and privacy aspects and allows a thorough analysis. The framework supports both the evaluation using theoretical metrics and the practical evaluation based on individual attacks. We validate the framework in two template protection systems, the fuzzy commitment systems for 3D face recognition and iris recognition. We quantify their security and privacy. Especially in the evaluation under the advanced threat model, we analyze the distribution of 3D face features and iris features. We find out that the security of these systems is very poor due to the dependency of biometric features. Additionally, we compare three different protection systems with the help of the framework. A basis for ranking different algorithms regarding security and privacy is created. We also demonstrate the generality of the framework using the existing security analyses of other template protection algorithms. The framework is an indispensable tool for security and privacy evaluation.

1.2. Outline of the Thesis

This thesis is organized as follows:

Chapter 2 gives an overview of biometric template protection techniques. The vulnerabilities in common biometric systems such as identity theft, unchangeability, cross matching and harm of privacy are elaborated. Different kinds of template protection algorithms are described. Furthermore, the high level abstract construction of template protection issued in the ISO international standard is shown. The desired properties of template protection are summarized. Furthermore, the security of biometrics at a system level is analyzed. It is shown that template protection is indispensable to enable renewability, to provide irreversibility and to avoid linkability in biometric systems.

Chapter 3 is the key chapter of the thesis. A generalized evaluation framework assessing privacy and security of template protection is proposed. The existing security analyses lack comprehensive investigation. Therefore, we identify the protection goals, which cover all security and privacy requirements. Meanwhile, threat models are given that limit the information and resource available for an adversary. The metrics assessing different protection goals are shown. The definitions of privacy and security with measurable metrics are given. Based on these, a generalized framework, which enables a rigorous evaluation process, is developed. At the end of the chapter, we analyze closely two important template protection algorithms, fuzzy commitment and fuzzy vault, regarding the identified protection goals.

Chapter 4 gives a rigorous evaluation of a protected 3D face recognition system. A histogram-based 3D face recognition algorithm is developed, which shows good recognition performance and computational efficiency. A template protection system using the fuzzy commitment scheme is built. A long secret can be derived and the recognition performance of the protected system is slightly reduced in comparison with the original unprotected system. The feasibility of fuzzy commitment for the 3D face recognition system is proved. Later, the security and privacy of the protected system is strictly analyzed. The statistical properties of the 3D facial features are characterized with a second order dependency tree. It allows quantitative measurement of the security and privacy protection ability. The achieved security is much lower than in an ideal perfectly secure case. Privacy leakage exists for the sake of error tolerance. Additionally, cross matching is evaluated with a practical attack. The possibilities to improve the resistance to linkage problems are discussed.

Chapter 5 assesses a protected iris recognition system. Iris features are extracted with an open source algorithm using Gabor filter. We implement the fuzzy commitment algorithm with a two-layer coding scheme proposed by Hao et al., which is a fundamental work of protecting iris features. The author claimed high security of this algorithm. We systematically analyze the protected system. We find out that the iris codes have Markov property. This introduces high leakage of security and privacy. We quantify the protection goals. Additionally, we prove the results of our security analysis with a cracking algorithm. Both iris features and secrets can be retrieved with low complexity.

Chapter 6 demonstrates how to compare different kinds of template protection systems with the help of the evaluation framework. Additionally, the framework is validated for the transformation-based template protection algorithms. The evaluations of the two real systems are summarized and completed for all threat models. The unique metrics given in the security and privacy definitions enable the comparison of the two demonstrated systems and a fuzzy vault system for fingerprint recognition. It can be proved that the fuzzy vault system is the best system regarding security. However, all these systems have high privacy leakage. The linkage is a serious problem in these systems. We also show that the framework is qualified to evaluate transformation-based algorithms. The existing analyses of these algorithms measure one or more protection goals for special threat models.

Chapter 7 concludes the thesis. The contributions of this thesis are highlighted. The benefits of this work are elaborated. An outlook for future research is given.

The appendices show the essential mathematic preliminary used in the thesis. In Appendix A the definition of the entropy, Min-entropy and guessing entropy, etc., are shown, which are important metrics for security and privacy assessment. Additionally the basic properties of binomial distribution and Markov chain are summarized, which are used in Chapter 4 and Chapter 5 to analyze the distribution of biometric features. Additionally the coding methods play an essential role for fuzzy commitment scheme. Appendix B shows the basic properties of linear block codes and introduces the BCH and RS codes as well as Hadamard code.

2. Biometric Template Protection

Template protection is an important privacy and security enhancing technique for biometrics. In this chapter we introduce this technique and give a detailed overview of the existing algorithms. Although biometrics provides considerable convenience and also some security advantages over token- or password-based authentication methods, the related privacy and security issues should not be underestimated. We reveal the privacy and security vulnerabilities in biometric systems such as strengthening of identity theft, cross matching between applications, and exposure of the user's sensitive information. Then, we elaborate biometric template protection techniques, which aim to stop abuse of biometric information. The idea is to derive numerous independent non-invertible references from a biometric datum, so that retrieval of original biometric information or tracing of individuals is infeasible. Different algorithms exist, which can be divided into transformation-based approaches and biometric cryptosystems. All these algorithms can be well described with a general architecture according to ISO international standard. Additionally, we summarize the desired properties of these algorithms, namely, irreversibility, robustness, diversity and unlinkability. At the end we reinvestigate the security and privacy requirements of biometric systems and show the corresponding possible countermeasures. We emphasize that among them, template protection is the only tool to enable the desired renewability of templates. Additionally, it can provide unlinkability and safeguard users' privacy. Therefore, template protection is an indispensable supplementary to biometric systems.

2.1. Privacy and Security Vulnerabilities in Biometric Systems

People are able to recognize other persons based on their face, voice, gaits trait, etc. Scientists reproduce this inherent way of authentication with automatic processes, so called biometric techniques. Many modalities can be adopted for recognition. They can be physiological characteristics such as face, fingerprint, iris, palmprint, vein, or behavioral ones like voice, taping rhythms, or the combinations of them. With these characteristics, an identity can be bound tightly with its owner. Neither is any physical possession like ID-document or smartcard required, nor is it needed to remember any prolong password. Therefore biometrics is becoming a strong competitor and supplementary to the traditional token- or knowledge- based authentications. It is a powerful tool against identity fraud.

A biometric system consists of acquisition, preprocessing, feature extraction, data storage and comparison processes. In an acquisition process, a sensor device gives a digital representation of a biometric modality. A preprocessing process filters irrelevant information and segments region of interest. For instance, a preprocessing in a 2D face recognition system includes normalization of face into a frontal view, illumination correction, crop of the facial area etc. In an extraction process, robust and discriminative features are derived. A subject, namely a user of a biometric system, should firstly be enrolled in a biometric system and can be authenticated afterwards. In an enrolment, biometric features or samples are stored as templates. In an authentication, a feature generated from a queried sample is compared with the stored data. It is distinct from verification and identification. In a verification scenario, an identifier of a subject is known (e. g. user ID, card number) and the queried datum is compared with one stored datum. In an identification scenario, no identifier information is available and searches in a database are necessary. An identification system requires high computational power.

Biometrics is a special application of pattern recognition. Biometric systems are designed to maximize difference of features between distinct subjects and minimize the variation of biometric data from the same subject. Acquisition devices are expected efficient and economical. They should be tolerant to changes of environment and modalities, such as strong or weak light in face recognition, humidity of fingerprint, temperature of body by vein recognition etc. The preprocessing is an important step to reduce noise in acquired samples. Quality measurement can be included and only samples with good quality are further processed. A new acquisition can be required if sample quality is not satisfactory. A feature extractor and a comparator aim at separating intraclass and interclass distributions of features. Normally a training process is necessary to adapt parameters used in an extractor and a comparator and to optimize recognition performance.

As biometric systems become more and more efficient, accurate and cost-effective, biometric applications are growing rapidly in areas such as physical and logical access control, time of attendance, e-Passport, border control, identity documents, banking, etc. Biometric users more and more appreciate benefits applying biometrics; meanwhile, new vulnerabilities of biometric systems and potential security risks have been drawing a lot of attention:

Identity fraud Biometric characteristics can not be copied, stolen or handed over like a token or a password. However, they can be faked. For example, it is shown in [MMYH02, CCCe04], how effortless to make a gummy or laminate finger using a left trace on a glass. With a camera, facial information can be completely exposed even without knowledge or consent of victims. A synthetic artifact can be created with stored biometric templates [Hil01, Bro06, Adl03]. To attack remote authentication systems based on digital transmitted biometric data, reconstruction of a biometric modality is even not necessary. These flaws strengthen identity fraud. Integrating liveness detection techniques in sensors is necessary to prevent counterfeits. Meanwhile, protection of stored and transmitted biometric data is also urgently required to avoid unauthorized access and exposure.

Irrevocable/Non-revocable references Applying biometrics, subjects and their identities are linked together with their unique personal biometric characteristics. In case that biometric data are compromised, they cannot be easily revoked or renewed as in password- or token- based authentication. We can only chose another biometric modality or try to modify the exposed one. Unfortunately, both are not suitable solutions: we own a limited number of biometric modalities, e.g. ten fingers, one face, two irises, on the other hand, an alteration is possible only with very complicated methods such as transplantation, cosmetic surgery.

Cross matching As the same biometric modality is adopted in multiple applications, all these applications are potentially linked. A malicious data collector can misuse these information and track activities of a subject in other applications. Additionally, if a biometric identity is compromised in one application, other biometric applications get also in danger.

Privacy Biometric data are derived from human bodies or activities of a person. It contains a lot of personal sensitive information. In [Sei06], the influence of disease and sexual orientation on fingerprint is shown. The eye disease such as free-floating iris cyst, diffuse iris melanoma and can change iris appearance. From a face photo, gender and race can be recognized. Applying DNA can expose genetic information. Such private information is not relevant for authentication purpose but is saved in biometric systems. In the European Data Protection Directive 95/46/EC [Dir95], it is defined that “[personal data] shall mean any information relating to an identified or identifiable natural person (‘data subject’)” and an individual have “the right of access to and the right to rectify the data concerning him”. In [ART03] of data protection working party in EU it is explicitly pointed out that biometric data are personal data. It also emphasizes the importance of using biometrics in privacy compliance way from legislation point of view.

Centralized storage By reason of interoperability, many applications such as AFIS, e-Passport, etc., have to collect, transmit and store biometric samples. Many biometric systems also need to store raw samples for re-training when software is updated and new subjects are enrolled. Despite of these, centralized storage of biometric data is indispensable in identification scenarios, such as forensics and double enrolment check. However, from the legislation point of view, the collection of biometric data is often strictly limited. Centralized storage of biometric data is critical due to privacy issue. Moreover, databases are the common attack target. Stored information can be intercepted, copied or tampered. It threatens the security of biometrics.

The above issued security and privacy problems arise from lacking protection of stored or transmitted biometric data. The Information and Privacy Commissioner/Ontario also elaborated in [CS07], that applying biometrics is often thought to be "a zero-sum game" regarding security. In [DSB07], the Office of the under secretary of defense for acquisition, technology and logistics in USA dwelt on the role of biometrics in identity management and show irrevocability is a big downside: "biometrics are forever, but their association with either an identity or with a privilege is not forever. Biometrics should never be used by themselves; when used as a reference, they need to be digitally signed, and their association with a privilege or identity must be revocable."

In order to overcome these drawbacks, safeguarding biometric data is necessary. In most commercial systems, biometric data are encrypted stored. Unlike common digital data, biometric templates or samples vary due to changes of body or ambient state, e.g. emotion changes, aging, humidity, illumination, etc. With a normal symmetric encryption, a comparison in an encrypted domain is not possible and decryption of data is needed. Risks that an adversary can access biometric data during comparison exist. Additionally a key management system is required. Recently, *homomorphic* encryption technique has been adopted to preserve privacy. It has a special property that some algebraic operations of plaintext are equivalent to other operations of the ciphertext. It allows comparisons of noisy data in an encrypted domain. An application in face recognition is shown in [EFG*09]. However, this method is computational expensive and can not solve unchangeability.

An alternative mechanism, "comparison on card" has been developed. Biometric data are stored decentralized in a smart card and can never leave the card. The card is held and managed by individuals. In order to prevent eavesdropping, substitution or replay, acquisition sensors as well as modules of feature extraction, comparison are all embedded in the smart card. Only a 'yes' or 'no' response is given after verifications. Nevertheless, the performance of this mechanism is limited by capacity of card storage and communication channel. Furthermore, each smart card must be authenticated prior to the usage of the contained template as well as its communication to outside. It is currently available for fingerprint recognition, since required sensors are small and recognition algorithms are relatively simple. It is incapable of identification.

Neither encryption nor "comparison on card" can give satisfactory resolution. In the following we introduce template protection techniques, which overcome these shortcomings of biometric systems. (In this section we focus only on the potential security and privacy risks happening during storage and transmission of biometric data. A system-level security observation will be given in Section 2.3.)

2.2. Biometric Template Protection

2.2.1. State of the Art

Template protection is a collective term for a variety of methods that aim to preserve privacy and enhance the secure storage of biometric data. Different kinds of algorithms exist, which can generate diverse unlinkable and non-invertible references from biometric data. In [JNN08] Jain et al. gave an overview on the existing techniques and categorized them into transformation-based approaches and biometric cryptosystems. The functions used in transformation-based approaches can distort or randomize biometric data so that the original data cannot be reconstructed from transformed templates. The renewability is realized by changing distortion parameters or randomization salt. Both parameters and salt are user- and application-specific. They are essential factors for security and must be kept secret. Different from encryption, secure templates can be compared directly. Additionally reconstruction of the original data should be hard or even impossible, even if this secret information is known. The biometric cryptosystems can embed or generate secrets from biometric data. With help of some auxiliary data, the secrets can be successfully and precisely retrieved in verification process. The secrets are comparable with cryptographic keys and can also be revoked and reissued. The auxiliary data should contain information neither about the secrets nor about biometric data and can be considered as public. Figure 2.1 shows the classification of template protection algorithms. In the following we show the details of different algorithms.

Template Protection		
Transformation-based Approach		Biometric Cryptosystem
Salting • Biometric encryption • Biohashing algorithm	Cancelable Biometrics	• Secure sketch • Fuzzy extractors • Fuzzy commitment scheme • Helper data architecture • Fuzzy vault scheme • Quantization index modulation

Figure 2.1.: An overview of template protection algorithms

Biometric salting methods use large random sequences to randomize biometric data. The random sequence is comparable with the salt used in cryptography to safeguard a key. Therefore this subclass of transformation-based approaches is called salting. Biometric encryption and biohashing are two typical salting methods.

In [RSGK99] Soutar et al. proposed *biometric encryption* method. A correlation filter is used to extract features from biometric samples in frequency domain and subsequently the features are multiplied with a random pattern. The result is transformed back into spatial domain and a blurred image is obtained. A random key is embedded into the image by providing a masked reference, which is stored in a lookup table. The randomized correlation filter, the lookup-table, and the hash of the key are stored in the user record. In verification, a blurred image can be reconstructed by multiplication of a queried image and the stored filter in frequency domain. With the help of the look up table, the key can be estimated. Every bit in the key contains more than one mask references in the lookup-table and the decision by majority is used to tolerate variation between the blurred images in enrolment and verification. The stored filter is strongly noised in comparison with the biometric features in frequency domain. Other stored data are not related to biometric data and privacy is preserved. A big advantage of this algorithm is that the random pattern is used only once in enrolment and is not stored. It reduces the risk of retrieving biometric data. However it is suspected to be vulnerable to hill-climbing attack (see Section 3.1.2). In [RSGK99], an implementation for fingerprint recognition is shown. This algorithm is well suited for image-based or 2D array biometric data, but recognition performance is limited by the correlation filter. This algorithm is also patented in [Pat01, Pat97, Pat96].

Similar algorithms are also used for face recognition [SKK04] and vein recognition [Tak07]. In [SKK04], Savvides et al. convolute face images with a random pattern before feature extraction and comparison process. For recognition, minimum average correlation energy (MACE) filter is used. They showed that convolution with the same random pattern does not influence the performance of MACE filter. In [Tak07], Takaragi convolute vein features with a random pattern after feature extraction. In verification, a queried vein feature is convoluted with the inversion of the random pattern. The comparison based on a mutual correlation map is not affected by the random pattern either. In these two methods the random patterns need to be stored secretly.

Biohashing algorithm converts biometric features randomly into binary sequences, so called biohashes, with a large amount of random codes. These random codes are typically stored in a token. Verification is possible only if both token and the authorized biometrics are present. It consists of two main processes, randomization and binarization. In [JLG04], Teoh et al. proposed biohashing for fingerprint recognition. Features are derived using an integrated wavelet and Fourier-Mellin transform framework (WFMT). The inner products of the feature and a matrix of orthogonal random patterns are calculated and binarized. The resulting bit string constitutes the pseudo identity of the subject. The idea behind is to project high dimensional features on randomly generated orthogonal basis vectors. The number of basis vectors is less than the dimensions of features. The orthogonality keeps Euclidean distance between the features in new feature space. Since different projection matrix is used, the discriminative power increases. However, Kong et al. showed later in [KCZ*06] that the recognition performance is degraded in comparison with the unprotected features in the case that projection matrix is stolen and used by impostor. This algorithm is further implemented for palm recognition [CTGN05], face recognition [TwGdCN06] etc.

In [AL09], Ao et al. also used scalar randomization process to protect infrared facial features. Here features are binarized by comparing them with randomly generated thresholds. In order to obtain uniformly distributed biohashes, the binarization thresholds have the same distribution as the interclass distribution of biometric features themselves. Moreover, the resulting biohashes are given as input for a fuzzy commit scheme. They showed that the biohashing process reduces the recognition performance, however, this degradation becomes smaller with increasing feature size.

A much more secure biohashing algorithm is also proposed by Teoh in [JTK07]. A set of complex numbers is built with randomly generated orthogonal vectors and biometric features, where random vectors and biometric features are imaginary and real part of the complex numbers respectively. The phase of the complex numbers according individual random vector are averaged. The averaged phase value is called biophasor and further discretized to improve recognition performance. The experimental results on FERET database with PCA feature extraction algorithm showed slight improvement of performance, even in the case that the randomization vectors are stolen. The one-wayness is also proved in the paper.

Cancelable biometrics belongs to transformation-based approach and transforms the original biometric features or samples using “non-invertible” functions. No match between the original data and transformed data exists. Diverse references can be generated by changing the transformation parameters of the functions. In [RCB01], a morphing function is used to distort a 2D facial image and extracting facial features from the distorted image. No match exists between the distorted and the original images or the images with other distortion parameters. Additionally, “one to many” transformations can be applied to biometric features so that retrieving the original feature is hard. Additionally, the robustness and discriminative power of the resulting references should not decrease, so that the classification power remains. In [RCCB07], the methods for minutiae-based fingerprint recognition with Cartesian, polar, and surface folding transformations, which change positions of the minutiae, are shown. In Cartesian transformation, a fingerprint image is divided into equal sized cells and a minutiae located in a cell is randomly projected into another cell with the projection parameter. It can happen that more than one cells are projected into the same cell. Polar transformation is similar as Cartesian transformation. Instead of equal sized cells, fingerprint region is divided into sectors and these sectors are also permuted into other position. Moreover the angle of a minutia is also altered. In surface folding transformation, a Gaussian kernel is used to change both position and angel information. The experimental results showed that surface folding gave the best performance. In all three transformation methods, pre-alignment of fingerprint is necessary. Another example of cancelable biometrics for iris recognition is shown in [ZRC08].

Biometric cryptosystems include fuzzy commitment, fuzzy extractor, fuzzy embedder, and fuzzy vault. This class has one-wayness property comparable with cryptographic functions. Additionally, they are robust to "fuzzyness" of biometric data.

In [JW99], Juels and Wattenberg introduced a *fuzzy commitment scheme*. The idea is to combine existing cryptographic function and error correction coding to protect noisy biometric data. Similarly to password authentication in Unix computer, biometric authentication is possible without knowing the original biometric information. The proposed fuzzy commitment scheme calculates a code offset, which is XOR between a randomly chosen error correction codeword and biometric feature. Only the code offset and the hash of the message code corresponding to the codeword are stored as secure reference. Error correction code makes the scheme error tolerant.

In [DRS04, DORS08], Dodis et al. defined *secure sketches* and *fuzzy extractors*. A $(\mathcal{M}, m, \tilde{m}, t)$-secure sketch consists of "sketch" (*SS*) and "recover" (*Rec*) functions: for biometric data $M \in \mathcal{M}$, $SS(M)$ returns a bit string in a binary space $\{0,1\}^\star$; if the distance between M and a queried M' is smaller than t, M can be successfully reconstructed and $M = Rec(M', SS(W))$. The min-entropy of M is denoted as m and the security is guaranteed by the average min-entropy $\tilde{H}_\infty(W|SS(W)) \geq \tilde{m}$. The definitions of min-entropy and average min-entropy are given in Appendix A.2. A $(\mathcal{M}, m, l, t, \varepsilon)$- fuzzy extractor consists of a generation function $Gen(X) = (S, W)$ and a reproduction function $Rep(Y, W) = S$. X and Y are data in $\mathcal{M}$ with min-entropy of m and $S \in \{0,1\}^l$. The secure string is nearly uniformly distributed even if its helper data is known. They also showed that fuzzy extractors are strongly related to secure sketches. The constructions of such functions in feature spaces under Hamming distance, set difference as well as edit distance were proposed. This construction covered other algorithms such as fuzzy commitment and fuzzy vault. Later, Buhan et al. showed practical implementation of fuzzy extractor for continuous noisy data in [BDH*08]. This algorithm can embed a secret directly into continuous data.

In [TG04], Tuyls et al. showed a *helper data architecture* for privacy preserving biometric authentication. Similar to fuzzy extractors, a secret and helper data are extracted in the enrolment. The helper data compensates difference between biometric data in enrolment and verification. More important, they proved that the secrecy capacity, the maximum secret rate with negligible small secrecy leakage in the helper data, is equal to the mutual information between biometric data in enrolment and verification. This architecture is comparable with secret extraction from common randomness. The fuzzy commitment scheme can be seen as a realization of helper data architecture.

The *fuzzy vault scheme* is also an important biometric cryptosystem designed for non-ordered features like minutiae of fingerprints. It was proposed by Juels and Sudan in [JS02]. The non-ordered features are in a set difference metric space, where the number of the components in the feature varies. A variant of Shamir's secret sharing protocol is used. In the algorithm, a polynomial is randomly created whose coefficients indicate the secret (key). The minutiae information is chosen as support points and projected on the polynomial. The vault contains pairs of the minutiae data and the corresponding projection. As the degree of the polynomial is lower than the number of minutiae used, a subset of minutiae is sufficient to recover the polynomial. This allows the cryptographic hash of the secret (i.e. the pseudo-identity) and the vault to be stored in the database; further obfuscation of the support points is provided by using *chaff* points.

The development of biometric cryptosystems is very successful. The fuzzy commitment scheme has been integrated in 2D face recognition system using texture information [vdVKS*06], fingerprints recognition system [VTDL03] and ear identification [TVI*04] etc. The implementation of the fuzzy vault scheme also achieved good performance as shown in [NJP07]. The security of biometric cryptosystems is comparable with underlying cryptographic model. Additionally no specific secret information is necessary and security can be guaranteed even if secure reference is made public.

Generally speaking, transformation-based approaches can be applied in both feature level and sample level. Their comparators are based on similarity measurement. However, biometric cryptosystems are normally integrated in feature level and use exact comparisons. In most transformation-based approaches, transformation parameters must be stored secretly. These algorithms are more proper for verification than for identification. Biometric cryptosystems do not require any secret information and secure references can be stored centralized, that facilitates identification. Transformation-based algorithms have an advantage in protection of biometric data. Even if transformation parameters and functions are compromised, biometric data can not be retrieved precisely. However, in biometric cryptosystems, inversion of secure references exposes essential information about biometric data. The security and privacy properties of transformation-based approaches and biometric cryptosystems will be discussed in Chapter 6. Biometric encryption can be used to protect biometric information in spatial or frequency domains and comparisons of secure references are based on correlation. Biohashing and cancelable biometrics can efficiently protect biometric data, however, degradation of discriminative power needs to be taken into account. Fuzzy commitment requires binary feature vectors as input. Fuzzy vault is appropriate for non-ordered feature set.

2.2.2. ISO Reference Architecture

The previous section gave an overview of the existing template protection algorithms. These algorithms are designed to diminish exposure of biometric data and to prevent possible attacks using stored or transferred data. They also enable revocation and renewing of templates, which are the crucial functionalities in identity management. Moreover, they can obviate linkages of different applications though similar templates. The international standard ISO/IEC 24745 [ISO11] defines a high-level architecture of template protection, which can model various types of algorithms. It consists of the following functions:

1. The *pseudonymous identifier encoder* (*PIE*) generates a pseudonymous identifier *PI* and auxiliary data *AD* from a biometric datum M in the enrolment: $[PI, AD] = PIE(M)$. *PI* is a protected identity of an individual or a data subject and *AD* is user-specific data, which help to reproduce *PI* in an authentication process. Only *PI* and *AD* are stored as a secure template in the system. The biometric datum M is deleted after the enrolment.
2. The *pseudonymous identifier recorder* (*PIR*) takes a queried biometric datum M' and the stored *AD* as inputs and calculates a pseudonymous identifier PI' in the verification: $[PI'] = PIR(M', AD)$.
3. The *pseudonymous identifier comparator* (*PIC*) compares PI' with the stored *PI*: $v = PIC(PI, PI')$. Depending on comparators, comparison result v is either a hard decision (yes/no) or a similarity score v.

Figure 2.2 depicts the construction of template protection with *PIE*, *PIR* and *PIC*. Biometric systems provide input data M and M' to template protection, which can be samples acquired directly from a sensor or some compact features extracted from biometric samples. Of course, the interface between a biometric system and a template protection algorithm marked with the red dashed line is an internal or virtual dataflow, which must be secure against any internal or external attack. The orange lines show the communication between *PIC*, *PIR* and *PIC*. They might take place over public and insecure channel. For instance, in many applications the enrolment stations and verification stations are not at the same location and the data needs to be centrally stored. A database easily becomes attack target. In remote enrolment or authentication, data needs to be transported, e.g. over internet. From security point of view, transferring and storing *PI*, which cannot conceal biometric information, are better than using biometric templates themself. Please note that *AD* is allowed to be public in some algorithms, however, in others *AD* is a secret parameter.

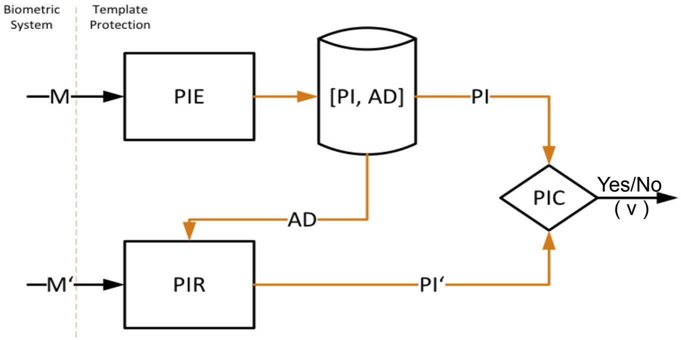


Figure 2.2.: ISO reference architecture of template protection

In order to produce secure and privacy-preserving templates, template protection must have the following properties:

Irreversibility The extraction of *PI* from biometric data with *PIE* and *PIR* should be efficient (executable with limited computational power), meanwhile, it is either computationally hard or impossible to deduce the underlying biometric data from *PI*.

Robustness Biometric data vary due to acquisition noise, environment changes, aging effect, etc. The derived *PI*s should be robust to variation of input biometric data and *PIC* can compare *PI*s directly. Additionally, applying template protection should not influence the recognition performance in comparison with the original biometric system.

Diversity and Unlinkability Numerous protected templates from one biometric characteristic that are independent of each other can be generated, i.e. knowledge of one protected template does not yield information on other protected templates derived from the same characteristics.

	Algorithm	**Requirements**			**Protected Template**	
		Irreversibility	Robustness	Unlinkability	*PI*	*AD*
Transformation-based Approaches	Biometric Encryption	Whitening of biometric sample and encryption	Correlation filter and key table	Randomly generated secret	Hash of secret	Randomized image and key table
	Biohashing	Random projection and binarization	Hamming distance comparator	Renewable projection basis	Transformed binary feature	Projection matrix
	Cancelable Biometrics	Non-invertible transformation function	Similarity comparator	Renewable transformation parameter	Transformed feature	Transformation parameter
Biometric Crypto-systems	Fuzzy Commitment	XOR and encryption	Error correction coding	Randomly generated secret	Hash of secret	Helper data
	Fuzzy Vault	Secret hiding and encryption	Similarity based retrieval	Randomly generated secret	Hash of secret	Point set

Table 2.1.: Examples of template protection algorithms: functions used in the algorithms and the meaning of *PI* and *AD*

Table 2.1 shows some examples of template protection algorithms. Different functions and constructions are used to meet the above-mentioned requirements. Additionally all these algorithms can be described with the ISO architecture. The meaning of *PI* and *AD* is also shown in the table. The first three algorithms belong to transformation-based approaches. Their *PI* is transformed features generated from transformation functions such as random projection, whitening. Their *AD* is parameters for the transformation functions. Renewing *PI* is through releasing a new *AD*. The *PIC*s use some similarity metrics or distance measure. The last two algorithms are biometric cryptosystems. Their *PI* is the hash values of randomly generated secrets, which can be renewed. Comparisons of *PI*s are based on exact matches. *AD* helps to tolerate noise and enables regeneration of *PI* in authentication.

A major difference of these two categories is the security. Transformation-based approaches require secret *AD* and their security is strongly dependent on the secrecy of *AD*. Biometric cryptosystems need no secret information. Both *PI* and *AD* are allowed to be public. It is also possible to combine methods from both categories or to use additional authentication information like passwords in a template protection algorithm. In this thesis, we only consider the basic transformation-based approaches and biometric cryptosystems without any combination or additional information in order to keep the problem simple at the beginning.

2.3. Biometric System Security

The components of biometric systems (sensor capturing biometric data, feature extraction, storage, and comparator as shown in Section 2.1) can be vulnerable to system internal or external attacks [CS07, JNN08, ISO11, KKM*10]: Data acquisition can be spoofed by dishonest subjects with counterfeits or masquerade modalities. Transmitted and stored data, for instance, biometric samples, features, even comparison scores, can be read, eavesdropped, manipulated or substituted. An attacker can use a Trojan horse to change important system parameters such as decision threshold or replay the data of an authorized subject. In [KKM*10], Kevenaar et al. defined that security of biometric systems is related to ingoing information and activities to illegitimately accept unauthorized subjects or to block authorized subjects and privacy is associated with outgoing information, which can be learned from systems. The security rests on the trustworthiness of the whole process.

In the ISO standard 24745 on “Security techniques - Biometric template” [ISO11], the security and privacy requirements on *overall* biometric systems are given to ensure biometric authentication: *Confidentiality* requires that data is only accessed by authorized entities and any disclosure or manipulation of data is not possible. *Integrity* ensures the completeness of data against any manipulation. *Availability* assures access and usage of authorized subjects. *Renewability* and *revocability* require diversification of biometric references. *Unlinkability* prevents link across databases of different applications with the help of biometric references. *Irreversibility* prevents retrieval of biometric information. *Data minimization* asks for minimizing stored information, which is irrelevant to authentication.

Different security countermeasures can be utilized in biometric systems, in order to meet these requirements. Liveness detection can stop sensor spoofing. Cryptographic techniques such as encryption, digital signature, access control, challenge and response are the powerful tools to guarantee confidentiality and integrity. Encryption with different keys is also helpful to prevent linkage attack. The importance of template protection techniques is to enable renewability and revocability, which is hard to achieve with other techniques. Biometric reference is unique to the underlying biometric modality. In cases that biometric references is compromised or related identities are expired, it is difficult or even impossible to revoke the reference and to reissue a new one. Therefore template protection is indispensable in biometric authentication. Additionally its constructions enable unlinkability. Meanwhile in most template protection algorithms private information related to users are reduced, which compliant with data minimization policy.

2.4. Summary

In this chapter the weaknesses of biometric systems with respects to security and privacy concerns were shown. These stimulate the research in biometric template protection, which aims at safeguarding biometric information and preventing potential attacks based on stored and transmitted data. An overview of the existing algorithms is given systematically. They can be classified into transformation-based approaches and biometric cryptosystems. Both of them can derive multiple unlinkable references from biometric data, which reveal no information about the original data. All these algorithms can be mapped into a general architecture defined by the ISO international standard. The difference of these algorithms in security characteristics and secure templates is shown. Furthermore, the important security and privacy requirements and possible countermeasures for biometric systems are given. Among different countermeasures, template protection is the only tool enabling renewability of stored reference data. Additionally it can improve other security and privacy properties such as unlinkability, irreversibility and data minimization.

The development of template protection demands the corresponding assessment of its security and privacy performance. Especially, comprehensive assessment of a real template protection is urgently required. In the next chapter we propose a generalized framework for security and privacy assessment, which can quantify different security and privacy requirements and enable empirical evaluation.

3. A Generalized Framework for Security and Privacy Assessment

The previous chapter showed that template protection is not only crucial for improving privacy and security, but also enables important functionalities such as renewing and revocation. As an indispensable supplementary to biometrics, template protection algorithms have been successfully integrated in different systems as shown in Section 2.2.1. The questions arise how secure these protected biometric systems are and how well security and privacy requirements are fulfilled. The existing analyses in the literatures either concern security and privacy performance from information-theoretical point of view, or focus on special attacks. Far fewer work defines the actual security and privacy goals and makes a systematic analysis involving threats and risks with reference to template protection systems. Even fewer work attempts to attach a numerical value to the these security and privacy properties. This chapter will address the main research problem of this thesis, namely:

> **How to give a comprehensive and systematic assessment on security and privacy of a real template protection system?**

We investigate the existing security and privacy analyses and propose a new generalized framework for security and privacy assessment. The important prerequisites are the protection goals and threat models. The first one covers the essential security and privacy requirements that template protection aims to achieve and the second one defines the capabilities and resources available to an adversary, which corresponds, for example, to accessible system parameters and available information during evaluation. We give the definitions of security and privacy, show how to define an evaluation process and finally demonstrate the framework on biometric cryptosystems, namely fuzzy commitment and fuzzy vault.

3.1. Related Work

Security and privacy analyses are very important to exhibit the advantage applying template protection. Since the very beginning of the development, the security of template protection, especially of biometric cryptosystems has been analysed from information-theoretical point of view. Biometric cryptosystems are secret-based methods and their security is easily compared with that of cryptography. Later, vulnerabilities of concrete algorithms have been found regarding to attacks from the practical side. In this section we give an overview of the existing analyses including theoretical analyses and special attacks. Before going to the details, we clarify the meaning of security and privacy for biometric applications: security relates to activities that an adversary manipulates or spoofs a verification process; privacy corresponds to information including biometric data and personal attribute thereof that an adversary can learn from systems.

3.1.1. Theoretical Analysis

Theoretical analyses are fundamental to successful development of template protection. It proves the feasibility of an abstract construction and is normally based on specific mathematical models. In such work security and privacy have been analysed and defined in a theoretical way. For instance, in [LT03] Linnartz and Tuyls introduced a new shielding function, where secrets are encoded in biometric data with a quantization method. The enrolment function G^{-1} produces a public information $W \in \mathcal{R}^{n2}$ from a random secret $S \in \{01\}^{n3}$ and biometric data $X \in \mathcal{R}^{n1}$ and the verification function can reproduce the secret S with W and biometric data Y, if Y is close to X. Here $n1, n2, n3$ are natural numbers. The shielding function should have the following three properties: *delta-contracting* requires that for all $X \in \mathcal{R}^{n1}$, at least one $W \in \mathcal{R}^{n2}$ and one $S \in \{0,1\}^{n3}$ exist such that $G(X,W) = G(Y,W) = S$, for all $Y \in \mathcal{R}^{n1}$ and $||X-Y|| \leq \delta$; *versatile* demands that for all $X \in \mathcal{R}^{n1}$ and $S \in \{01\}^{n3}$, at least one $W \in \mathcal{R}^{n2}$ exists such that $G(W,X) = S$; ε*-revealing* is defined for a δ-contracting function, if for all $X \in \mathcal{R}^{n1}$ a contracting vector W exists, such that the mutual information $I(W;S) < \varepsilon$. These are desired characteristics of a shielding function. "δ-contracting" indicates the robustness and also relates to recognition performance, "versatile" interprets universal of the function, that the construction works for all the possible input biometric features, and "ε-revealing" describes the small (or neglectable) leakage of S given W. The secret S, with can not be arbitrarily long, must be uniformly distributed.

In [TG04], Tuyls and Goseling showed the secrecy and identification capacity of the helper data scheme, which can be seen as a kind of fuzzy extractor. They modeled biometric features as independent identically distributed (i.i.d.) variables of length n. The reference and queried features are assumed to be randomly (and noisily) generated from the same source. The secrecy and identification capacity were calculated for the asymptotic cases, where n is sufficiently large. The secrecy capacity C_S is the maximum secret rate with small false reject rate (FRR) and neglectable small leakage of the secret, meanwhile, the identification capacity C_{id} is the maximum number of identifiable users normalised by feature length n with small average FRR. The construction is similar to the extraction of common randomness from correlated data with public information [AC93]. It is shown that the secrecy capacity is equal to the information rate between reference and queried features $I(X;Y)$. It is also proved that zero leakage of the secret (in an information-theoretically secure system) is achievable for uniformly and independently distributed biometric features. If a binary symmetric channel exists between X^n and Y^n with a cross over probability of p, then $C_S = 1 - h(p)$, where $h(p)$ is the binary entropy function. X^n and Y^n are the n bit long biometric features and $I(X;Y) = \lim_{n\to\infty} \frac{1}{n} I(X^n;Y^n)$. In [Ign09], Ignatenko also analysed the privacy leakage in this construction in term of the *mutual information* between the public helper data and biometric features. A trade-off between maximum secret key rate and privacy leakage was given.

In [DORS08], Dodis et al. proposed a $(\mathcal{M}, m, \tilde{m}, t)$- secure sketch and a $(\mathcal{M}, m, l, t, \varepsilon)$- fuzzy extractor for arbitrarily distributed biometric data X in space $\mathcal{M}$ with *min-entropy* $H_\infty(X) = m$. Secure sketch consists of a sketch function $SS(X) = W$ and a recover function $Rec(Y,W) = X$ for a distance function $dist(X,Y) \leq t$ with threshold t. Additionally if an adversary observes W, the probability that he can recover X, is not greater than $2^{\tilde{m}}$, namely the *average min-entropy* $\tilde{H}_\infty(X|W) = \tilde{m}$. *Entropy loss* is defined as $m - \tilde{m}$, which is necessary to compensate noise. Secure sketch targets precise reconstruction of a secret from noisy data, while fuzzy extractor focuses on generation of a reproducible key $S \in \{0,1\}^l$ from noisy data. It is important for a fuzzy extractor that S *is nearly uniformly distributed given* W, with $AD((S,W),(U_l,W)) < \varepsilon$, where AD is a *statistical distance* between two distributions and U_l is the uniform distribution in $\{0,1\}^l$. It was also shown that fuzzy extractor and secure sketch are strongly related. A fuzzy extractor can be derived from an existing secure sketch. Its key length l is also related to the secret size $\tilde{m}$ of the secure sketch that $l \leq \tilde{m} - \log(\frac{1}{\varepsilon}) + 2$. The factor $\log(\frac{1}{\varepsilon})$ describes the tolerance of the distribution of extracted keys to an ideal uniform distribution. In the secure sketch and fuzzy extractor, the security is determined by the average min-entropy and privacy leakage is declared by the min-entropy per definition. The statistical distance is used to measure uniformity and independency of extracted keys given W.

The existing theoretical analyses focus on biometric cryptosystems, since the security of transformation-based methods is normally based on the hardness problem. It shows possible metrics and concepts assessing security and privacy. However it is still unknown whether these metrics are suitable for empirical evaluation and how they can be measured in practice.

3.1.2. Possible Attacks on Template Protection

In addition to theoretical analysis, attack-based analysis exploits vulnerabilities of template protection and conducts concrete attacks on special algorithms. In this section a number of possible attacks are discussed.

FAR attack In biometrics, decision of a positive or negative response is made based on the similarity of compared features. Biometric data are random variables. Due to overlap between intraclass and interclass distributions, false acceptance and false rejection can occur. For example, assume that the probability of false acceptance (False Accept Rate *FAR*) of a biometric system is 0.01% at a given system setting. It means that two "identical" subjects can be found if, on average, 10^4 comparisons of features from different subjects are done. An adversary who owns or has access to a large biometric database can exploit the false acceptance properties.

Biometric modalities can be genotypical or/and phenotypical. Irises are phenotypical; Fingerprints are semi phenotypical; Faces are genotypic. People sharing the same genes as identical twins or 50% gene as parent and children have similar looks, however, this similarity can change over the time. A genetic disease can influence the genotypic modalities. For example, the patients of Down syndrome (trisomy 21) have similar faces such as hypoplastic nasal bone, flat nasal bridge. The similarity of different subjects especially for the genotypical characteristics is an inherent property of biometrics. The *FAR* attack for look-alike data subjects is feasible for all biometric systems and cannot be prevented by applying template protection.

Linkage attacks One of the advantages of using biometrics is the relative uniqueness of biometric features, which creates a direct connection between a subject and her/his identity. However, if the same biometric characteristic is utilized in different applications, similar or correlated identities of the same subjects are stored in different databases. This might lead to linkage of individuals over applications. One of the goals of template protection is to overcome this drawback and to enable generation of independent templates.

Biometric cryptosystems are suspected to be vulnerable to linkage attacks, since secure templates may contain information about biometric features. In the fuzzy vault approach, the true support points, which contain position of minutiae and the corresponding projection on a secret polynomial, are hidden in numerous chaff points. When an adversary has two references of the same subject from different databases, it is trivial to cover the true points by intersection of the two references [SB07]. It reduces the effort of an adversary to estimate the secret. Even worse when the secret is compromised, he can also generate valid support points with his own minutiae and insert them in the vault set. Then the manipulated reference works with the fingerprints of both the victim and the adversary. This kind of substitution is difficult to be detected, but it can be prevented with a digital signature. Nevertheless linkage attack is a serious problem for fuzzy vault.

In the fuzzy commitment scheme, the auxiliary data may contain subject-specific information. For instance, in [STP09], Simoens proposed an indistinguishability attack and irreversibility attack to exploit information leakage of biometric data in auxiliary data. The detailed description and further analysis of these two attacks will be shown in Section 3.4.2. In some implementations, length of binary features might be longer than allowed codeword length. Then the most reliable bits are selected and their positions are noted and stored. Since selection of the reliable bits lies on the statistical characteristics of an individual subject, it is likely to observe the correlation of stored data in different applications. An example of such an attack is demonstrated in Section 4.3.3.

Generally, transformation-based approaches have better resistance to linkage attack. In these algorithms, user- and application- specific transformation parameters are utilized, that increases the randomness of resulting secure templates. Only in [SB07], Scheirer et al. showed that it is possible to link the auxiliary data in biometric encryption systems using correlation of phase information. However no concrete simulation of the attack was given.

Hill climbing attacks Comparison scores in biometric systems reveal information on how similar the target template (stored reference) and the reference template (query) are. The information is helpful for an adversary to estimate enrolled images or templates with a recursive method [Adl04, Hil01].

The hill climbing attack is an optimization method to improve searching efficiency. For example, a facial image can be chosen at initialization. Different random modifications on the pixels in the image are done. The modified image, which has the best score to the target image, is selected. This process can be repeated until there is no significant improvement of the similarity. In other words, the similarity between the modified images and the target one can be increased iteratively with the help of comparison scores. As mentioned in [Adl05], "if biometric comparison releases information on partial match, then hill climbing is possible."

In biometric cryptosystems, comparisons are based on an exact match between a stored pseudonymous identifier and a live calculated one, which are normally hashes of random secrets. Only a hard decision can be made and no similarity score is available. A hill climbing attack is impossible. However, the transformation-based approaches rely on the similarity scores. For instance, in the biometric encryption method, the biometric samples are randomized by multiplying a random pattern and the original biometric information is still hidden in the randomized image. A quantized hill climbing can be used to attack it as shown in [Adl04]. Although no similarity score is directly available, a value, which is comparable with quantized scores, can be obtained with the help of the lookup table of the secret. In each iteration, modifications are not applied globally, but locally, so that the changes can cause sufficient improvements of the (quantized) similarity score. In [Adl04], an example of a quantized hill climbing is given for facial images. A small facial gallery is collected and eigenfaces of the images are calculated. An initial image is chosen and divided into 4 quadrants. Noise is added on a quadrant, meanwhile, the opposite quadrant is varied slightly in the eigenface space, so that similarity score increases at least by one quantized level. The experimental results show that a matchable similarity to the target image can be obtained with a randomly selected initial image. In cancelable biometrics, the comparison is also based on similarity. Theoretically, a hill climbing attack should be possible. However, its feasibility might be influenced by the non-invertible function used.

Feature estimation attacks A template protection algorithm might be insecure and an adversary can perform an efficient estimation method to retrieve biometric features. For instance, in [Bal08], Ballard proposed a biometric key generation system for signature recognition. He analysed a distribution of biometric features. The distribution information was used to crack the developed system by ranking possible features. *Guessing Distance* was utilized to measure the security. Guessing distance is originated from *guessing entropy*. Guessing entropy shows the average number of attempts needed to get an successful estimation by means of ordering the candidates in an descending order of probabilities, while the guessing distance determines the number of guesses needed for guessing a particular biometric data or secret key. Guessing distance of a feature is dependent on its position in the candidate list. It is shown that the successful rate of the first attempt is already at 15%.

3.2. A Generalized Evaluation Framework for Security and Privacy Assessment

The existing work analyses the security and privacy of biometric template protection from different aspects. However, only part of security and privacy requirements are addressed and analysis in a general level is still lacking. In the *secret-based* biometric crypto systems, correlated biometric data is observed and public information is shared between enrolment and verification. It is expected that a unique secret can be extracted and the public information reveals little information about the secret and biometric data. In the transformation-based approaches (using *secret auxiliary data*), enrolment and verification processes share the same secret supplementary data and can extract similar transformed features. It is hard to retrieve biometric data from transformed features.

In this section a generalized evaluation framework is proposed. Firstly the protection goals for template protection are determined, which are the evaluation criteria and indicate security and privacy aspects to be assessed. Secondly, the threat models are given, which define the information and resource available to an adversary. Finally, we will show how to conduct a rigorous evaluation based on a framework. In order to keep generalizability, the general construction of template protection according to ISO standard [ISO11] is used as shown in Section 2.2.2.

3.2.1. Threat Models

Template protection improves resistance of biometric systems against internal and external attacks. Before assessing security and privacy, identifying the information and computational resource available to an adversary is crucial. For example, secret size can be used to quantify the security of *PI* in fuzzy commitment systems. However, if biometric features are correlated and their distribution is known, leakage of the secret exists and the security of *PI* can be much smaller than the secret size. We define three main threat models as follows:

1. Naive Model: an adversary has neither information of the underlying algorithm in a template protection system, nor owns a large biometric database. He only has access to secure templates. The protected system is considered as a blackbox. Attacks that can be performed or biometric information that can be obtained are restricted.
2. Advanced Model: we assume Kerckhoffs' principle and an adversary has full knowledge of the underlying algorithm. Essential details of the algorithm are known. System internal parameters can be accessed and adjusted. Secure templates from one or more databases can be obtained. Additionally, we assume that an adversary also knows statistical properties of biometric features. It is very important priori information and can strongly influence security and privacy.
   If a system possesses a secret parameter, for example, transformation parameters in cancelable biometrics, and projection matrix in biohashing, its security relies on the secrecy of the secret parameter. Security can be assessed under assumption that an adversary has no access to secret information. We can also make stronger assumption that he can use the secret information but does not know it explicitly. Additionally in privacy assessment, we can assume that an adversary also knows the secret information in clear text. It is important to see whether leakage of biometric information exists, if secret information is compromised. In a secret-based system, there is no secret information. We assume that all system parameters are known to an adversary.
3. Collision Model: we assume that an adversary owns a large amount of biometric data. This allows him to gain enough information about biometric data. He can exploit inaccuracy of biometric systems, make an exhaustive search in his own database and find biometric data, which have sufficient similarity to that of a target person. If *FAR* is false acceptance rate of the system under a given setting, $1/FAR$ is the average number of biometric data from different users, which an adversary needs in his own database.

Naive and advanced models are comparable with the models in the cryptanalysis, which a cryptanalyst defines during assessment of cryptosystems. Naive model is the basic and weakest one. Advanced model is stricter, which can verify the security of a system against an experienced adversary. Collision model is derived based on inherent properties of biometric systems. It is possible to refine threat models or extend new requisitions according to security and privacy requirements on biometric systems. Threat models are prerequisites for quantifying security and privacy.

3.2.2. Protection Goals

Before starting an evaluation, it is necessary to clarify *what are the evaluation criteria*. In Section 2.2.2, the requirements on template protection are issued. From recognition point of view, integration of template protection should not affect accuracy of biometric systems. More important, template protection should achieve the one-wayness and randomness. With help of these indispensable properties, the desired security and privacy requirements such as renewability, revocability, confidentiality, unlinkability and data minimization can be fulfilled (see Section 2.3). The expected properties of template protection can be evaluated with the following protection goals, namely, security, privacy protection ability, unlinkability and randomness:

***Security of** PI* In a protected biometric system, an authentication result is based on the comparison of Pseudonymous Identifiers PI. The security of PI is determined by the hardness to find data M', which can produce a $PI' = PIR(M',AD,AD)$ and $PIC(PI',PI)$ gives a positive result. Additionally for the secret-based algorithms, the security of PI also includes the complexity to find a secret S', which is equal to the true secret S generated in enrolment process. This evaluation is comparable with the “pre-image” attack in cryptanalysis. S' equates to a pre-image of PI. The security of PI ensures trustworthiness of authentication.

Privacy Protection Ability One of the main motivations for applying template protection is to safeguard biometric information. The privacy protection ability includes two aspects:

- *Irreversibility of biometric data* indicates the hardness to retrieve the original biometric data. It is not always the same as that of PI. Data, which can pass PI-verification process, may not have enough similarity to the original biometric data. If a “pre-image” space of a PI is larger than its corresponding biometric data space, the system has better protection of biometric data. The security shows only expense to retrieve biometric data, however, it can not tell us the leakage of biometric data.
- *Privacy leakage* shows the amount of information about biometric data exposed in protected templates. In many template protection algorithms privacy leakage exists to compensate variation of biometric data as shown in [Smi04,Ign09]. Exposure of biometric information is not only threat for privacy but also a serious security shortcoming. It can be exploited to retrieve activities of a subject in other biometric applications. The revelation is permanent and hard to amend and can also influence the renewability of PI. Therefore, secure template $[PI,AD]$ should contain as little biometric information as possible.

Unlinkability One of the motivations to use template protection is to stop cross matching. Unlinkability is a crucial criterion. It also includes two parts:

- *Cross matching*: Assume that an adversary obtains two protected templates. It should be hard for him to verify whether they are generated from the same subject or not. However, cross matching can happen if secure templates contain “personal identifiable information”. For instance, AD is generated by PIE and required in PIR. If AD is not random and contains user-specific information, identification of a subject is feasible with AD. It is necessary to measure whether and how much personally identifiable information is contained in AD.
- *Leakage amplification*: Combing two or more protected templates should not be helpful to estimate secrets or to retrieve biometric features. Whether combination of several secure templates can increase privacy leakage and reduce security needs to be analysed. Leakage amplification limits long term applications and multiple uses of biometrics.

The protection goals substantiate the security and privacy requirements on template protection with consideration of empirical assessment. The security of PI is fundamental for the confidentiality of authentication with protected templates. The irreversibility of biometric data is an indispensable privacy protection property, since compromise of biometric data results in a hardly reparable loss of biometric identity. The privacy leakage is essential for data minimization and also has influence on the unlinkability. Both irreversibility and privacy leakage show the ability of an algorithm to safeguard biometric information. The cross matching shows unlinkability between different applications. Together with leakage amplification, it also determines renewability and revocability of protected templates. These protection goals are gaugeable with different metrics.

3.2.3. Evaluation Metrics

In the previous section we identified the protection goals of template protection and propose threat models for evaluation. In order to quantify protection goals, evaluation metrics are needed. In this section we show possible metrics and interpret their meaning for security and privacy and roles in evaluation. Furthermore, we give the definitions of security and privacy regarding computational complexity. The metrics used in the definitions have good measurability in practice. They are more general and can be used in evaluation of different algorithms.

Section 3.1.1 showed the metrics used in the existing security analysis. Many information-theoretical metrics and metrics used in cryptoanalysis are well suited for security and privacy assessment of template protection. Entropy, conditional entropy and mutual information are the common information-theoretical metrics. *Entropy* indicates how much information a random variable contains. It shows the discriminative power of an random variable. It is suitable for measurement in the naive threat model, where neither additional information is available nor other parameters and variables are taken into account. *Conditional entropy* is a power tool to quantify the security and irreversibility of biometric data in the advanced threat model. For instance $H(S|AD)$ shows the uncertainty about secret with known auxiliary data AD. *Mutual information* is an important metric to assess privacy leakage in advanced model, e.g. $I(X;AD)$ shows the common information in X and AD.

Min-entropy, average min-entropy, guessing entropy, conditional guessing entropy and statistical distance are the most frequently used metrics in security assessment of a cryptographic algorithm. They assess the security and privacy from different aspects. *Min-entropy* corresponds to the probability of the most frequently occurring element of a variable. It can measure irreversibility in advanced model without taking AD into account. *Average min-entropy* can also quantify both the security and irreversibility in advanced model. It corresponds to the probability of the most likely secret or biometric data given AD. *Guessing entropy* and *conditional entropy* measure the average number of attempts needed to retrieve target data with and without the help of AD. *Statistical distance* can measure the distance between two distributions. In the secret-based template protection methods, the secrets are expected to be random even if auxiliary data is given. The statistical distance can show the deviation of the secret distribution from an ideal uniform distribution.

Table 3.1 gives an overview of different metrics. The information-theoretical metrics quantify the protection goals with entropy and show average case performance. Min-entropy and average min-entropy show the lower bound of security and privacy achieved and correspond to the worst-case performance. Entropy loss measures privacy leakage in this case. Guessing entropy and conditional guessing entropy represent average complexity by retrieving secrets or biometric data in an attack scenario. In [NJ09], Nagar et al. proposed *coverage and effort*, which can also measure security and irreversibility in an attack scenario. Coverage is a recovering rate of a variable at a certain number of guesses (effort). It is a more detailed measurement than (conditional) guessing entropy. The statistical distance measures the randomness of extracted secrets with reference to an ideal uniform distribution. They can measure one or more protection goals in different threat models. Measurability shows whether these metrics are applicable in practice. The highly measurable metrics are already made use of in the assessment of concrete algorithms. The lowly measurable metrics are rather concepts and difficult to measure in practice.

Other metrics measuring recognition performance can also be used for security and privacy evaluation, especially for cross matching. Cross matching can be assessed with the recognition ability of protected templates. The False Match Rate (*FMR*), False Non-Match Rate (FNMR) and Equal Error Rate (*EER*) are proper met-

Metric	**Threat Model**	**Protection Goal**	**Measurability**	**Remarks**
Entropy	naive	security, $H(S)$	high	average case scenario
Conditional Entropy	advanced	security, $H(S\|AD)$ irreversibility, $H(X\|AD)$	medium	average case scenario
Mutual Information	advanced	privacy leakage, $I(X;AD)$	medium	average case scenario
Secrecy Capacity	all	security	low	proposed in [TG04] for a helper data scheme, boundary of achievable secret size and independent of adversary's resources
Identification Capacity	collision	security	low	proposed in [TG04] for a helper data scheme and boundary of rate of identified subjects
Min-Entropy	advanced	irreversibility, $H_\infty(X)$	medium	worst case scenario without taking *AD* into account
Average Min-entropy	advanced	security, $\tilde{H}_\infty(S\|W)$ irreversibility, $\tilde{H}_\infty(X\|W)$	medium	worst case scenario (see definition in [DORS08])
Entropy loss	advanced	privacy leakage $H_\infty(X) - \tilde{H}_\infty(X\|W)$	medium	worst case scenario (see definition in [DORS08])
Guessing Entropy	naive	security, $G(S)$	medium	attack scenario
Conditional Guessing Entropy	advanced	security, $G(S\|AD)$	medium	attack scenario
Conditional Guessing Distance	advanced	security	high	attack scenario (see definition in [Bal08])
Coverage and effort	all	security irreversibility	high	attack scenario (see also [NJ09])
Statistical Distance	advanced	security	low	randomness test with reference to a uniform distribution

Table 3.1.: Possible metrics for assessment of security and privacy protection ability

rics. In [STP09], indistinguishability is proposed, which measures the difference between the probabilities of successful guesses with secure templates and of totally random guesses.

Template protection has similarity to cryptography. There are two kinds of security in cryptographic systems, *conditional (computational) security* and *unconditional (information-theoretical) security*. Most of cryptographic methods such as RSA, public-key cryptography etc. are based on the assumption of hardness of computation problems. Their computational complexities are not really proved. The security is held only if an adversary owns limited computational resources. Unconditional security, also called perfect security, does not rely on any assumption of attack model. And the security can be held even if an adversary has unlimited computational power. In this case, an adversary can learn nothing about message from cipher text and can not perform an attack better than brute force. It is Shannon's definition of perfect secrecy. He also proved that the perfect secrecy requires one-time pad, which is, however, very impractical. The detailed elaborations on unconditional and conditional cryptographic security are given in [Wol98, Mau99].

Similarly security of biometric cryptosystems such as fuzzy commitment and fuzzy vault can be perfectly secure under certain requirements. In a perfect secure system, different security metrics become harmonized, for instance entropy, conditional entropy and conditional min-entropy converge. In contrast, the security of transformation-based algorithms is mainly based on the secrecy of transformation or randomization parameters. The privacy of these algorithms relies on inaccuracy of inversion functions, e.g. an inversion of a many-to-one function or a quantization function.

In practical applications, perfect security is not sufficient. For instance, in a perfectly secure fuzzy commitment system, secure templates expose no information about secrets. However, if the achieved secret size is too small, an adversary can use a brute force attack to retrieve the secret. Therefore computational security is more important for practical applications and a quantitative measurement is necessary.

Measuring computational security, computational powers and storage also need to be taken into account. For example, there are two biometric cryptosystems, one uses cryptographic hashing to protect a random secret of length 80, another one hides 20 secret data points in 100 random points. If brute force attack is used, the search space of the first system is 2^{80} uniformly distributed data and the one of the second system is $\binom{100}{20} \approx 2^{69}$ identically probable combinations. The larger the search space is, the more storage is necessary. Additionally, cryptographic hashing and hiding secret demand *different* computational power. Both of them should be considered. We propose formal definitions of security and privacy from computational security aspect.

A template protection algorithm consists of a pseudonymous identifier encoder PIE, $[PI, AD] = PIE(M)$, a pseudonymous identifier recorder PIR, $[PI'] = PIR(M', AD)$ and a pseudonymous identifier comparator PIC as defined in Section 2.2.2. M is an input biometric datum, the pseudonymous identifier PI and the auxiliary data AD are stored as a protected template. The *security and privacy* of template protection is defined as:

Definition 1. *Let $\mathcal{A}(AD, PI) = [\hat{M}, \hat{PI}]$ be a reconstruction function, where $\hat{PI} = PIR(\hat{M}, AD)$. $T_{\mathcal{A}}$ is the computational time required in one reconstruction attempt and n is the average number of reconstructions needed to get a $[\hat{M}, \hat{PI}]$, such that $PIC(PI, \hat{PI}) = 1$ for a positive authentication result. A template protection algorithm is $(\mathcal{T}, \varepsilon)$-* **secure***, if for all reconstruction functions $\mathcal{A}$,*

$$T_{\mathcal{A}} \geq \mathcal{T} \tag{3.1}$$

$$\log_2 n \geq \varepsilon \tag{3.2}$$

This security definition represents the average effort to find a biometric datum $\hat{M}$, which can successfully pass pseudonymous identifier verification process. It emphasizes computational security, however, it is also strongly related to information-theoretical security. To break verification, a reconstruction function $\mathcal{A}$ is necessary. It demands some computational power, which is quantified with computational time $T_{\mathcal{A}}$. It is the lower limit for all the possible reconstruction functions. The reconstruction function is tied up with PIE and PIR. For a well-designed template protection algorithm, PIE and PIR should be hard to invert (e.g. PIE and PIR are one-way functions). The reconstruction is possible, for instance, only with a kind of brute force using PIR and PIC functions. In some of transformation-based algorithms, inverse functions can exist and the inversion is possible, if transformation parameter (AD) is known. Inversion might be a one-to-many function. Only biometric data is protected, however, security can not be ensured if AD is compromised. The factor ε indicates the average number of guesses (reconstructions). It is dependent on the properties of the search space. In the case that inversion function exists, the search space can be very small and $\varepsilon = 1$. For the secret-based algorithm ε is related to the conditional guessing entropy $G(S|AD)$. In practice both ε and $\mathcal{T}$ should be large enough that an adversary can not find an $\hat{M}$ successfully in reasonable time.

Definition 2. *Let $\mathcal{A}(AD,PI) = [\hat{M},\hat{PI}]$ be a reconstruction function, where $\hat{PI} = PIR(\hat{M},AD)$. $T_{\mathcal{A}}$ is the computational time required in one reconstruction and n is the average number of reconstructions needed to get a $[\hat{M},\hat{PI}]$, such that for a threshold t distance function $dist(\hat{M},M) \leq t$. A template protection algorithm is $(\mathcal{T},\varepsilon,t)$-* ***preserving****, if for all reconstruction functions $\mathcal{A}$,*

$$T_{\mathcal{A}} \geq \mathcal{T} \tag{3.3}$$

$$\log_2 n \geq \varepsilon \tag{3.4}$$

This definition shows the cost to find $\hat{M}$, which is similar to M. Biometric data is random variable. It is not necessary to reconstruct the same M as in the enrolment. We use a distance function and a threshold to represent the desired accuracy of the reconstruction. Other privacy related information such as birthday, gender, name, might be saved in a protected biometric system. But we only take the input biometric data to be protected into account.

In the definitions, the average number of attempts is used as one of the evaluation metrics. Other information-theoretical metrics are also good metrics for the evaluation, however, they are not suitable for measurement of the transformation-based methods. The average number of attempts represents the computational security. The proposed definitions interpret the meaning of security and privacy from attack point of view.

3.2.4. A Generalized Evaluation Framework

In this section we will propose a generalised evaluation framework. It aims at providing a guideline, how to design an evaluation process for a template protection algorithm. In the following we show sequentially the process:

1. **Determining protection goals**: The first step is to clarify the objectives of the evaluation. They depend on what we want to achieve with a template protection method. The possible protection goals are the security, privacy protection ability, and unlinkability as elaborated in Section 3.2.2, which cover all the security and privacy expectations on template protection.

2. **Specifying threat models**: Furthermore, it is necessary to define the ability of an adversary, e.g. system information and computational resources available for him. It represents, which kinds of information and system parameters an adversary can access in a practical attack. On the other hand, the same information is also allowed to be used during the evaluation. We range the capability of an adversary into three threat models, namely, naive, advanced and collision model as described in Section 3.2.1. The higher the security requirements are, the stricter is the threat model and the more information and computational power is available for an adversary.

   Obviously the power of an adversary is strongly underestimated in the naive model. In a rigorous evaluation, we recommend that assessment should be done at least under the advanced threat model. If high security is required, additionally the evaluation should be performed in the collision model. Please note that evaluation in advanced and collision model cannot be substituted by each other. Collision, that biometric data of different subjects can be matched, arises from the overlap of biometric data from different subjects. It is an inherent problem of biometrics. It cannot be solved with template protection. However, applying template protection should not increase inaccuracy of systems. The advanced model characterizes the security and privacy regarding adversaries with other information source.

3. **Defining evaluation metrics and evaluation process**: Choosing appropriate metrics is the crucial step and is the core of an evaluation. An evaluation process is designed to measure the metrics. The identified protection goals and threat models determine which kinds of metrics can be used and how these metrics can be assessed. The possible metrics are shown in Section 3.2.3.

   Evaluation processes distinguish between theoretical evaluation and practical evaluation. Theoretical evaluation measures the information-theoretical metrics, average min-entropy, guessing entropy etc. These metrics require knowledge of distribution or conditional distribution of biometric data or secrets. However, the probability estimation is not always possible, e.g. due to high dimension of features, limited number of testing data. Additionally, information-theoretical metrics may not be suitable for the algorithms, which are not based on information-theoretical security. Alternatively, practical evaluation can be used, which depends on individual attack. It provides a direct way to evaluate an algorithm by assessing the efficiency of a defined attack.

   The theoretical evaluation shows the security and privacy in a systematic way. It can show basically whether an algorithm has potential vulnerabilities or not. However, it cannot show whether any attack on vulnerability is feasible in practice or not. In contrast, practical evaluation simulates what an adversary can really achieve. But it is strongly dependent on the attack. Therefore, the theoretical and practical evaluations complement each other. Their results will be also convergent. If a system is proved to be highly secure with theoretical evaluation, it will be well resistant to possible security attacks. Vice versa, if a system is found to be vulnerable to an attack, security weakness can be detected with theoretical evaluation.

4. **Evaluation and analysis**: After designing the evaluation process with the metrics, an evaluation can start. Depending on the threat model, testing material, e.g. a face database, can be required. In many attacks, adversaries may need data for initialization. Moreover, the statistical properties of biometric data can be learned from testing material. These are very essential input for assessment of concrete algorithms and are an important prior knowledge for an attack. At the end of the evaluation, the results with evaluation metrics are obtained and analyzed. If different metrics or evaluation methods are used, their experimental results need to be compared with each other. The whole evaluation from determination of protection goals to the analysis of evaluation results should be well documented.

Figure 3.1 illustrates the proposed evaluation framework. To sum up, the threat model and the protection goal should be determined before an assessment process starts. Based upon these, the metrics quantifying protection goals need to be determined. The experiments should be designed to give a substantial measurement on the developed metrics. The assessment is completed with the analysis of the results.

Template protection is a privacy and security enhancing technique. The security and privacy assessment is even more important than evaluation of recognition performance. This proposed framework enables an *empirical* evaluation. It meets the challenge of privacy and security assessment in practice. The framework is helpful during development of an algorithm, such that potential weaknesses can be avoided in advance. It can be specified for assessment of different algorithms. In the next two sections, we give an overview of the security and privacy in fuzzy commitment and fuzzy vault with consideration of this framework.

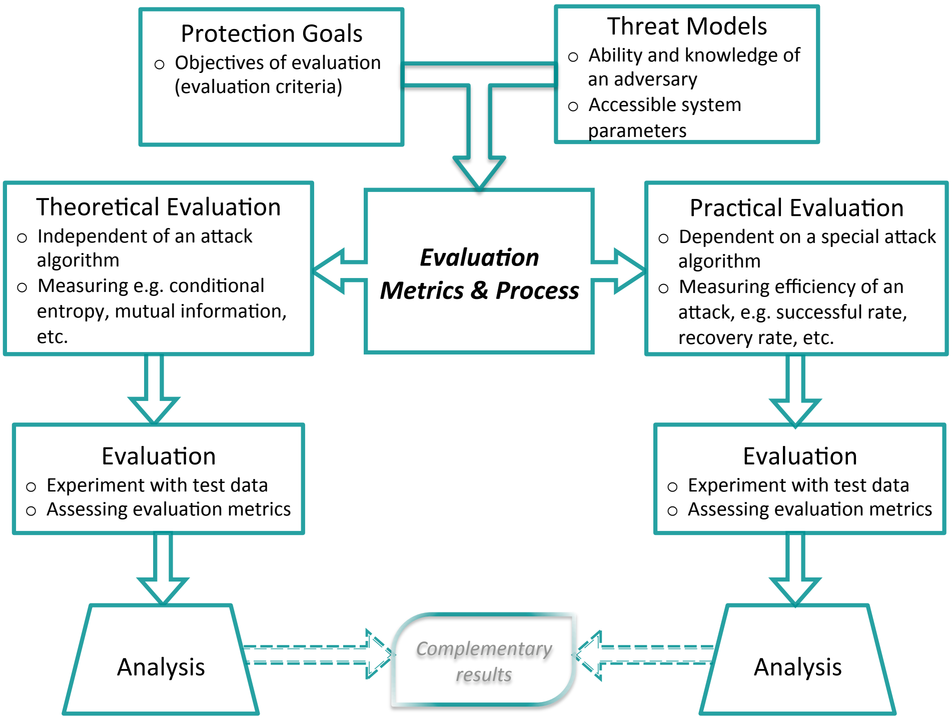

Protection Goals
○ Objectives of evaluation (evaluation criteria)
Threat Models
○ Ability and knowledge of an adversary
○ Accessible system parameters
Theoretical Evaluation
○ Independent of an attack algorithm
○ Measuring e.g. conditional entropy, mutual information, etc.
Evaluation Metrics & Process
Practical Evaluation
○ Dependent on a special attack algorithm
○ Measuring efficiency of an attack, e.g. successful rate, recovery rate, etc.
Evaluation
○ Experiment with test data
○ Assessing evaluation metrics
Evaluation
○ Experiment with test data
○ Assessing evaluation metrics
Analysis
Complementary results
Analysis

Figure 3.1.: The generalized evaluation framework

3.3. Importance of Distributions of Biometric Data

The probability distribution of biometric data plays a very important role in security and privacy assessment. For the security reason, we expect that secure references are random and prediction or linkage of them is infeasible. However, biometric data are stochastic variables. The inherent dependency exists, for instance, fingerprint images share the similar pattern. The *FAR* attacks and feature estimation attack shown in Section 3.1.2 are based on this property of biometric systems.

On the one hand, protected templates are generated from dependent biometric data. The risks exist that derived references contain user-specific information and template protection can be prone to linkage attacks. On the other hand, distribution of biometric data can help an adversary to retrieve the original biometric data from protected templates. Therefore, we define distribution as important priori information in advanced threat model.

In a rigorous assessment, estimation of distribution of biometric data is indispensable. Especially, in theoretical evaluation, distribution of biometric data is necessary. Unfortunately, in the existing security analyses, precise estimations were substituted with simple assumptions of e.g. independent and identical distribution [BCC*07, VDRY09], etc. That led to overestimation of security. We will show how to accurately estimate distributions of 3D face features and iris features in Sections 4.3.1 and 5.3.1, which allows strict quantification of security and privacy.

3.4. Assessment of the Fuzzy Commitment Scheme

The fuzzy commitment scheme is one of the most successful template protection algorithms. It was firstly proposed by Juels and Wattenberg in [JW99]. The main idea is to assign a random secret to a subject instead to use biometric data itself. Authentication is performed though the correct regeneration of the secret with a biometric datum and helper data. The helper data is useful to compensate errors between enrolled and queried biometric data. A block diagram is shown in Figure 3.2.

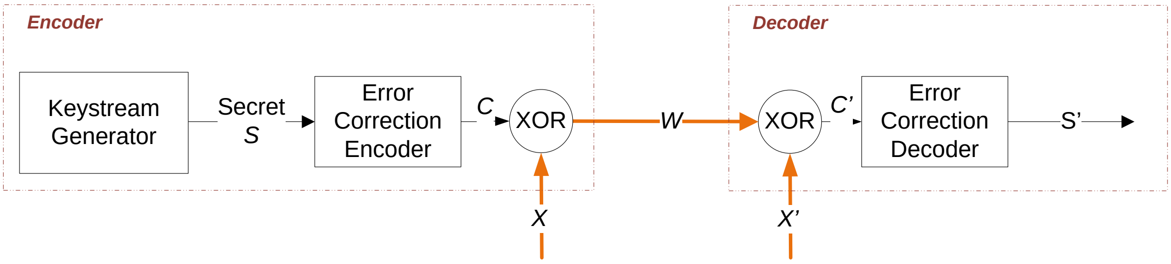


Figure 3.2.: A block diagram of fuzzy commitment

The encoder and the decoder of fuzzy commitment share a public side information W and the two correlated biometric feature X and X'. They try to extract exactly the same secret S. C is an error correction code of S and W is also called helper data, which should reveal neither information about S nor about X.

$$W = C \oplus X \tag{3.5}$$

Error correction coding is necessary, since biometric features are noisy data. It is simple to map fuzzy commitment into the ISO architecture (see Section 2.2.2). The *PIE* consists of a fuzzy commitment encoder and a hash function. A protected template is composed of $[PI, W]$, where $PI = h(S)$ and W is the auxiliary data according to the standard. The *PIR* is built with a fuzzy commitment decoder and a hash function. The decoder takes biometric feature X' and W as inputs and returns a hash of the estimated secret $h(S')$. The *PIC* makes an exact comparison of the stored *PI* and the new one.

Obviously fuzzy commitment is appreciate to protect binary features. The extracted biometric feature may not be binary. In such a case, binarization process is needed to convert features into binary string X. Here we only focus on privacy and secrecy performance regarding binary feature X. Information loss happening in binarization process will not be addressed in this work. In this section we investigate the existing theoretical security analysis of fuzzy commitment and give a systematic overview of security and privacy properties regarding different protection goals. Here we make an assumption of *advanced threat model* that an adversary knows the details of fuzzy commitment, e.g. coding algorithms, coding parameters etc.

3.4.1. Security and Privacy

Assume secret $S \in \{0,1\}^{L_S}$ and C is its codeword of length L ($L > L_S$). Binary biometric feature X also contains L bits. During enrolment process, S is randomly chosen and independent of X. The following equations are valid (the proof is given in section 4.2.2 of [Ign09]):

$$
\begin{aligned}
I(S;W) &= H(W) - H(W|S) = H(W) - H(C \oplus X|S) \\
&\overset{a}{=} H(W) - H(X) \qquad (3.6) \\
I(X;W) &= H(W) - H(W|X) = H(W) - H(C \oplus X|X) \\
&\overset{b}{=} H(W) - H(S) \qquad (3.7)
\end{aligned}
$$

the equality of a and b is valid, since X is independent of S and C. The mutual information $I(S;W)$ shows the *secrecy leakage* in auxiliary data W, while $I(S;W)$ represents the *privacy leakage*. The mutual information is non-negative, therefore, $H(W) \geq \max\{H(X), H(S)\}$.

Fuzzy commitment can be seen as a special case of helper data scheme and fuzzy extractor. The security and privacy performance of fuzzy commitment is well analyzed in literatures. In the following we summarize the important properties of fuzzy commitment:

- *The number of secret bits, which can be exacted with negligibly small secrecy leakage, is* ***not larger*** *than the mutual information between reference and queried biometric features $I(X;X')$.* It is the boundary of achievable secret size for a perfectly secure system with helper data scheme. In [Tuy04] Tuyls proved it for both discrete and continuous variables. In [Ign09] Ignatenko proved it for independently identically distributed variables and stationary ergodic variables.
- *If binary biometric feature X is uniformly and independently distributed (u.i.d.), namely any element x_i of X with $p(x_i = 1) = p(x_i = 0) = 0.5$, then fuzzy commitment is* ***perfectly secure***. Eq 3.6 shows that W exposes no information about secrets, only if $H(W) = H(X)$. It is trivial to prove that this condition holds, if X is u.i.d. In [JW99] Juels et al. show that retrieval of a secret is as hard as inversion of its hash. It is also proved from information-theoretical point of view in [Tuy04, Ign09].
- *If X is non-uniformly identical independently distributed, namely any element x_i of X with $p(x_i = 1) = p(x_i = 0) = p \neq 0.5$, where p is constant for all x_i,* ***secrecy leakage*** *exists.* For instance, Ignatenko proved the existence of the secrecy leakage in the case that X is identically independently distributed or is a non-uniform stationary ergodic sequence in [Ign09].
- *The irreversibility of biometric data is* ***equivalent*** *to security of PI.* $H(S|W)$ represents the *security* of *PI* and $H(X|W)$ indicates the *irreversibility* of X. With this construction, biometric feature X is as secure as S, since the uncertainty about X is equal to the uncertainty about S with known W:

  $$
  \begin{aligned}
  H(S|W) &= H(S) - I(S;W) \\
  &= H(S) + H(X) - H(W) \qquad (3.8) \\
  &= H(X|W) \qquad (3.9)
  \end{aligned}
  $$

  Obviously the security of biometric information relies on the security of S. As soon as S is compromised, X is also totally exposed.
- *Privacy leakage is* ***unavoidable*** *in fuzzy commitment.* The auxiliary data leaks information about enrolled biometric data in order to enable error tolerance. In a perfectly secure system, $I(X;W)$ is at least $H(X|Y)$ as proved in [Tuy04, Ign09]. In [Smi04], Smith also proved it for the secure sketch in a Hamming distance space with uniformly distributed bit errors. In practice this lower bound is hard to achieve and real privacy leakage is much higher.

  Fuzzy commitment exacts secrets from noisy data source. It is comparable with secret extraction from common randomness, where helper data – the information shared between enrolment and verification – is necessary for error compensation. In [Ign09], Ignatenko analyzed the achievable privacy performance with the helper data scheme. Fuzzy commitment can be seen as a special case of the helper data scheme, but it is *not* the only one construction. She showed that fuzzy commitment has extremely high privacy leakage in comparison with an ideal construction. And privacy leakage increases with the decreasing secrecy performance.

Fuzzy commitment is one of the very few methods, which can achieve information-theoretical security. However, its security and privacy performance is optimal with uniformly identically distributed features at the maximum secret size. Unfortunately, this strict condition is difficult to fulfill in practice. In many applications, dependency of biometric features is ignored and security is thus suspected to be highly overestimated. Therefore, a rigorous assessment is necessary and important.

The information-theoretical metrics shown in Table 3.1 can be used to quantify the security and privacy. Due to XOR operation, security and privacy are strongly related. To evaluate a fuzzy commitment system, a randomness test on input biometric features can be firstly performed. Different kinds of tests are shown in [RSN*08], which can verify whether features are u.i.d or not. If features are u.i.d, the security and privacy can be directly determined by the secret size and the codeword length. If not, the distribution of biometric features needs to be estimated.

These security and privacy metrics can only be measurable, if distribution of biometric features as well as condition distribution of secrets are known. It is a big challenge to estimate the distribution of high dimensional biometric features. In Chapter 4 and 5, we will show how to model the distribution of 3D facial features as well as iris features and give a rigorous estimation on the corresponding fuzzy commitment systems.

3.4.2. Unlinkability

Privacy leakage existing in fuzzy commitment can be misused by an adversary, especially when he has access to many secure templates. As shown in Section 3.2.2, there are two kinds of risks related to unlinkability of template protection, namely cross matching and leakage amplification. In principle, any personal identifiable information contained in stored template can cause these problems. In this section we take a close look at these two potential risks and their effects on fuzzy commitment.

In [STP09], two possible linkage attacks on fuzzy commitment were proposed. One is the *distinguishability attack*, also called decodability attack, which is a cross matching attack; the other is the *irreversibility attack*, which is a kind of leakage amplification attack. In [CS08, STP09, Kel10], decodability attack on fuzzy commitment has been addressed. Carter and Stoianov showed in [CS08] that fuzzy commitment is vulnerable to linkage attack due to error correction coding and XOR function. Simoens et al. gave a detailed analysis in [STP09] regarding indistinguishability. Indistinguishability is an important property of a public key encryption system. Based on a ciphertext, an adversary should have no advantage in guessing which key was used in encryption. Analogously, given two secure templates, an adversary should not be able to verify whether they are derived from the same subject or not. They defined indistinguishability and N-indistinguishability to assess this attack. A challenger randomly sends two secure templates to an adversary and denote $i = 1$, if they are from the same subject or $i = 0$, if they are from different subjects. In the basic indistinguishability test, the probabilities of $i = 1$ and $i = 0$ are equal; while in the N-indistinguishability, the probability of $i = 1$ is $1/N$, where N is the number of the subjects in the challenger's database. The adversary should guess whether the template sent is derived from the same subject or not. If linking secure templates is possible, the adversary can do better than a random guess.

In [STP09] indistinguishability and N-distinguishability are defined as:

$$Adv_{ind} = 2\left|P(i=\hat{i})-\frac{1}{2}\right| \tag{3.10}$$

$$Adv_{ind-N} = \frac{N}{N-1}\left|P(i=\hat{i})-\frac{1}{N-1}\right| \tag{3.11}$$

where $\hat{i} \in \{0,1\}$ is the adversary's estimation result. Adv_{ind} and Adv_{ind-N} measure the advantage of an adversary over a random guess.

Simoen et al. proposed the following practical attack on fuzzy commitment. The auxiliary data $W = X \oplus C$ is the distance between biometric feature X and a codeword C. The linear error correction code has the property that the sum of any two codewords is also a codeword. The sum of two auxiliary data is the distance between two enrolled biometric features plus a codeword. The intraclass distance is larger than the interclass distance on average. Additionally, the space of correctable codes is much smaller than the whole code space in many linear error correction codes. Therefore, with high probability the sum of two auxiliary data is decodable, if they are derived from the same subject; otherwise, the sum is probably undecodable. They showed a lower boundary of a $(\mathcal{M}, m, m', t)$- secure fuzzy sketch with uniformly independent features and uniformly distributed intraclass errors E with Adv_{ind}:

$$Adv_{ind} \geq 1-2^{-[I(X;W)-H(E)]} \tag{3.12}$$

where the Hamming distance of E is not larger than t. The zero-indistinguishability can only be achieved, if $I(X;W) = H(E)$. In this case, $L_S = H(X;Y)$ and the maximum secret size is achieved, where $H(X;Y)$ is the mutual information between the reference and queried features. However, they also prove that an optimal code enabling zero-indistinguishability does not exist in practice. Although the lower bound of indistinguishability given by Simoen is derived from uniformly independent features, the distinguishability attack is general and is applicable in many fuzzy commitment schemes.

Kelkboom analyzed the performance of the decodability attack and evaluated it in a fingerprint fuzzy commitment system [Kel10]. For uniform and independent biometric features, he showed that *FAR* of the decodability attack is 2^{L_S} larger than the *FAR* of the original fuzzy commitment system. In the fuzzy commitment scheme, a false acceptance happens only if a feature of another subject falls into the sphere of the reference feature within a radius t, where t is the number of correctable bit errors. However, in the decodability attack, there are 2^{L_S} spheres, which can cause false acceptances. The difference between their centers and the original reference feature is equal to a codeword. In contrast, *FRR* becomes smaller, since decodable feature space enlarges. He also proposed a bit-permutation process to improve the resistance to the decodability attack. Before calculating the XOR of the chosen codeword and the biometric feature, a permutation function Π is used to shuffle bit position of biometric feature. The following equations are used to describe different enrolment processes:

$$\begin{aligned} \Pi_1(X_1) + S_1 \cdot G &= W_1 \\ \Pi_2(X_2) + S_2 \cdot G &= W_2 \end{aligned}$$

where G is a generator matrix of an error correction coding method. After permutation the intraclass distance of biometric features increases so much that decoding the sum of auxiliary data is not possible any more. The parameter of permutation is an additional auxiliary data and is independent of secrets and biometric features.

The second attack, reversibility attack, is also proposed by Simoen in [STP09]. He showed that linking different secure templates can lead to more leakage. Due to different coding method used in fuzzy commitment, secure templates may contain different information about biometric features and combining them can gain more information about biometric features as well as secrets. This reduces *irreversibility* of secure templates. Assuming that X_1 and X_2 are the reference features of a subject in different applications; $W_1 = X_1 + S_1 \cdot G_1$ and

$W_2 = X_2 + S_2 \cdot G_2$ are their auxiliary data, where S_1 and S_2 are the secrets and G_1 and G_2 are the two different generator matrixes. $E_{intra} = X_1 + X_2$ is an intraclass distance. According to the paper of Simoens,

$$
\begin{aligned}
S_1 \cdot G_1 + S_2 \cdot G_2 &= W_1 + W_2 + E_{intra} \\
[S_1, S_2] \cdot \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} &= W_1 + W_2 + E_{intra} \qquad (3.13)
\end{aligned}
$$

In this equation, S_1, S_2 and E_{intra} are unknown. Let $R_{1,2} = Rank\left\{ \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \right\}$ be the rank of the new concatenated matrix and $\max\{L_{S_1}, L_{S_2}\} \leq R_{1,2} \leq \min\{L_{S_1} + L_{S_2}, L\}$. Especially when $R_{1,2} = L_{S_1} + L_{S_2}$, the cost to retrieve S_1 and S_2 reduces to that of guessing E_{intra}. In contrast, he showed that zero-irreversibility can be achieved, if $R_{1,2} = \max\{L_{S_1}, L_{S_2}\}$ and no additional leakage exists.

The indistinguishability (decodability) attack links the secure templates through privacy leakage contained in auxiliary data. It is feasible, if the two pseudonymous identifier encoders use the same coding method. And ω_1 indicates the case that W_1 and W_2 are from the same subject and ω_0 is for the case that W_1 and W_2 are from different subjects. Generally, a fuzzy commitment system is vulnerable to cross matching, if $I(W_1, W_2|\omega_1) > I(W_1, W_2|\omega_0)$. Eq 3.12 gives the condition for a perfect system, which is resistant to cross matching. And the mutual information between W_1 and X_1 is equal to the entropy of the noise, which is the difference between X_1 and X_2. No additional leakage exist. In this case, linking W_1 and W_2 is impossible.

The irreversibility attack combines privacy leakage in different secure templates of the same subjects and tries to gain more information. It addresses the second linkage problem - leakage amplification as shown in Section 3.2.2. It happens, when $I(X_1; W_2|W_1) > 0$. Using different error correction codes can increase the risk of leakage amplification. We propose an attack based on exhaustive searches: Given W_1, the XOR of W_1 and any codeword is a candidate of X_1. The set $\{\hat{X}_1\}$ and $\{\hat{X}_2\}$ contain all the candidates of X_1 and X_2. If the exactly same linear coding method is used, then one candidate set is the linear translated set of the other. If different coding methods are used, two sets are very different and the candidate pairs with the small distance may be two enrolled features. This method is more efficient than the irreversibility attack, since it is not necessary to try all the possible error patterns. However, it obviously requires a large memory and may be very impractical. An adversary can benefit from irreversibility attack, if $L_{S_1} + L_{S_2} - R_{1,2} + H(E_{intra}) < \min\{L_{S_1}, L_{S_2}\}$. For instance, if the secret size is much smaller than the number of correctable bit errors, it is not necessary to use irreversibility attack.

It should be avoided to change the coding scheme from privacy amplification point of view. The bit- permutation process proposed in [Kel10] can enhance indistinguishability, however, it can also cause high privacy amplification. If the permutation function Π is known, its unique inverse function Π^{-1} can be calculated and $X = \Pi^{-1}(\Pi(X))$, then:

$$
\begin{aligned}
\Pi_1^{-1}(\Pi_1(X_1) + S_1 \cdot G) &= \Pi_1^{-1}(W_1) \\
X_1 + S_1 \cdot \Pi_1^{-1}(G) &= \Pi_1^{-1}(W_1) \qquad (3.14) \\
X_2 + S_2 \cdot \Pi_2^{-1}(G) &= \Pi_2^{-1}(W_2) \qquad (3.15) \\
(X_1 + X_2) + [S_1, S_2] \cdot \begin{bmatrix} \Pi_1^{-1}(G) \\ \Pi_2^{-1}(G) \end{bmatrix} &= \Pi_1^{-1}(W_1) + \Pi_2^{-1}(W_2) \qquad (3.16) \\
(X_1 + X_2) + [S_1, S_2] \cdot \mathcal{G} &= \Pi_1^{-1}(W_1) + \Pi_2^{-1}(W_2) \qquad (3.17)
\end{aligned}
$$

Assuming that $G = [\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_n]$, $(u_1^1, u_2^1, \cdots, u_n^1)$ and $(u_1^2, u_2^2, \cdots, u_n^2)$ are the new indexes of $\mathbf{g}_i$ after the permutation function Π_1^{-1} and Π_2^{-1}:

$$\mathcal{G} = \begin{bmatrix} \mathbf{g}_{u_1^1} & \mathbf{g}_{u_2^1} & \cdots & \mathbf{g}_{u_n^1} \\ \mathbf{g}_{u_1^2} & \mathbf{g}_{u_2^2} & \cdots & \mathbf{g}_{u_n^2} \end{bmatrix} \tag{3.18}$$

$$n \geq \min\{n, 2k\} \geq \; Rank(\mathcal{G}) \; \geq Rank(G) = k \tag{3.19}$$

$\mathcal{G}$ is a $2k \times n$ matrix. After permutation the rank of $\mathcal{G}$ can be much larger than k. Combining W_1 and W_2 will expose more information about the secrets. In order to avoid this, the permutation functions should be kept secret.

Linkage attacks require knowledge about template protection systems. They can only be performed with experienced adversaries. To assess unlinkability, it is reasonable to assume the *advanced threat model*. In a cross matching attack, an adversary needs to have access of two protected templates. Additionally he should have access to two templates from the same subjects to perform a leakage amplification attack. It means that leakage amplification demands more information from a system than cross matching. Due to intraclass noise, attacks of leakage amplification are very impractical. Therefore, resistance against cross matching has higher priority than against leakage amplification in practice.

Nevertheless, leakage amplification determines diversity, renewability and revocability of template protection. In the worst case an adversary can learn information from revoked templates and biometric information can be totally compromised. Although leakage amplification cannot be realized with practical attacks yet, it is a potential weakness of fuzzy commitment.

Unlinkability is strongly related with practical attacks. Practical evaluation based on different attacks is proper for assessment. The metrics such as *FAR*, *FRR* can be used to quantify the efficiency of cross matching attack, while the metrics such as coverage and effort are the proper ones.

Both cross matching and leakage amplification are caused by privacy leakage. A system designer should try to minimize privacy leakage. Additionally any user-specific information such as name, gender, and age contain privacy information and is suspicious of linkage problems. Therefore, the stored templates and all related records need to be examined.

3.5. Assessment of the Fuzzy Vault Algorithm

The fuzzy vault algorithm is also a kind of fuzzy extractor for features in set difference space. In this section, we will elaborate the fuzzy vault algorithm and the existing security analysis. We will analyze its security and privacy performance based on the evaluation framework. Here we also assume the advanced threat model.

The fuzzy vault algorithm was firstly proposed by Juels and Sudan in [JS02] in order to protect fingerprint minutiae. Minutiae are characteristic points of a fingerprint, which are end or bifurcates of ridge lines. They are chosen as standardized fingerprint features in the ISO international standard. They are stored as a set of points and their comparison must be tolerant to reordering, deletions and insertions of minutiae in the feature set. Therefore, Shamir's secret sharing is exploited in fuzzy vault.

It works as follows: In the enrolment a randomly generated secret forms a polynomial *poly* of degree $\kappa - 1$. A minutia feature α_i is projected on the polynomial and a genuine point $\{\alpha_i, \beta_i\}$ is obtained, where α_i can contain position and angle information of the minutia and $\beta_i = poly(\alpha_i)$. Then t minutiae are used to produce the genuine points and $t > \kappa$. In order to protect minutiae information, the genuine points are hidden into r chaff points, which do not lie on p. Only the hash of the secret and the vault set consisting of both genuine points and chaff points are stored in a secure template. In the verification, if the genuine fingerprint is available and κ matched genuine points are found in the stored vault set, then the polynomial can be successfully reconstructed and the correct secret can be released.

In [JS02], the Peterson-Berlekamp-Massey algorithm - a classical RS decoding algorithm - is chosen for the polynomial reconstruction and the polynomial can be reconstructed with at least $\frac{t+k}{2}$ genuine points. The security of the algorithm is calculated by counting the number of possible polynomials of degree less than $\kappa-1$, which includes exact t points of the vault set. It is shown that at least $\frac{\mu}{3}q^{k-t}(r/t)^t$ such kinds of polynomials exist, where $q=r+t$ and μ is a probability factor. If an adversary owns δt genuine points, the probability that he can crack fuzzy vault is not larger than $2\sqrt{\frac{1}{3}q^{k-(1+\delta)t}(r/t)^{(1-\delta)t}}$.

In [NJP07], Nandakumar et al. showed an implementation of fuzzy vault. During minutiae extraction in the enrolment, local image quality is estimated. Based on this the most reliable minutiae are selected to calculate genuine points. Additionally, cyclic redundancy check (CRC) code is applied on the secret before it forms the polynomial, which makes it easier to check the correctness of the secret. The high curvature points on the fingerprint is also stored and used as reference points for fingerprint alignment. High curvature points detection is much more reliable than singular point (cores and delta) detection, since singular points do not exist on all fingerprints. They can not reveal much information about minutiae points. In the verification, only minutiae with high quality extracted from a query image are used in the further steps. The queried minutiae points are aligned based on the stored high curvature points and those detected on the queried image with the iterative closest point (ICP) algorithm. A candidate point is selected in a vault set if it is close to a minutia in the queried set. The polynomial is reconstructed with Lagrange interpolation, if more than κ candidate points are found. However, Lagrange interpolation is not tolerant to selection errors. The possible subsets of size κ from the candidate points need to be tried until the genuine set is found. A large number of candidate points need many reconstructions. Therefore, an additional coarse filter is used to filter wrongly detected genuine points, when the number of the candidate points is beyond a threshold.

They analysed the security of this implementation based on the complexity to reconstruct the polynomial. A successful reconstruction requires κ genuine points. A vault set contains $t+r$ points. They assume that chaff points and genuine points are similarly distributed and an adversary can not distinct genuine points from the chaff points. There are $\binom{t+r}{\kappa}$ different κ-combinations from the vault set. From those, $\binom{t}{\kappa}$ combinations contains the κ genuine points, which can successfully reconstruct the polynomial. Then, the average number of reconstructions required to retrieve the polynomial is:

$$n=\frac{\binom{t+r}{\kappa}}{\binom{t}{\kappa}} \tag{3.20}$$

Assessing fuzzy vault also requires the corresponding threat models. Here we assume the *advanced model*. Obviously Eq 3.20 measures the security of *PI* in the advanced model with knowledge of system parameters of t, r and κ. All the genuine points lie on the polynomial. Minutiae information will be totally compromised if the secret (the polynomial) is known. Therefore, the irreversibility of minutiae is equivalent to the security of *PI*. Those minutiae, which are not chosen in the enrolment, are safe. Assume that there are M possible minutiae positions in a fingerprint image with a fix resolution and u possible orientations at each position. The uncertainty of t minutiae is $\log(u\cdot\binom{M}{t})$. The privacy leakage can be calculated as follows:

$$\begin{aligned}\log(u\cdot\binom{M}{t})-\log n &= \log(u\cdot\binom{M}{t})-\log\frac{\binom{t+r}{\kappa}}{\binom{t}{\kappa}}\\ &= \log u+\log\binom{M}{t}+\log\binom{t}{\kappa}-\log\binom{t+r}{\kappa}\end{aligned} \tag{3.21}$$

Please note that both Eq 3.20 and 3.21 are based on the assumption that the minutiae are uniformly distributed in the feature space and all the t- or κ-combinations are possible minutiae set. It is not really true: minutiae distribution is not uniform and some finger regions have high minutiae density; minutiae in a fingerprint are correlated e.g. due to the orientation information. These equations may overestimate the security and privacy. Therefore, we recommend using additional practical evaluations in practice.

Although fuzzy vault is appropriate to handle the set difference metric, a disadvantage is that the protected information is only hidden in a vault set and it is susceptible to linkage attack and substitution attack [SB07]. An adversary who has access to two vault sets of the same subject, it is trivial to uncover the genuine points in the clouds of chaff points. The genuine points are present in both vaults, while the (independently generated) chaff points are different. Additionally, an adversary can generate valid support points with his own minutiae information and add them to the vault set, such that the verification process works for both the genuine user and the adversary. This substitution attack can be easily prevented with digital signature. Obviously, linkage attack also strengthens privacy leakage, that can not be stopped by digital signature. Therefore, researchers try to use additional information and to circumvent this drawback. For instance, Nandakumar et al. also proposed the approach of hardening fingerprint fuzzy vault using password to prevent the linkage attack in [NNJ07] .

Due to noise between acquisitions, the selected genuine minutiae points may be different. The inserted chaff points may disturb the matching process. The performance detecting overlapped genuine minutiae in two vault sets might be much worse than the performance of fuzzy vault. If fingerprint alignment information is used as in [NJP07], it is helpful for an adversary to retrieve the genuine points. The resistance of cross matching can be very different. It is also based on the efficiency of adversary's minutiae matchers. Cross matching can be assessed with the performance of corresponding attacks.

3.6. Summary

In this chapter we proposed a generalized evaluation framework, which enables a comprehensive assessment of template protection. It consists of the fundamental steps of an assessment, namely identifying protection goals and threat models, deriving evaluation metrics and designing evaluation process. Three main protection goals – security of *PI*, privacy protection ability and unlinkability – were defined, which cover all the requirements on template protection. Threat models were given, which are necessary to specify adversary's ability and set the evaluation environment. Based on these, the metrics and the corresponding evaluation process can be developed.

I emphasized the importance of distributions of biometric features in the assessment. The inherent dependency exists in biometric data. An adversary can exploit this priori information to crack a template protection algorithm. Additionally, security of many algorithms is based on the independency of biometric data. It is necessary to check whether such a prerequisite is fulfilled in practice or not. Therefore, analysis of distribution of biometric data is indispensable in a rigorous assessment.

We compare computational security and unconditional security and explain their roles in the assessment of template protection. Moreover, we give the general definitions of security and privacy regarding the computational security, namely the complexity to invert pseudonymous identifier and to retrieve biometric data. Furthermore, different metrics measuring protection goals are elaborated with respect to their security meanings and the corresponding threat models.

Additionally, the framework was also applied on two important biometric cryptosystems, fuzzy commitment and fuzzy vault. Here the advanced threat model was assumed. The existing analyses were summarized, which show the assessment of different protection goals. These analyses are based on special assumptions of distributions of biometric features or intraclass errors. The security and privacy properties were shown only in a theoretical way. In the following two chapters, we will evaluate two real fuzzy commitment systems based on the advanced threat model, estimate distributions of biometric features and quantify different protection goals. In Chapter 6 we will discuss the generalizability of the framework and use it as a basis to compare different algorithms.

4. Evaluation of Template Protection for 3D Face Recognition

In the previous chapter we proposed a generalized framework for privacy and security assessment of template protection. In this chapter we apply the framework on a template protection system for 3D face recognition and give a rigorous assessment. Firstly, we develop our own histogram-based 3D face recognition algorithm. Compact and robust feature vectors can be derived. They represent the distribution of the facial surface. A good recognition performance is shown. Fuzzy commitment is integrated to protect 3D facial features. The protected system has slightly performance degradation, but a high secret length is achieved. Secondly, we evaluate the security and privacy of the developed protected system. Here we assume the advanced threat model: an adversary has full information about the system and biometric features. We analyze the distribution of the features, which has strong influence on the security and is important priori knowledge for an adversary. The information-theoretical metrics are used to quantify the security and privacy protection ability. Unfortunately, 3D facial features are dependent and the security and privacy performance is quite poor. Additionally, we evaluate the unlinkability of the system. Secure templates contain personal identifiable information and cross matching using auxiliary data is possible. The system is also vulnerable to leakage amplification. Finally, we summarize the results and experiences obtained during the evaluation. The assessment based on the evaluation framework detects the potential risks and weakness of the developed fuzzy commitment system. It helps us design better systems.

4.1. 3D Face Recognition

The face is an important biometric modality. Face perception is a natural and easy way for humans to recognize a person. Therefore, face recognition is utilized in a broad range of applications such as border control, access control and surveillance scenarios. Face information can be represented as e.g. 2D color images, infrared images or 3D shapes. 2D face recognition systems rely on intensity values of images and extract significant features from a face. They have been an active research area for more than three decades. One of the most influential 2D face recognition algorithms is the Eigenface approach of Turk and Pentland [TP91] using the Principal Component Analysis (PCA) [MP01]. Von der Malsburg et al. introduced the Gabor Wavelets [LVB*93]. Lu et al. [LPV03] proposed fisher faces based on the Linear Discriminate Analysis (LDA), and the Independent Component Analysis (ICA) is used by Liu et al. [LWC99]. Today, mature 2D recognition systems are available that achieve low error rates in controlled environments [PSO*07]. However, face recognition based on 2D images is sensitive to illumination, pose variation and facial expressions. Moreover, a facial photo is easy to acquire even without consent of a person and may be used to spoof a 2D face recognition system.

In contrast to 2D face recognition, 3D face recognition relies on the geometry of the face. Due to this fundamental difference, it has the potential to overcome the shortcomings of 2D approaches. The 3D geometry of the face is inherently robust to varying lighting conditions [1]. A combined 2D-3D face recognition system may use

[1] Nevertheless, the 3D acquisition system itself can be sensitive to varying lighting conditions, especially to strong ambiance light.

the spatial information to compensate pose changes and can make 2D recognition more accurate. Modeling and faking the geometry of a face is much more expensive and complicated than in 2D scenario.

Different approaches for 3D face recognition have been published in the past. The Eigenface method for 2D face recognition was extended to an Eigensurface approach by Heseltine et al. [HPA04]. Bai et al. proposed to use the LDA for a 3D system by replacing the luminance values with depth information [BYS05]. An algorithm combining Eigenfaces and Hidden Markov Models was introduced by Achermann et al. [AJB97]. Morphing of face models has also been investigated by Huang et al. [HHB03] and Blanz et al. [BV99] to handle pose and illumination changes. As shown, feature extraction methods were in many cases carried forward from 2D into 3D. In the following we propose a novel 3D face recognition algorithm using facial surface information.

4.1.1. A Histogram-based 3D Face Recognition

3D face recognition consists of the normalization, feature extraction and comparison process. The normalization transforms a face model into a frontal view in order to compensate pose variations during acquirement. I use a recursive normalization method as shown in [ZSBF08]. With help of an orthographic projection matrix, a 3D facial point cloud is converted into a range image[2]. The most important landmark for 3D face recognition is the nose[3]. It can be detected by finding maximum length convex hull segments for each horizontal line in the range image. The intersection points for two maximum length segments are calculated. The bridge orientation is estimated by applying PCA to the intersection points. The facial image is rendered according to the alignment of the bridge position. The process is repeated until the translation and rotation required are below a given threshold or convergence stops.

This normalization method is able to transform any face dataset, which has a sufficient representation of the nose region, into a common reference orientation. It allows further processing towards a comparison of different datasets. After the normalization, the nose tip is at the origin of the Cartesian coordinate system. The face is vertical symmetric to the $y-z$ plane and the noise bridge has an angle of 30° to the y-axis.

The transformed face dataset resulting from the normalization stage is used as input to the feature extraction process. Since a frontal view on the face model is obtained, a straightforward approach is to compare the normalized 3D model using an appropriate distance metric for surfaces such as the Hausdorff distance as proposed by Pan et al. [PW03, PWWL03]. The downside of this immediate comparison is the poor robustness regarding normalization inaccuracies and the necessity to store complete 3D models as biometric references, which might need storage of several megabytes for an individual face. Here, we present an efficient histogram-based method to extract a compact feature set from the face surface.

The distribution of depth values of a normalized face model can efficiently describe the characteristics of an individual facial surface. In order to obtain more detailed information about the local geometry, the 3D model is divided into N horizontal stripes, which are orthogonal to the symmetry plane of the face. The features are extracted from the depth value distribution in each sub area. In the following, we elaborate the training process to detect the facial region and the feature extraction algorithm.

Before starting the feature extraction, a region of interest within the 3D model must be identified, which includes the bulk of the points belonging to the face surface. We assume p_i with $[x_i, y_i, z_i]$ is a point in the 3D model, where z_i indicates the depth value. The tip of the nose corresponds to the origin of the coordinate system at $[0,0,0]$. Around the tip of the nose a rectangle with $[X_{min}, X_{max}]$ and $[Y_{min}, Y_{max}]$ is defined as the bounding box for the x- and y-value as shown in Figure 4.1. The points describing the background or clothes are located outside

[2] A range image is similar to a 2D image. Instead of illumination, depth information is given to each pixel.

[3] The most important landmark for 2D face recognition is eye positioned. However, fine structure of eye regions and disturbing of eyelashes, etc., make acquired 3D information in those regions very noisy. In contrast, the acquisition and detection of the nose are very reliable.

of this region. Nevertheless, there are still points, which do not belong to the face surface like the points in the lower left and right corner of the rectangle in Figure 4.1, or spikes in the data set. A depth range for the points in the rectangle can be further applied to filter out the non-facial and mismeasured points. A simple statistical test is applied to the points in each sub area to find possible maximum and minimum depth values for facial points, where a number of normalized 3D models from different subjects are required. The experiment of the training process is shown in Section 4.1.2.

After the training process, the face region is determined. Figure 4.2 shows an example of the selected face region. Then, the selected facial region is further divided into N disjoint horizontal stripes (see Figure 4.3). The facial points of stripe S_n are defined as:

$$S_n = \{p_i(x_i, y_i, z_i) | x_i \in [X_{min}, X_{max}], y_i \in [Y_{n,min}, Y_{n,max}], z_i \in [Z_{n,min}, Z_{n,max}]\} \tag{4.1}$$

where $n \in [1, \cdots, N]$. The y-range $[Y_{n,min}, Y_{n,max}]$ and the depth range $[Z_{n,min}, Z_{n,max}]$ depend on the specific sub area under consideration.

Given the bins $\{Z_{n,0}, Z_{n,1} \cdots, Z_{n,K}\}$, where $Z_{n,0} = Z_{n,min}$, $Z_{n,K} = Z_{n,max}$, the percentage of the subset of points in S_n with in the range $[Z_{k-1}, Z_k]$ is given by

$$v_{k,n} = \frac{||\{p_i(x_i, y_i, z_i) | p_i \in S_n, Z_{k-1} < z_i < Z_k\}||}{||S_n||} \tag{4.2}$$

where $||\cdot||$ denotes the number of points and $k \in [1, \cdots, K]$ and $n \in [1, \cdots, N]$.

By counting the points in each depth range, a feature vector with K elements for each stripe S_n is obtained. The feature vector corresponds to the histogram of the stripe with respect to the bins given above. Figure 4.3 shows the division of the face area in several uniform horizontal stripes. The resulting feature is depicted in Figure 4.4. The feature of every stripe is represented as a row in the image and the color indicates the percentage of the number of points within the stripe falling into the respective bins.

The proposed algorithm adopts a simple statistical analysis to describe the geometrical characteristics of a facial surface. Hetzel et al. [HLLS01] used a similar method to recognize different 3D objects. In my algo-

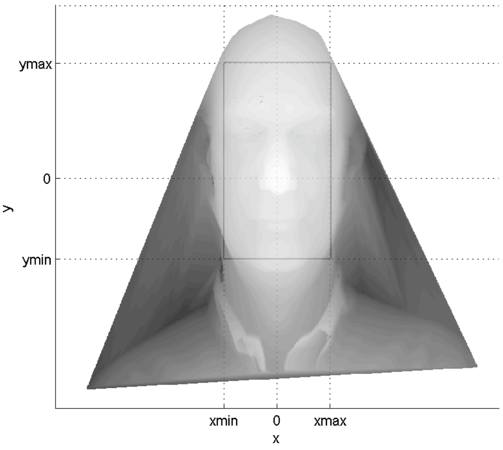


Figure 4.1.: Selecting the face region in the x-y view

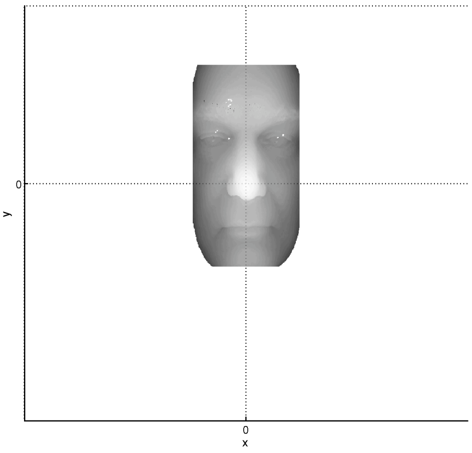


Figure 4.2.: Selected face region in the x-y view

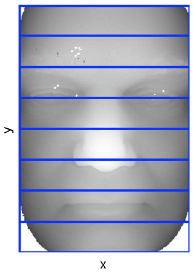


Figure 4.3.: Stripes division of the facial points in x-y view

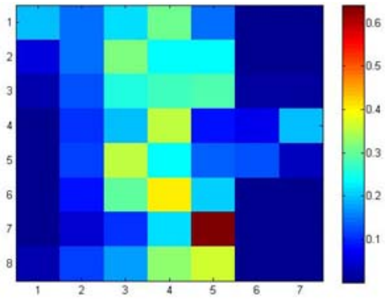


Figure 4.4.: An example of feature vector at $N = 8$ and $K = 7$

rithm, the precise normalization of face range images enables classification based on the histogram-features. In comparison to other approaches, it can be implemented in a very efficient way. The resulting feature is robust to small variations of the facial points like slight normalization errors, or slight facial expressions and even to larger variations such as spikes and holes. The distribution for each stripe is already normalized to the number of points in the stripe such that small variations or normalization inaccuracies have only minor impact on the feature vector.

Due to the inherent properties of the algorithm preprocessing steps like surface smoothing, interpolation of holes in the surface or removal of outliers, which are crucial for e.g. PCA or LDA based recognition method, are not strictly required. In the next section we present simulation results for the proposed algorithm.

4.1.2. Experimental Results

The proposed system has been implemented and tested with the database of face recognition grand challenge [PFS*05] (FRGC) version 1.0 and 2.0, which consist of 4950 range images from 547 subjects. The normalization algorithm was implemented as a proof of concept. The current approach doesn't perform optimally. 4522 range images of the FRGC database have been normalized correctly. The failure to normalize rate is at 8.65%.

The range of valid facial region can be determined in a training process. 250 models of different subjects are randomly chosen from the correctly normalized 3D models as training data. As the detection and removal of outliers are computationally expensive, we use the percentile of depth values as bounding in order to suppress the effect of outliers. In Figure 4.5 the candidates of the upper limit for each sub area are plotted, where the stripe number increases from the lower jaw to the forehead. As shown in the lower sub figure, the circle marker of the 99.95 percentile has significant difference in stripes 4, 10, 11 and 12 to the magenta cross of the local maximum and it is more robust to the outliers in the data set. The variation of the 99.95, 99.9 and 99.5 percentile in nose area (stripes 6 to 10) is relatively small as shown in the upper figure, since the nose tip is defined as the origin and the normalization is oriented according to the form of the nose. It indicates also that the normalization is very precise. In other areas such as the mouth and forehead stripes the difference is high. Especially, the variation of stripes 15, 16 and 17 is extremely high. In these areas the data is disturbed by the hair, therefore, their upper limit is taken from the adjacent area, stripe 14.

After determining the facial region, the proposed feature extraction algorithm is applied to the selected facial regions of the correctly normalized 3D models. The face region is divided into N stripes. The feature vector of each stripe is calculated in K continuous depth values intervals. The resulting feature vector consists of $N \times K$

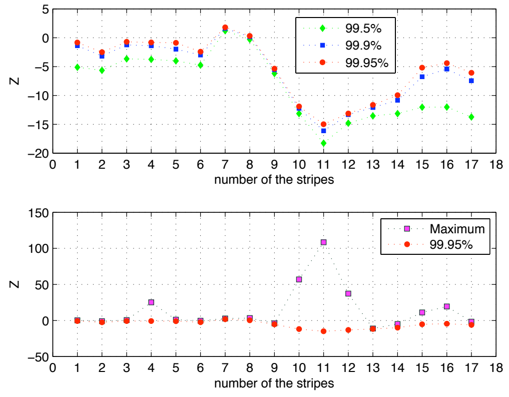


Figure 4.5.: The candidates of the upper limit for each sub area

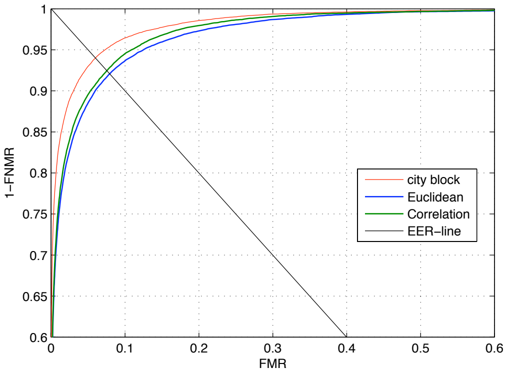


Figure 4.6.: The ROC curves using city block, Euclidean distance and correlation

components. To compare the features, different metrics can be utilized. We tested our results with three different metrics. Other metrics such as maximum likelihood, support vector machine can also be used. Given two feature vectors $V = \{v_i\}$ and $U = \{u_i\}$, the city block metric is defined as:

$$L_1 = \sum_i |v_i - u_i| \tag{4.3}$$

The Euclidean distance can be calculated with:

$$L_2 = \sqrt{\sum_i (v_i - u_i)^2} \tag{4.4}$$

And the correlation is calculated as follows [4]:

$$C = 1 - \frac{(V - \mu_V)^T (U - \mu_U)}{\sigma_U \sigma_V} \tag{4.5}$$

where μ_V, μ_U are the mean of the feature vectors, σ_V, σ_U are their standard deviations.

For $N = 67$ and $K = 6$, the ROC curves using different metrics are depicted in Figure 4.6. The use of different metrics has a strong effect on the verification performance. The comparator using city block metric gives the best results: the red line of its ROC curve is above the blue line of Euclidean distance and the green of correlation. The correlation comparator is slightly better than the Euclidean distance comparator.

Changing the parameters N and K influences the robustness and discriminative power of the algorithm. If K remains constant and the facial region is divided into different segments, Figure 4.7 shows that both $FNMR$ and FMR shift to left by decreasing N. A small N increases the number of evaluated points per stripe. Therefore, the robustness of the resulting features is improved, however, their discriminative power reduces. Similarly, if N is fixed and different depth value division is chosen, both $FNMR$ and FMR move to left by reducing K as shown in Figure 4.8. So enlarging the number of evaluated depth regions strongly enhances discriminative power and

[4] Normally, the correlation indicates the similarity of the templates. In order to compare it with the other distance-based comparators, the comparison score C is one minus the correlation coefficient.

reduces robustness. The adjustment of K and N is dependent on the size of facial region. Comparing Figures 4.7 and 4.8, changing K has a much stronger influence on the robustness and discriminative power than N. Similar results can also be observed in Figure 4.9. The performance of the algorithm is dependent on K and N. The equal error rates (EER) at different N and K are shown in Table 4.1. The best equal error rate of 5.89% is achieved at $N = 67$ and $K = 12$.

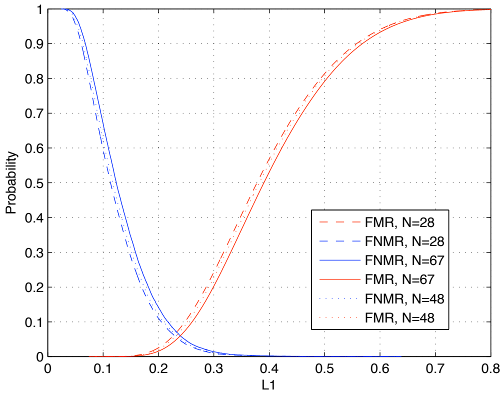


Figure 4.7.: False match rates and false non-match rates at $K = 6$

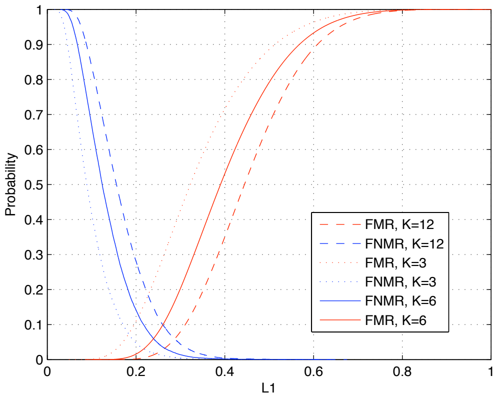


Figure 4.8.: False match rates and false non-match rates at $N = 67$

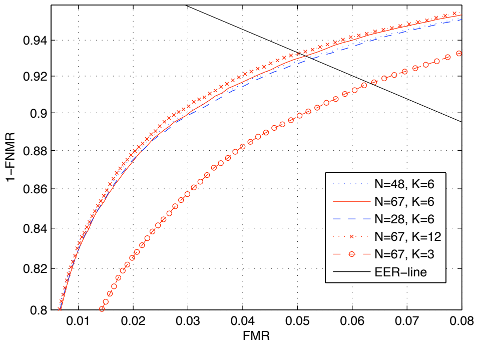


Figure 4.9.: The ROC curves at different N and K

N	K	EER
67	3	7.36%
28	6	6.18%
48	6	6.13%
67	6	6.00%
67	12	5.90%

Table 4.1.: EER at different N and K.

In this section a 3D face recognition algorithm was introduced and its recognition performance in the FRGC database was evaluated. In the next section a template protection algorithm is integrated to protect the 3D facial features.

4.2. The Fuzzy Commitment Scheme for 3D Face Recognition

The fuzzy commitment scheme is proposed in [JW99]. As shown in Section 2.2.1, it is one of the most successful template protection algorithms and has been implemented in different kinds of biometric systems. We showed in the previous section that the extracted 3D face features are vectors with a fixed length and have good robustness. The integration of fuzzy commitment is very promising. In this section, we show the details of the fuzzy commitment implementation in the 3D face recognition system.

4.2.1. Implementation of the Fuzzy Commitment Scheme

Fuzzy commitment binds unique secrets to biometric data. It combines error correction coding and cryptography so that reliable secret regeneration from noisy data is possible. Helper data is necessary to compensate the noise during biometric acquisitions. Therefore, fuzzy commitment is a kind of helper data scheme [Tuy04]. The helper data is the auxiliary data defined in the ISO standard [ISO11]. It is not allowed to reveal information about secrets. In the following we show the fuzzy commit scheme for 3D face recognition. The block diagram is depicted in Figure 4.10.

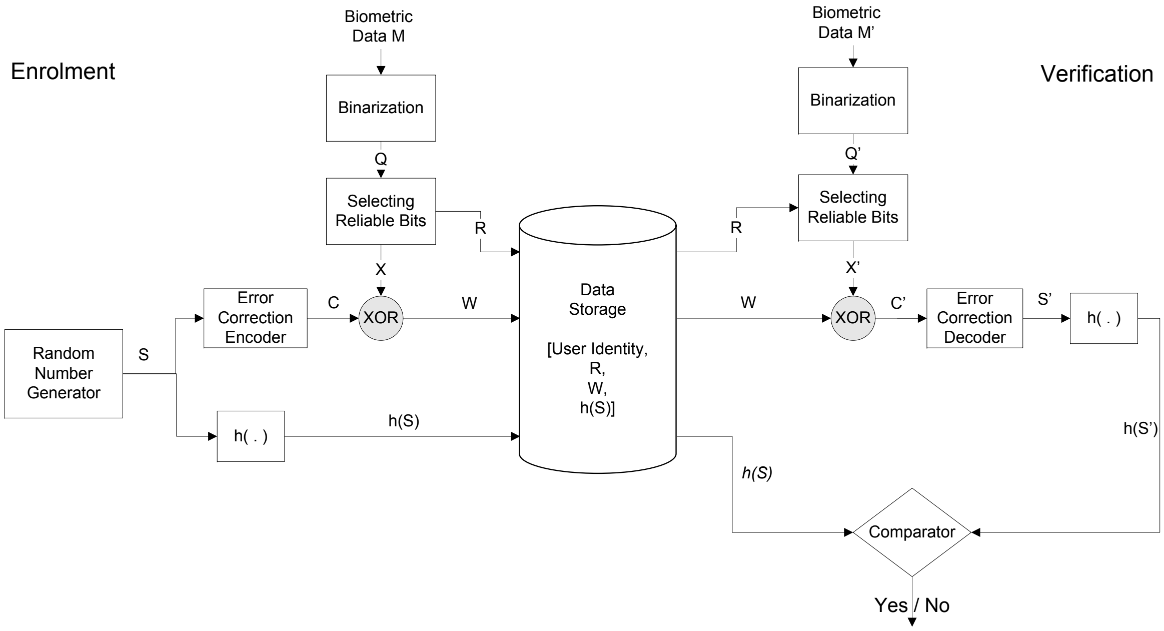


Figure 4.10.: The block diagram of the fuzzy comment scheme for 3D face recognition

A biometric template M is extracted from a biometric sample. In the enrollment process, the binarization converts the biometric template M into a binary vector Q. The binarization should make Q uniformly distributed for different users and invariant for identical user. The binarization is detailed described in Section 4.2.1.1. The random number generator creates randomly a secret S. The hash $h(S)$ is the pseudonymous identifier and stored as a part of the secure template. The error correction encoder adds redundancy and produces a codeword C, which is longer than S. Depending on the property of bit errors, different error correction codes can be adopted.

To correct uniformly distributed bit errors, the BCH- code can be used. It has a codeword length of $2^L - 1$ (L is a natural number). If the length of the bit string Q extends the length of the codeword C, only the most reliable bits in Q are selected so that the resulting binary string X is as long as the codeword C and robustness can be further improved. R indicates the position of the reliable bits. W, the bitwise XOR of X and C, is the so-called helper data. With the help of W, the same secret S can be regenerated in the verification process. Only the position vector R, the helper data W, the hashed secret code $h(S)$ and user identity information are stored in data storage. Ideally, both W and $h(S)$ should reveal little information about S.

During the verification process, R, W and $h(S)$ are released from data storage with a claimed identity. The binary string Q' is extracted from biometric template M', which is a noise-distorted version of M. The binary string X' is estimated with M' and R. A corrupted codeword C' can be acquired from W and X'. The following error correction decoder removes errors in C' and outputs a secret S'. Comparing $h(S)$ with $h(S')$, a positive or negative verification response can be given. Only a "hard decision" (rejected or accepted) is given and no similarity scores are available in the comparer of the fuzzy commitment system due to the hash function. Hill climbing attack, which iteratively reconstructs biometric data using matching scores [Adl04,Sou02], is prevented.

The random number generator enables randomness in the system. Distinct secure templates can be created from the same biometric for different applications. Additionally, revocation and reissuing of templates are enabled. Error correction coding eliminates bit errors due to variations in biometric measurements. The length of the secret is restricted by the error correction ability, if the length of the codeword is fixed. Ideally, the secret length should not be larger than the average min entropy of binary feature X given the helper data W [DORS08]. Binarization and selecting reliable bits are decisive to the recognition performance. In the following we introduce their functionalities and constructions.

4.2.1.1. Binarization

Binarization is the core component of helper data scheme. The binarized features should be uniformly and independently distributed from the security point of view (see Section 3.4). Additionally, these features should have good robustness to noise, since the error correction code has limited error correction ability. The binarization aims to extract a long uniformly and independently distributed bit string from biometric templates without significant degradation of authentication performance.

We use here a simple method, which depends on the statistical analysis of the input biometric templates. Assuming that a training set contains N subjects and each subject has K samples and $M_{n,k} = \left[m_{n,k,1}, m_{n,k,2}, \cdots, m_{n,k,T}\right]$ is the template with T components extracted from the k-th samples of the subject n, where $k \in \{1, \cdots, K\}$ and $n \in \{1, \cdots, N\}$. Assume that each component is statistically independent and at least one bit can be extracted from each component, the binarization function B can be defined as:

$$q_{n,t} = B_{k \in [1,\cdots,K]}(m_{n,k,t}) = \begin{cases} 1 & \text{if} \quad \mu_{n,t} \geq \mu_t \\ 0 & \text{if} \quad \mu_{n,t} < \mu_t \end{cases} \tag{4.6}$$

where $\mu_{n,t}$ is an estimation of the real feature component for subject n and the binarization threshold μ_t is the median of $\mu_{n,t}$ over all the subjects in order to achieve the uniform distribution of binary vectors. Instead of the median, the mean can also be adopted. If the training set is large enough, there is no significant difference between median and mean. In practice, we suggest to use median, which is resistant to outliers caused by measure errors.

4.2.1.2. Selection of Reliable Bits

Selecting reliable bits contributes to the robustness of the system. It is based on the estimation of the error probability for each bit. Only the bits with the lowest error probability are selected. Error probability depends on the distance between $\mu_{n,t}$ and μ_t. For a relatively stable bit, its $\mu_{n,t}$ is far from μ_t. On the other hand, intraclass variation is also decisive for error probability. The smaller the intraclass variation is, the more reliable is the corresponding bit.

Statistical analysis of intraclass characteristics for each subject has a major effect on the performance of selecting reliable bits. If biometric templates are Gaussian distributed, then:

$$\mu_{n,t} = E\left\{m_{n,k,t}\right\} \tag{4.7}$$

$$\tilde{p}_{n,t} = \frac{|\mu_{n,t} - \mu_t|}{\sigma_{n,t}} \tag{4.8}$$

where E is the function calculating the expected value, $\sigma_{n,t}$ is the standard deviation of $m_{n,k,t}$ for $k \in [1, \cdots, K]$. $\tilde{p}_{n,t}$ is derived from the Gaussian error function and shows the strength of the error probability of the t-th component of subject n, (see also [vdVKS*06]). The smaller the $\tilde{p}_{n,t}$ is, the lower is the error probability.

If the templates are uniformly distributed, then $\mu_{n,t}$ and $\tilde{p}_{n,t}$ can be calculated with:

$$\mu_{n,t} = median\left\{m_{n,k,t}\right\} \tag{4.9}$$

$$\tilde{p}_{n,t} = |\mu_{n,t} - \mu_t| \tag{4.10}$$

Actually, a reliable estimation of error probabilities is only possible with a sufficient number of enrolment samples. However, in practice, we can not make too many acquirements during an enrolment. Gaussian distribution is commonly used in the case of lack of information about a random variable. In the next section we show the recognition performance of the implemented fuzzy commitment scheme for 3D face recognition.

4.2.2. Experimental Results

We have implemented the template protection algorithm in the 3D face recognition system described in Section 4.1.1. As proof of concept, we firstly evaluate the recognition performance with a subset of FRGC version 1.0. Later we give an enormous evaluation with the test data from both FRGC database version 1.0 and 2.0 [PFS*05].

4.2.2.1. Results with Small Dataset

A small-scale experiment is done with FRGC v1.0. During the test, 99 of 289 subjects are chosen, who have at least 4 samples. Three samples per subject are randomly chosen as enrolment data and one sample as verification data. The tests are repeated 4 times and different enrolment samples are chosen each time. A feature vector is extracted from 68 sub-areas of the normalised facial image and consists of $68 \times 6 = 408$ real values. The false match rate (FMR) and false non-match rate ($FNMR$) using the correlation classifier are plotted in Figure 4.11. The equal error rate (EER) is equal to 3.38%.

Then, we use the above mentioned binarization function to convert the extracted feature vectors into binary strings. The receiver operation characteristic (ROC) curves before and after binarization are plotted in Figure 4.12. The solid line of the binary vectors is obviously above the dashed line of the real-valued feature vector. That is to say, binarization function improves slightly the authentication performance. Generally, a good binarization function should not result strong degradation of the recognition performance.

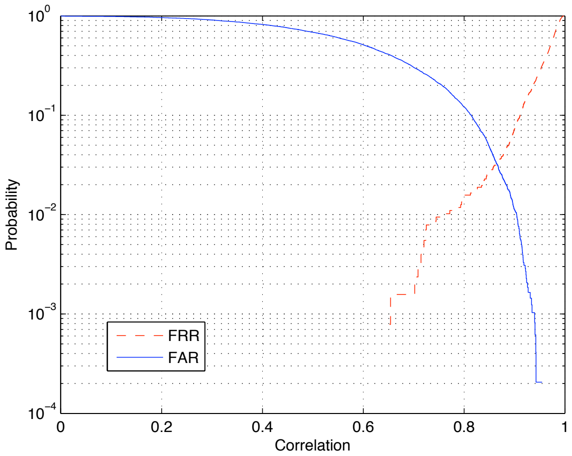


Figure 4.11.: Classification results of the histogram-based face recognition algorithm

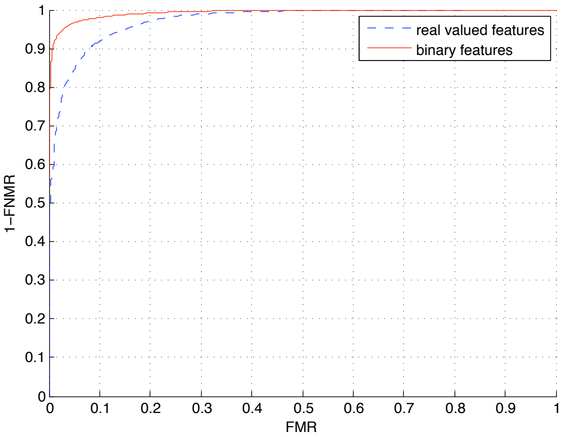


Figure 4.12.: ROC curves of real-valued feature vectors and binary feature vectors

In the previous experiment, the median is adopted to calculate the binarization thresholds. If we compare the FMR and $FNMR$ curves of the binarization using median (the blue ones) and mean (the red ones in Figure 4.13), there is no significant difference regarding recognition performance. Both EER are around 3%, however, the $FNMR$-curve of mean-based binary vectors deviates from the probability-axis in comparison with the one of median-based binary vectors. The median-based binarization has higher robustness to noise. This makes it better than the mean-based binarization, since the performance of fuzzy commitment is restricted by errors occurring in the binary feature vectors.

BCH (L_C, L_S, L_E)	Correctable BER	Results for uniform distribution	Results for Gaussian distribution
255, 107, 22	8.6%	$FNMR$=12%; FMR=0.4%	$FNMR$=21%; $FMR\approx 0$
255, 91, 25	9.8%	$FNMR$=11%; FMR=0.6%	$FNMR$=16%; FMR=0.2%
255, 79, 27	10.5%	$FNMR$=10%; FMR=0.7%	$FNMR$=13%; FMR=0.3%

Table 4.2.: Examples of possible BCH code settings and the corresponding $FNMR$ and FMR

In the implemented scheme, a BCH-code is chosen as error correction code. The maximum length of a codeword below 408 is 255. The 255 most reliable bits are selected from the 408-bits long binary vector. The classification results under the assumption of uniformly distributed templates and Gaussian distributed templates are shown in Figure 4.14. Both classification results are similar. Under the assumption of uniform distribution, the robustness is better than under the assumption of Gaussian distribution, however, the discriminative power is slightly worse.

We denote L_C, L_S, and L_E as the codeword length, the secret length and the number of correctable bit errors respectively. With the BCH-code, only certain combinations of L_C, L_S, and L_E are possible. Several examples and their corresponding Bit Error Rate (BER), $FNMR$ and FMR are given in Table 4.2. For all the settings, the $FNMR$ under the assumption of uniform distribution is significantly better than under the assumption of Gaussian distribution, while its FMR decreases slightly.

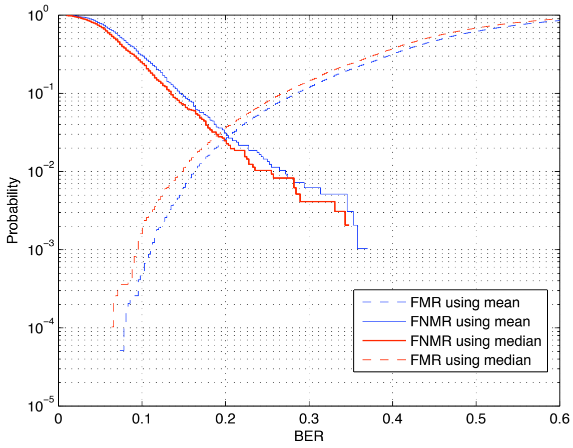


Figure 4.13.: Classification results of the binary vectors using the median-based and mean-based binarizations

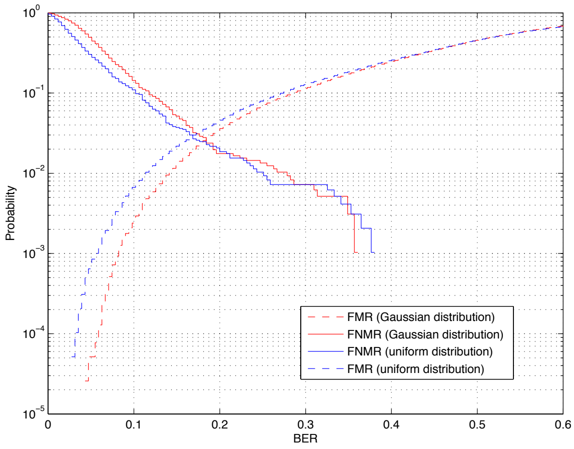


Figure 4.14.: Classification results of the selected binary vectors under the assumptions of uniformly distributed templates and of Gaussian distributed templates

4.2.2.2. Results with Full Dataset

We extend our experiments with all range images from face recognition grant challenge (FRGC) database version 1.0 and 2.0. There are 4950 range images from 547 different subjects. Only 380 subjects have more than 4 samples. 3 samples per subject are randomly chosen as enrolment samples and the rests are for verification. The tests are repeated 4 times.

Figure 4.15 and 4.16 show the influence of binarization on the recognition performance. Each line represents a ROC curve of real-valued or binary features by a setting of $N \times K$, (N is the number of stripes, K is the number of bins in histogram calculation and $N \times K$ is the length of the feature vectors). The solid lines - ROC curves of binary features - are below the dashed lines of real-valued features. The performance is degraded after applying binarization. The degradation is strong in the area of small FMR ($FMR < 0.1$). Changing the parameters of N and K, the effects on real-valued and binary features are very similar: the performance is improved with increasing K and there are no significant changes by changing N.

After the binarization process, the most reliable bits are selected in order to fit the length of the BCH-codeword. The performance of selected bits at different length L_C of 127, 255 and 511 is shown in Figures 4.17 and 4.18. The performance changes in the area of large FMR are not as significant as in the area of small FMR. As described in Section 4.2.1.2, different estimation methods of error probability, namely Gaussian model and uniform distribution model (using median) are tested. Figure 4.17 shows that the dashed lines of the results using median are below the solid lines of the Gaussian model. The Gaussian model gives more reliable error estimation in comparison with the median. In Figure 4.18, we can see that the best three ROC curves are at ($L_C = 255, 68 \times 13$), ($L_C = 255, 68 \times 7$) and, ($L_C = 127, 68 \times 13$). The best setting of L_C is 255. A longer L_C cannot always improve the performance. For instance, for biometric features with a length of $m = 68 \times 13 = 884$, the performance of $L_C = 511$ is the worst one in $L_C \in \{127, 255, 511\}$. The black dash-dotted line is the best ROC curve of binary features without feature selection. It is very close to the three best ones with selected features. Therefore, the selection influences slightly the performance.

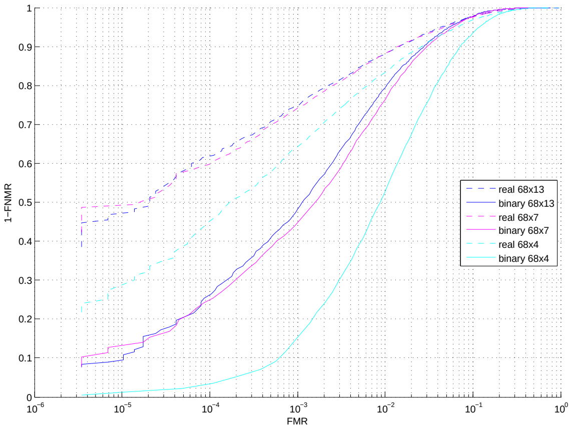


Figure 4.15.: ROC curves of real-valued and binary features at $N = 68$

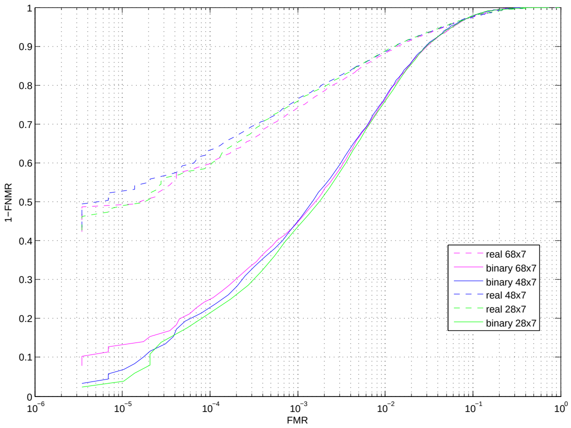


Figure 4.16.: ROC curves of real-valued and binary features at $K = 7$

Figure 4.19 shows the performance after applying the fuzzy commitment scheme. *FMR* and *FNMR* at some sampled operational points are given in Table 4.3. The best recognition performance is achieved with $m = 68 \times 13$. The codeword length $L_C = 255$ is the best for all possible feature lengths.

$m = 28 \times 7 = 196$			$m = 68 \times 13 = 884$		
(L_C, L_S, L_E)	*FNMR*	*FMR*	(L_C, L_S, L_E)	*FNMR*	*FMR*
(127, 8, 31)	4.28%	6.06%	(127, 29, 21)	3.88%	6.32%
(127, 15, 27)	6.90%	4.14%	(127, 36, 15)	7.42%	3.43%
(127, 29, 21)	13.20%	2.16%	(127, 50, 13)	9.27%	2.62%
$m = 68 \times 7 = 476$			(127, 64, 10)	13.64%	1.59%
(127, 15, 27)	2.25%	9.33%	(127, 71, 9)	15.61%	1.29%
(127, 29, 21)	4.13%	6.03%	(255, 29, 47)	4.81%	5.13%
(127, 43, 14)	9.22%	3.09%	(255, 37, 45)	5.28%	4.68%
(127, 64, 10)	14.75%	1.72%	(255, 47, 42)	6.09%	4.03%
(255, 21, 55)	4.58%	5.28%	(255, 55, 31)	11.44%	2.04%
(255, 29, 47)	7.07%	3.59%	(255, 71, 29)	12.86%	1.73%
(255, 37, 45)	7.96%	3.21%	(255, 87, 26)	15.43%	1.34%
(255, 47,42)	9.64%	2.75%	(511, 19, 119)	7.40%	3.84%
(255, 55, 31)	17.68%	1.32%	(511, 31, 109)	9.98%	2.79%
(255 , 71, 29)	19.97%	1.12%	(511, 49, 93)	16.08%	1.59%

Table 4.3.: *FNMR* and *FMR* at different coding settings and feature lengths

In comparison with the results in the previous section, the recognition performance becomes worse. Here the full FRGC dataset is used, which includes challenging samples with strong variations. The reliability of the feature extraction algorithm has to be improved. The performance improvement with binarization cannot be observed any more. However, binarization has only a minor influence on the performance. The selection of the reliable bits can filter the unreliable bits and choose the stable bits individually for each subject. Therefore,

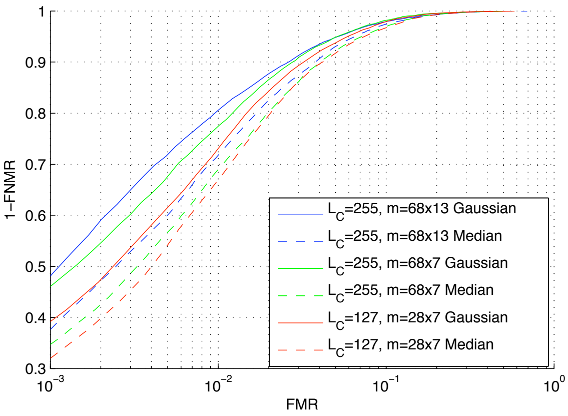


Figure 4.17.: ROC curves of selected reliable bits based on the Gaussian model and uniform distribution

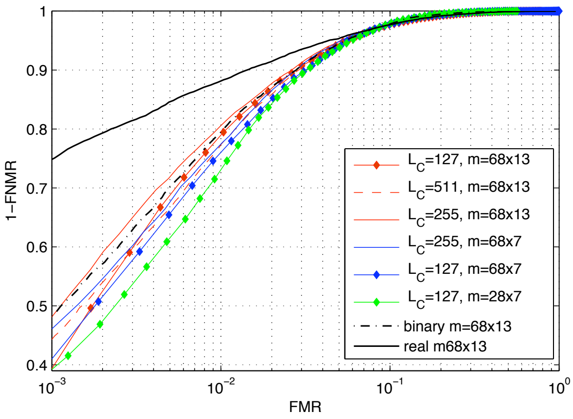


Figure 4.18.: ROC curves of selected reliable bits at different settings using Gaussian model and ROC of the real-valued and binary features with the best performance

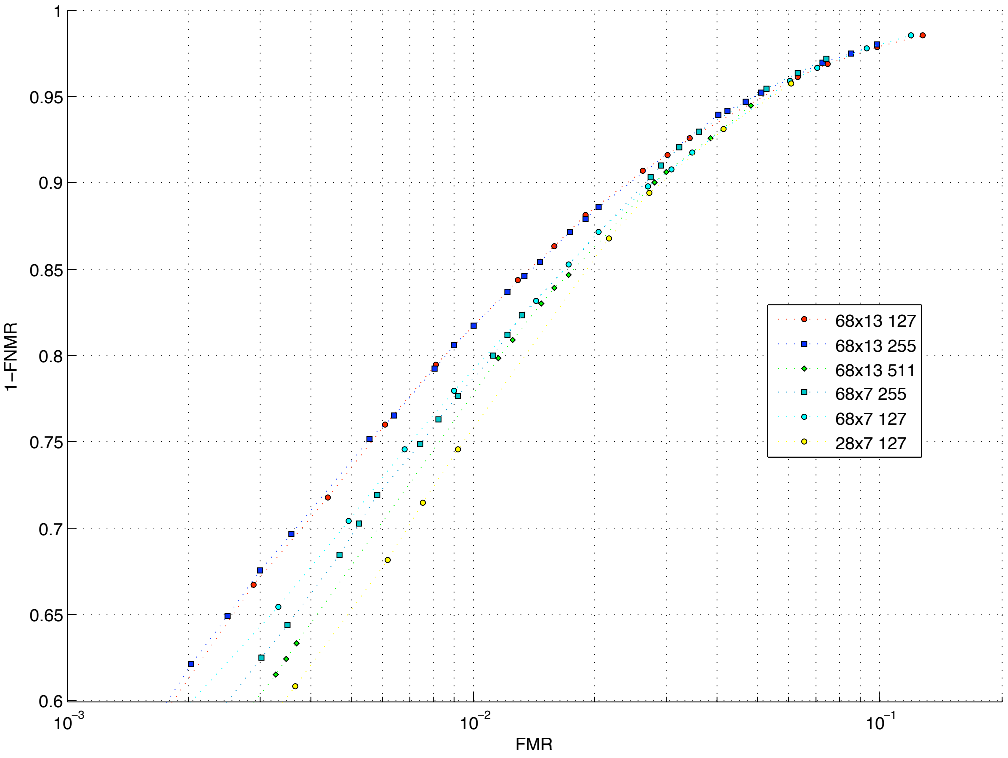


Figure 4.19.: ROC curves after applying fuzzy commitment

the performance after selection does not change. Although error probability estimation with median delivers better results in the previous section, the opposite result is obtained with the full dataset. On the one hand, the error probability estimation is dependent on the dataset. On the other hand, Gaussian distribution shows better generalizability than the uniform distribution. In practice the best setting of a system can be found with well chosen training data and a good training algorithm. Additionally, a longer secret is desired for security reason. However, the length of the secret is limited by the robustness of the features, since the BCH-code can only correct about 25% bit errors. In this section we focused on the recognition performance of the fuzzy commitment system. In the next section we focus on the security and privacy assessment.

4.3. Privacy and Security Assessment

In this section we evaluate security and privacy of the developed fuzzy commitment system for 3D face recognition. Here we assume the *advanced threat model*. The assessment of “naive attack model” and “collision model” will be shown in Section 6.1.1.

4.3.1. Statistical Properties of the 3D Face Features

Section 3.4.1 showed that a fuzzy commitment scheme is perfectly secure if input biometric features are uniformly and independently distributed. In this section we examine whether the binary 3D facial features fulfill this requirement or not. Furthermore, the statistical properties of the features are analyzed.

The binary features are binarized from the real-valued features with interclass means. Let $X = [x_1, x_2, \cdots, x_m]$ be a m-bit long facial feature. A uniformly distributed bit has $p(x_i = 1) = p(x_i = 0) = 0.5$. We give an estimation of $p(x_i)$ with the interclass mean of x_i and denote it as $\hat{p}(x_i)$. The number of samples to estimate $p(x_i)$ is limited and $\hat{p}(x_i)$ may be different from the real $p(x_i)$. Assuming that $\hat{p}(x_i)$ is estimated from n independent trials. The confidence interval of $\hat{p}(x_i)$ with probability $1-\alpha/2$ can be calculated as follows:

$$\hat{p}(x_i) \pm z_{1-\alpha/2}\sqrt{\frac{\hat{p}(x_i)(1-\hat{p}(x_i))}{\mathrm{n}}} \tag{4.11}$$

where $z_{1-\alpha/2}$ is $1-\alpha/2$ percentile of a standard normal distribution [Ken64]. If x_i were uniformly distributed, then 0.5 should be within the confidence interval of $\hat{p}(x_i)$:

$$\begin{aligned} \hat{p}(x_i) - z_{1-\alpha/2}\sqrt{\frac{\hat{p}(x_i)(1-\hat{p}(x_i))}{\mathrm{n}}} \leq \quad & 0.5 & \leq \hat{p}(x_i) + z_{1-\alpha/2}\sqrt{\frac{\hat{p}(x_i)(1-\hat{p}(x_i))}{\mathrm{n}}} \\ \frac{1}{2} - \frac{1}{2}\frac{1}{\sqrt{1+\frac{\mathrm{n}}{z_{1-\alpha/2}^2}}} \leq \quad & \hat{p}(x_i) & \leq \frac{1}{2} + \frac{1}{2}\frac{1}{\sqrt{1+\frac{\mathrm{n}}{z_{1-\alpha/2}^2}}} \end{aligned} \tag{4.12}$$

We evaluate the distribution of the binary features with the length of 196, 476 and 884. These settings are representative for other settings and have relatively good performance (see Section 4.2.2.2). The 95% confidence interval with $z_{95} = 1.96$ is chosen. The features are derived from different 380 subjects and n = 380. If $45\% \leq \hat{p}(x_i) \leq 55\%$, the expected probability of 0.5 is within the 95% confidence interval of $\hat{p}(x_i)$ and x_i can be seen as uniformly distributed. Figure 4.20 depicts $\hat{p}(x_i)$ at different settings. Obviously many bits are not within the desired interval: only 75 of 196 bits, 196 of 476 bits and 289 of 884 bits can be seen as uniformly distributed. It is about 30%-40% of all the bits in binary features.

Figure 4.21 shows some examples of the interclass distribution of real-valued features. Some features can not be converted into uniformly distributed bits as shown in the histogram of x_{116} on the left of the figure. It contains a lot of zeros. Such features occur often at the smallest or largest bins in the depth value interval in a stripe during feature extraction. On the other hand, there are some real-valued skew-distributed features (e.g. the histogram on the right of the figure). Their binarization results are much more sensitive to the variation of the thresholds in comparison to those symmetrically distributed features as show in the middle of the figure. It is not always possible to achieve a uniform distribution in practice.

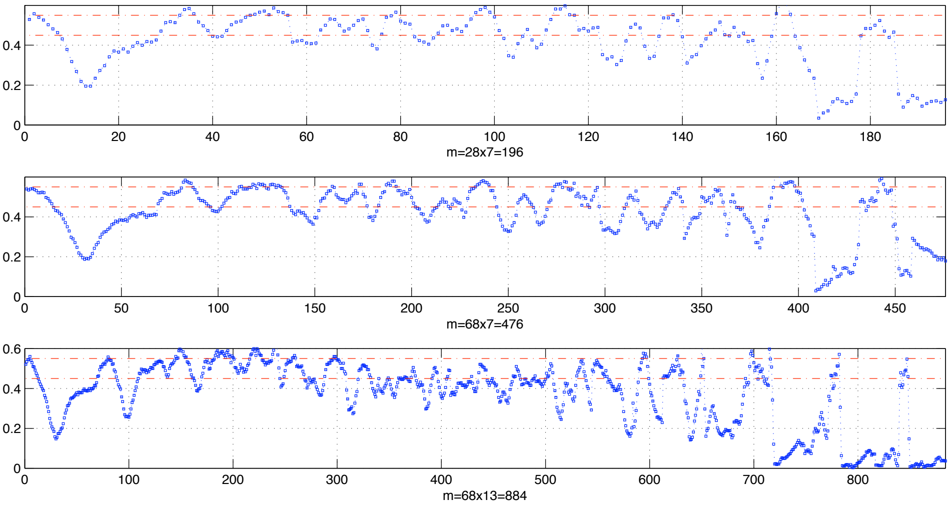


Figure 4.20.: $\hat{p}(x_i)$ for $m = 196, 476, 884$ (blue line with circles) and the expected range [0.45, 0.55] of a uniform distribution (red solid-dashed lines).

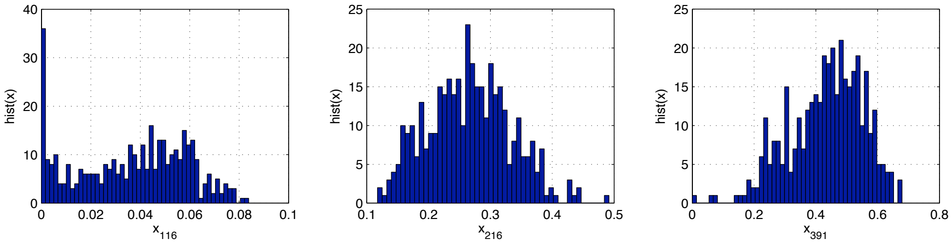


Figure 4.21.: The interclass histograms of different real-valued features for $m = 476$ (the number of the bins is 50).

Most of the bits in the feature are not uniformly distributed. Moreover, we analyze their dependency. We denote the probability of feature $X = [x_1, x_2, \cdots x_m]$ as $P(x_1, x_2, \cdots x_m)$. It is very hard to estimate the probability distribution of high dimensional data. Here I make a simplification and describe $P(x_1, x_2, \cdots x_m)$ with *a second-order dependency tree*:

$$\hat{P}(x_1, x_2, \cdots, x_m) = \prod_{i=1}^{m} P(x_{u_i} | x_{u_{j(i)}}) \tag{4.13}$$

where $[u_1, u_2, \cdots, u_m]$ is a permutation of index $[1, 2, \cdots, m]$, $0 \leq j(i) < i$ and $P(x_{u_1}|x_{u_{j(1)}}) = P(x_{u_1})$. Chow and Liu analyzed how to optimize this estimation in the sense of Kullback-Leibler distance [CL68]. Therefore, Eq 4.13 is also called Chow-Liu representation. The definition of Kullback-Leibler distance is given in Eq A.15 of Appendix A.1.

The Kullback-Leibler distance between the real distribution of X and the second-order dependency tree is dependent on the following variables [CL68]:

$$D(P(X)||\hat{P}(X)) = -\sum_{i=1}^{m} I(x_{u_i}, x_{u_{j(i)}}) + \sum_{i=1}^{m} H(x_{u_i}) - H(X) \tag{4.14}$$

The last two terms - the entropy of X and the sum of the entropy of individual bits - are constant. Minimizing the estimation error in the sense of Kullback-Leibler distance is equivalent to maximizing $\sum_1^m I(x_{u_i}, x_{u_{j(i)}})$. Then finding the best estimation $\hat{P}(x_1, x_2, \cdots, x_m)$ is to determine optimal $[u_1, u_2, \cdots u_m]$, the tree structure, which maximizes $\sum_1^m I(x_{u_i}, x_{u_{j(i)}})$.

The entropy of X can be estimated with $\hat{P}(X)$. According to the chain rule of the joint entropy:

$$\begin{aligned}
\hat{H}(X) &= \hat{H}(x_{u_1}, x_{u_2}, \cdots, x_{u_m}) \\
&= H(x_{u_1}) + \sum_{i=2}^{m} H(x_{u_i}|x_{u_{j(i)}}) \\
&= \sum_{i=1}^{m} H(x_{u_i}) - \max_{[u_1, \cdots, u_m]} \left\{ \sum_{i=1}^{m} I(x_{u_i}, x_{u_{j(i)}}) \right\}
\end{aligned} \tag{4.15}$$

In the experiments, the mutual information $I(x_i, x_{i'})$ for all $i, i' \in [1, 2, \cdots, m]$ and $i \neq i'$ is calculated. If x_i and $x_{i'}$ are independent, $I(x_i, x_{i'}) = 0$. If they are totally dependent on each other, then $I(x_i, x_{i'}) = H(x_i) = H(x_{i'})$. The sum of the mutual information is maximized with a hierarchical clustering method and the corresponding permutation of feature vectors is returned. The database contains 4 subsets generated with different enrolment samples. We take one subset as a training set and estimate $[u_1, u_2, \cdots u_m]$ and $\hat{H}(X)$ with the second order dependency tree. Then we apply the resulting tree structure to the remaining 3 subsets and calculated $\hat{H}(X)$. The experimental results are shown in Table 4.4.

If X were uniformly independently distributed, its entropy should be equal to the feature length. Obviously, the estimated entropy is much smaller, since the dependency of features is taken into account. The features of $m = 196$ have the highest information rate. However, the corresponding recognition performance is spoiled due to the poor discriminative power. A trade-off between security and recognition performance is necessary. Although the tree structures trained with different datasets are similar, variations of 17.4 bits, 21.9 bits and 69 bits between training and testing can be observed for $m = 196, 476, 884$ respectively. The estimation results are sensitive to the change of the tree structure. If high order dependency between features is taken into account and a sufficient amount of training data is available, the estimation will be more stable. Despite that, the uncertainty of X reduces strongly when applying the training structure on the testing data. Additionally, the standard deviation of the results is very small. It means that the estimation of $\hat{H}(X)$ with training and testing set is very reliable.

The entropy $\hat{H}(X)$ only shows the properties of interclass distribution. The security and recognition performance of fuzzy commitment are based on both interclass and intraclass distributions.

Moreover, $\hat{H}(X)$ is an approximation of the real entropy. More accurate estimation is possible, if high order dependency of the features is analyzed. The dependency in binary features inherits the real valued features. Figure 4.22 shows the correlation of the 3D face features before and after binarization. The correlation between features remains after binarization. The binarization method shown in Section 4.2.1.1 is not optimal and not

m	$\hat{H}(X)$				$\hat{H}(X)/m$	
	Training		Testing		Training	Testing
	Mean	Std	Mean	Std		
196	88.4	0.31	105.8	0.32	0.451	0.539
476	153.7	1.51	175.6	1.45	0.323	0.370
884	280.2	1.67	349.2	2.62	0.317	0.395

Table 4.4.: The mean and standard deviation of the estimated entropy (in bits) and the information rate for the training and testing set

suitable for binarizing dependent features. A better alternative of binarization might be to group the highly correlated features and binarize them together in order to get more independent and reliable bits.

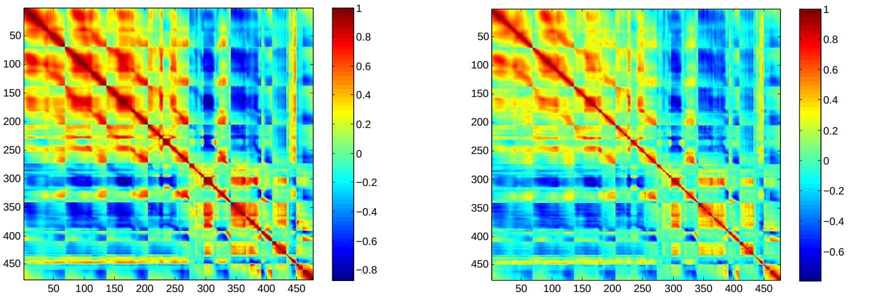


Figure 4.22.: Correlation coefficients of the real-valued features (left) and the binary features (right) at $m = 476$ (The color indicates the absolute values of the correlation coefficients.)

In this section we analysed the distribution of binary facial features. They are neither totally uniformly nor independently distributed. We used the second order dependency tree to simulate their distribution and estimated the entropy as well. In the following section we analyse the influence of the dependent features on the security and privacy of the template protection system.

4.3.2. Assessment of Privacy and Security

In this section we measure privacy and security of the protected 3D face system with information-theoretical metrics. We can give an upper bound of the security based on the knowledge about systems and statistical properties of X. Based upon this, we evaluate the privacy protection ability.

In fuzzy commitment, helper data $W = C \oplus X$, where C is a (n,k)-codeword of S, where n is the codeword length and k is the secret length. Assuming that C is a linear block code with $C = S \cdot G$:

$$(c_1, \cdots, c_n) \quad = \quad (s_1, \cdots, s_k) \cdot \begin{pmatrix} g_1^1 & \cdots & g_1^n \\ \vdots & \ddots & \vdots \\ g_k^1 & \cdots & g_k^n \end{pmatrix} \tag{4.16}$$

where g_i^j is the element at the i-th row and the j column in the $k \times n$ generator matrix G. The rank of G is denoted as $r_G = Rank(G) = k$. We denote $\mathbf{g}_i$ as the i-th row of G and $\mathbf{g}^j$ as the j-th column of G. Each bit in C is a linear combination of S with a corresponding column vector in G:

$$c_j = (s_1, \cdots, s_k) \cdot \mathbf{g}^j \tag{4.17}$$

In order to retrieve S, at least k bits in C must be known:

$$(s_1, \cdots, s_k) = (c_{u_1}, \cdots, c_{u_k}) \cdot (\mathbf{g}^{u_1}, \cdots, \mathbf{g}^{u_k})^{-1} \tag{4.18}$$

where $\mathbf{u} = [u_1, \cdots, u_k] \subset [1, \cdots, n]$ is the index vector of the bits selected from C and $\mathbf{g}^{u_i}$ is the corresponding column vector of c_{u_i} in G as shown in Eq 4.17. An inverse matrix of $(\mathbf{g}^{u_1}, \cdots, \mathbf{g}^{u_k})$ exists, if and only if its rank is equal to k. Then an upper bound of $H(S|W)$ can be given:

$$\begin{aligned} H(S|W) &= H(x_{u_1}, x_{u_2}, \cdots, x_{u_k}|W) && (4.19) \\ &\leq H(x_{u_1}, x_{u_2}, \cdots, x_{u_k}) && (4.20) \end{aligned}$$

The first equation is valid, since S can be calculated with W and $x_{u_1}, x_{u_2}, \cdots, x_{u_k}$, if $Rank\{(\mathbf{g}^{u_1}, \cdots, \mathbf{g}^{u_k})\} = k$. The second inequality is valid due to the chain rule of joint information.

Recall that Eq 3.9 in Section 3.4.1 shows: $H(S|W) = H(X|W) = H(S) + H(X) - H(W)$. Given an error correction code and biometric features, $H(S) = L_S$ and $H(X)$ are constant. Therefore, a coding process should be optimized to minimize $H(W)$.

In our protected 3D face recognition system (see Section 4.2.1), the BCH-code is used. The BCH-coding method is introduced in Section B.2. The BCH-code is a systematic code, which consists of k secret bits and $n-k$ redundant bits. It is sufficient to retrieve S, if the first k elements in X are successfully guessed. Therefore, we can use a sub-optimal method to give an approximation of $H(S|W)$ with the entropy of the first k bits in X.

The mutual $I(x_i, x_j)$ for all $i, j \in [1, \cdots, m]$ and $i \neq j$ is calculated. And L_C is denoted as the codeword length. For each subject, the enrolled secure template is loaded. The secure template contains the position vector U, which is the index of the L_C most reliable bits in X. $U = [u_1, u_2, \cdots, u_{L_S}, \cdots, u_{L_C}]$ and $U \subset [1, \cdots, m]$. Figure 4.23 shows the information rate of the selected binary feature $\hat{H}(X_1^{L_C})/L_C$ at different settings. Comparing with $\hat{H}(X_1^m)/m$ shown in Table 4.4, the selected bits become more uncorrelated, since less bits are used. The information rate decreases with increasing number of selected bits. The information rate at $m = 196$ and $m = 884$ is higher than that of $m = 476$ at the same L_C. The variation of the boxplot of $\hat{H}(X_1^{L_C})/L_C$ is due to the difference of the selected reliable bits between the subjects.

We give an approximation $\hat{H}(S|W) = \hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$ and use it to measure the security of the system. Here the bits $[x_{u_1}, \cdots, x_{u_{L_S}}]$ are those corresponding to the secret S. Then the entropy of these features is calculated using Eq. 4.15. The variation of $\hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$ is shown as the boxplot in Figure 4.24. $\hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$ is not the half of L_S. Strong degradation of security is observed here. Additionally for the same L_S, $\hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$ of $m = 196$ and $m = 884$ is higher than $m = 476$. The variation of $\hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$ increases with L_S. Additionally the boxplot shows strong variations of $\hat{H}(x_{u_1}, \cdots, x_{u_{L_S}})$. The variation also increases with L_S. For instance, the minimum and the maximum at $m = 476$ and $L_S = 71$ have 18 bits difference. It shows that the system provides different security to various subjects. In practice, we should set a minimum security number and the system should achieve this for all the subjects.

We show the results with different settings in detail in Table 4.5. The security increases with secret size, since the uncertainty of the secret is enlarged. In the current estimation, only the first L_S bits in the selected binary

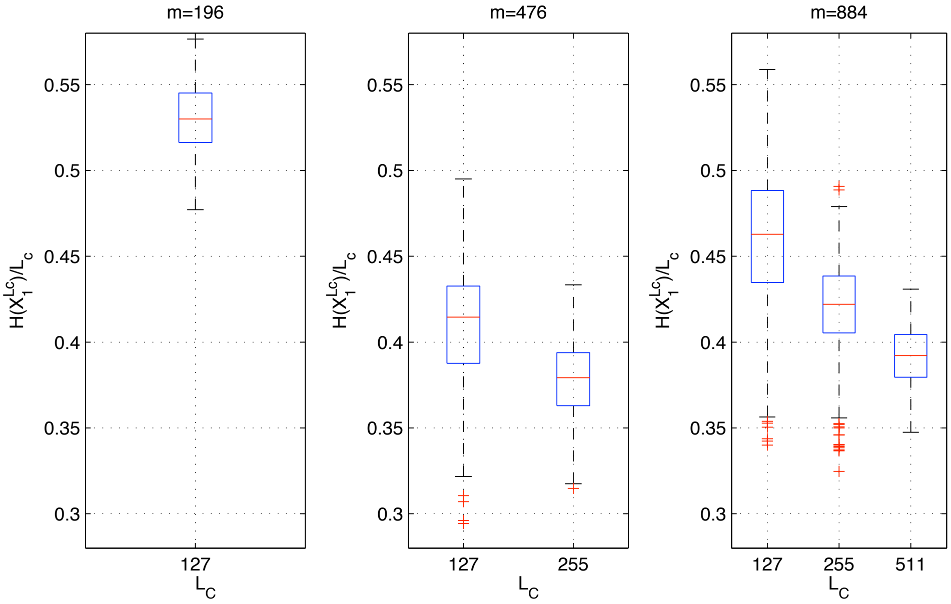


Figure 4.23.: Boxplot of $\hat{H}(X_1^{L_C})/L_C$ at different m and L_C

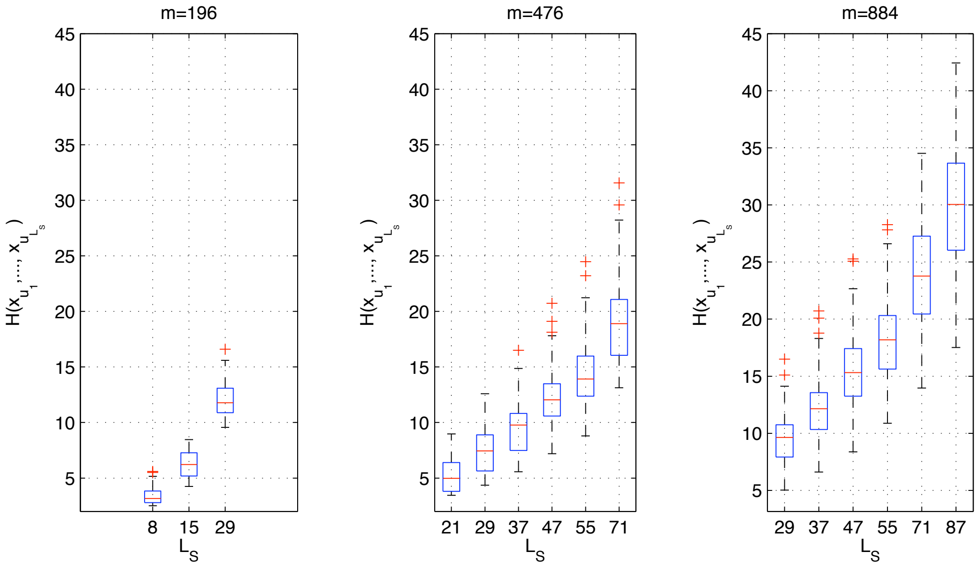


Figure 4.24.: Boxplot of $\hat{H}(x_{u_1},\cdots,x_{u_{L_S}})$ at different L_S

feature are used. Eq 4.20 shows that this results is a close upper bound of $H(S|W)$. In the optimal estimation, all L_S bits combinations should be tested, whose corresponding bits in the codeword can reveal the remaining bits. Additionally, the influence of W should be taken into account.

If we estimate S with W and $[x_{u_1},\cdots,x_{u_{L_S}}]$, then the conditional guessing entropy $G(S|W)$ is approximately equal to the guessing entropy of $[x_{u_1},\cdots,x_{u_{L_S}}]$. Eq A.19 in Appendix A.2 shows the relation between guessing entropy and entropy. From Eq A.19, we can give the following lower bound of $G(S|W)$:

$$\begin{aligned}\hat{G}(S|W) &= G(x_{u_1},x_{u_2},\cdots,x_{u_{L_S}}) \\ &\geq 2^{H(x_{u_1},x_{u_2},\cdots,x_{u_{L_S}})-2}+1 \end{aligned} \tag{4.21}$$

Privacy protection ability is another important evaluation criteria. In the fuzzy commitment scheme, the privacy is strongly related to the security. If the secret S is compromised, the biometric feature $X_{u_1}^{u_{L_C}} = [x_{u_1},\cdots,x_{u_{L_C}}]$ is also exposed. Depending on the requirements of applications, privacy can also be measured regarding real-valued feature M or acquired biometric samples. Along data flow in biometric systems, information about raw biometric data reduces. For instance, a 3D range image contains more information about the 3D face than the extracted facial feature. In this section we only look at the privacy regarding binary feature X [5]. We use the conditional entropy to quantify the irreversibility of secure templates:

$$\hat{H}(X_{u_1}^{u_{L_C}}|W) = \hat{H}(S|W) = \hat{H}(X_{u_1}^{u_{L_S}}) \tag{4.22}$$

$$\begin{aligned}\hat{H}(X|W) &= \hat{H}(X_{u_1}^{u_{L_C}}|W)+\hat{H}(X_{u_{L_C+1}}^{u_m}|W,X_{u_1}^{u_{L_C}}) \\ &\overset{(a)}{=} \hat{H}(X_{u_1}^{u_{L_C}}|W)+\hat{H}(X_{u_{L_C+1}}^{u_m}|X_{u_1}^{u_{L_C}}) \\ &= \hat{H}(X_{u_1}^{u_{L_S}})+\hat{H}(X)-\hat{H}(X_{u_1}^{u_{L_C}}) \end{aligned} \tag{4.23}$$

the equality of (a) is valid, since $W = X_{u_1}^{u_{L_C}} \oplus C$ and W gives no additional information about $X_{u_{L_C+1}}^{u_{L_X}}$ if $X_{u_1}^{u_{L_C}}$ is known.

The irreversibility shows the hardness to retrieve biometric data. Additionally, the information about biometric data contained in secure templates needs to be measured, namely the privacy leakage. Irreversibility and privacy leakage are not directly related. For instance, a protected biometric system can be very safe and it is hard for an adversary to estimate biometric data, meanwhile, it can have high privacy leakage. The privacy leakage can cause further security problems such as linkability. Therefore, it is important to evaluate privacy leakage. We use the mutual information to assess the privacy leakage. With Eq 4.23 and Eq A.11, it can be calculated with:

$$\hat{I}(X;W) = \hat{H}(X_{u_1}^{u_{L_C}})-\hat{H}(X_{u_1}^{u_{L_S}}) \tag{4.24}$$

The equation shows that the privacy leakage is only related to the selected binary feature $X_{u_1}^{u_{L_C}}$.

Table 4.5 shows the experimental results of irreversibility and privacy leakage. For each setting, irreversibility is larger than security. The binary feature is more secure than the secret, since several bits of the binary feature are discarded and not used in the secure template generation. The privacy protection ability can be improved with the enhanced security. For the same secret size, irreversibility of a short codeword is much higher than that of a long codeword and privacy leakage is also much lower than the long codeword. For the settings with the same feature size and codeword length, the irreversibility increases and privacy leakage reduces with the secret size. It shows that the high secret size can improve irreversibility and reduce privacy leakage. It also confirms the theoretical results of fuzzy commitment in the work of Ignatenko [Ign09].

[5] If the privacy of real-valued feature M need to be considered, the quantization loss during binarization process should be calculated, for instance, using rate-distortion theory.

m	L_S	Security $\hat{H}(S\|W)$			Irreversibility $\hat{H}(X\|W)$		Privacy Leakage $\hat{I}(X;W)$	
		mean	min	max	$L_C = 127$	$L_C = 255$	$L_C = 127$	$L_C = 255$
196	8	3.35	2.52	5.60	24.4	-	64.0	-
	15	6.21	4.26	8.46	27.3	-	61.1	-
	29	12.08	9.57	16.60	33.2	-	55.2	-
476	21	5.29	3.45	8.97	-	62.7	-	91.0
	29	7.35	4.36	12.59	109.0	64.8	44.7	88.9
	37	9.37	5.58	16.50	-	66.8	-	86.9
	47	11.95	7.20	20.73	-	69.4	-	84.3
	55	14.14	8.79	24.48	-	71.6	-	82.1
	71	18.72	13.13	31.57	-	76.2	-	77.5
884	29	9.44	5.03	16.50	231.3	182.7	48.9	97.5
	37	12.09	6.60	20.72	-	185.3	-	94.9
	47	15.41	8.37	25.27	-	188.6	-	91.6
	55	18.10	10.89	28.28	-	191.3	-	88.9
	71	23.74	13.96	34.52	-	197.0	-	83.2
	87	29.64	17.51	42.44	-	202.9	-	77.3

Table 4.5.: Assessment of security, irreversibility and privacy leakage (in bits) at different secret length L_S and feature length$m$

If a fuzzy commitment scheme is perfectly secure, the uncertainty about the secret given the auxiliary data is equal to the secret length. Our assessment shows that the developed system is far from perfect security. The security and irreversibility are poor. Privacy leakage is quite high. It is possible to improve the security and privacy performance to a certain extent by changing the coding construction. However, the perfect security with fuzzy commitment can be achieved with uniformly and independently distributed binary features. More appropriate efficient binarization process is necessary.

4.3.3. Assessment of Unlinkability

Section 3.4.2 elaborated linkage problems in fuzzy commitment. In the developed fuzzy commitment system for 3D face recognition, a secure template consists of $[R, W, h(S)]$, where R is the vector indicating the positions of the most reliable bits, W is the XOR of the selected binary biometric feature and the codeword of the secret S. In this section we will carefully analyze auxiliary data R and W and examine the possibility of linkage attacks.

The position vector R is determined by the statistical properties of biometric features. It is user-specific. As shown in Section 4.2.2, only L_C bits are chosen from an m-bit feature vector. L_C is the length of a BCH-codeword and $L_C = 2^N - 1$ for $N \in \mathcal{N}$. $R = [r_1, r_2, \cdots, r_{L_C}] \subseteq [1, 2, \cdots, m]$. $||R||$ is the number of all possible R:

$$||R|| = \binom{m}{L_C} \tag{4.25}$$

An intersection function is used to measure the similarity of two position vectors R and R' and is defined as:

$$InS(R, R') = ||R \cap R'|| \tag{4.26}$$

where $InS(R, R') \in \{\max\{0, 2L_C - m\}, \cdots, L_C - 1, L_C\}$. If $L_C > m/2$, $InS(R, R')$ is at least $2L_C - m$.

We calculate the intersection of the stored position vectors in the dataset generated in Section 4.2.2. Between different enrolment processes of a subject, at least one enrolled sample is different. The overlap between the position vectors of the same subject is computed as well as that of different subjects.

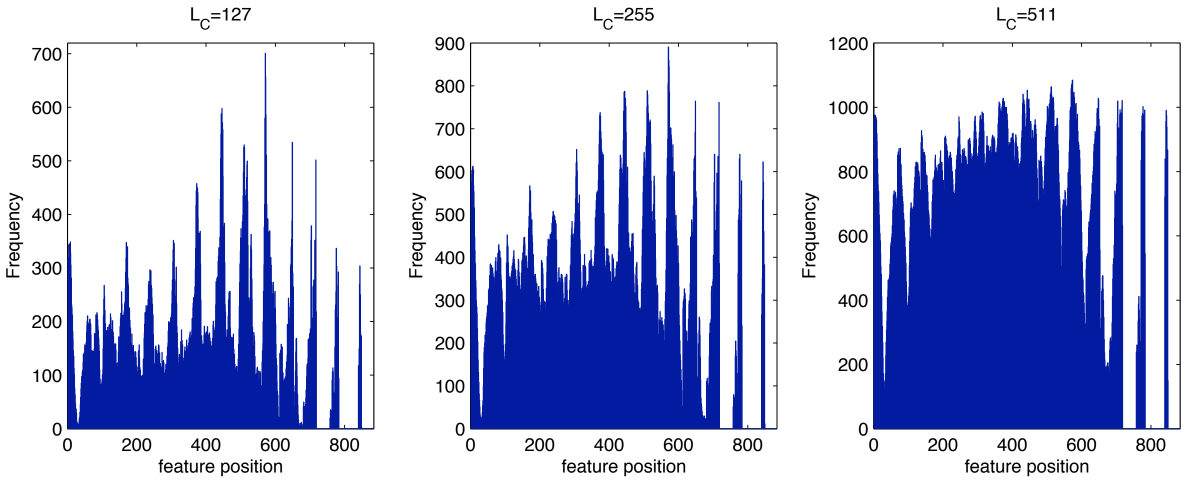


Figure 4.25.: The selection frequencies of individual bits for $m = 884$ and $L_C = \{127, 255, 511\}$

We take the enrolment sets with $m = 884$ and different L_C as examples and plot the frequencies in Figure 4.25, that an individual bit is selected as a reliable one for all the subjects. It is shown that some bits are more reliable and selected more frequently than others. There are also bits, which are never selected. Their corresponding real-valued features are strongly skewed distributed and can not be binarized into uniformly distributed bits (see Section 4.2.2) or their error probabilities are too high. The variations of the frequencies show that R is user-specific and contains distinguishing information. Additionally, the local maxima of the frequencies are located at the same positions and occur periodically. They are easier to recognise at smaller L_C. Those are the features with relatively good discriminative and robustness.

We calculate InS of position vectors at different settings. The range of interclass and intraclass InS is shown in Table 4.6. For the same m, both intraclass and interclass InS increase with L_C. The more features are selected, the more overlapping occurs in R. The minimum of InS_{inter} shows how many features are always selected in the ranking list of the L_C most reliable bits.

m		476		884		
L_C		127	255	127	255	511
InS_{inter}	max	87	213	74	185	479
	min	6	105	4	41	287
InS_{intra}	max	119	249	114	241	503
	min	35	149	21	86	359

Table 4.6.: The minimum and maximum of InS at different m and L_C

Figures 4.26, 4.27, 4.28, and 4.29 show the recognition performance using the InS at different settings. Figures 4.26 and 4.28 show that for the same m, FMR and $FNMR$ of different L_C are located at different ranges of InS

(see also Table 4.6). Figure 4.27 shows that for $m = 476$, the performance of $L_C = 127$ and $L_C = 255$ are similar and their equal error rate is about 5%. Figure 4.29 shows that for $m = 884$, the best performance can be achieved at $L_C = 255$ and the worst one is at $L_C = 511$.

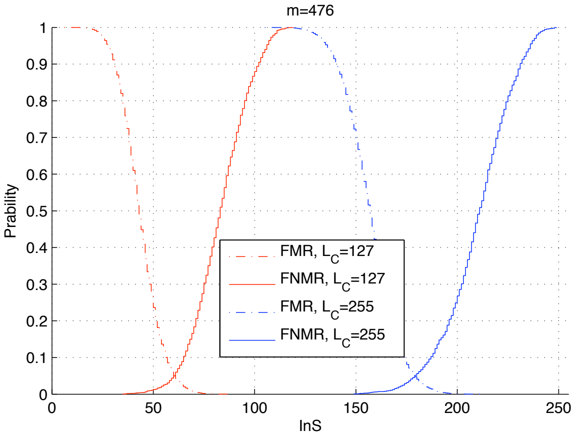


Figure 4.26.: *FMR* and *FNMR* over *InS* at $m = 476$

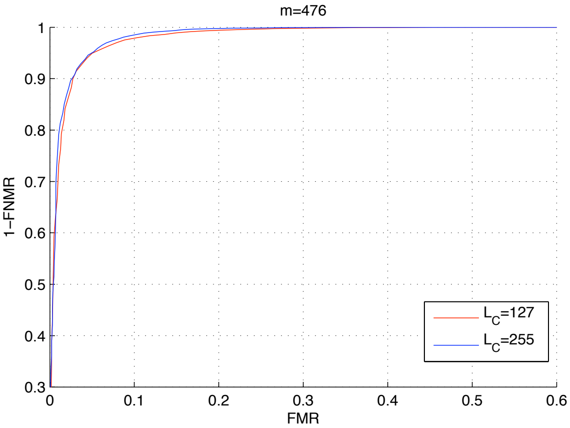


Figure 4.27.: ROC curves using *InS* at $m = 476$

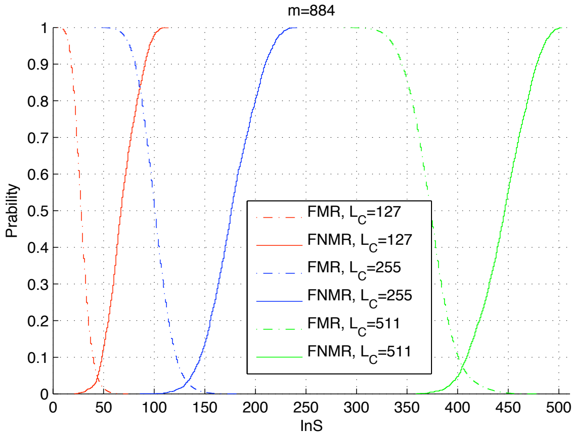


Figure 4.28.: *FMR* and *FNMR* over *InS* at $m = 887$

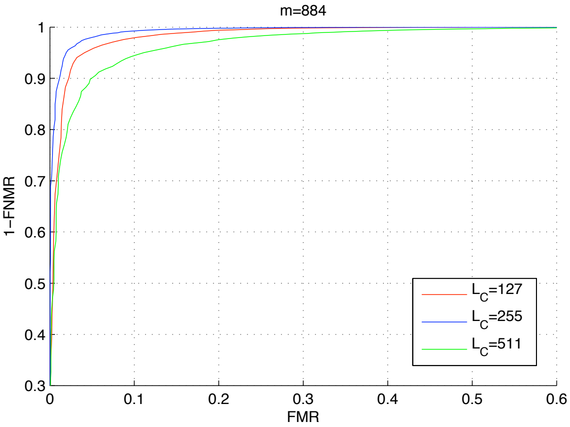


Figure 4.29.: ROC curves using *InS* at $m = 887$

At the same m, cross matching of two secure templates is possible, even if different codeword lengths are used. We denote L_{C1} as the codeword length used in one enrolment and L_{C2} as the codeword length used in the other enrolment. Figures 4.30 and 4.31 show the performance comparing R generated with different codeword lengths. Figure 4.30 shows that all intraclass *InS* stop at $\min\{L_{C1}, L_{C2}\}$. Figure 4.31 shows that the setting of $m = 884$, $L_{C1} = 127$, and $L_{C2} = 255$ gives the best performance. The performance of $m = 884$, $L_{C1} = 255$, and $L_{C2} = 511$ is similar to $m = 476$, $L_{C1} = 127$, and $L_{C2} = 255$. The setting of $m = 884$, $L_{C1} = 127$, and $L_{C2} = 511$ is the worst one. A large difference between L_{C1} and L_{C2} reduces the performance.

Figure 4.32 compares the performance of cross matching using R, the real-valued features and selected binary features. The performance of $m = 887$ is better than $m = 476$ in all the cases. Using $L_C = 255$ is also better

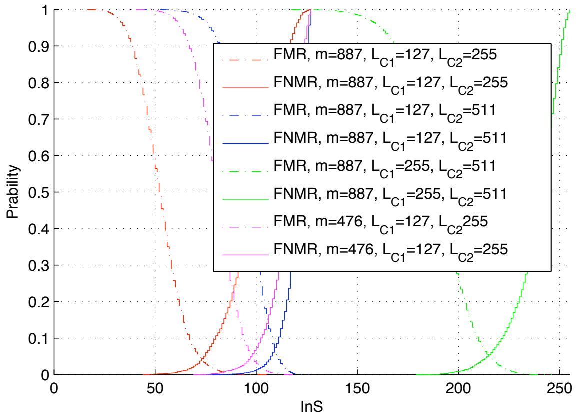


Figure 4.30.: *FMR* and *FNMR* over *InS* of different L_C

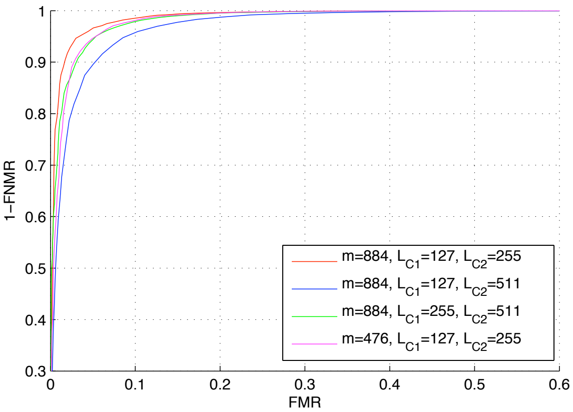


Figure 4.31.: ROC curves using *InS* of different L_C

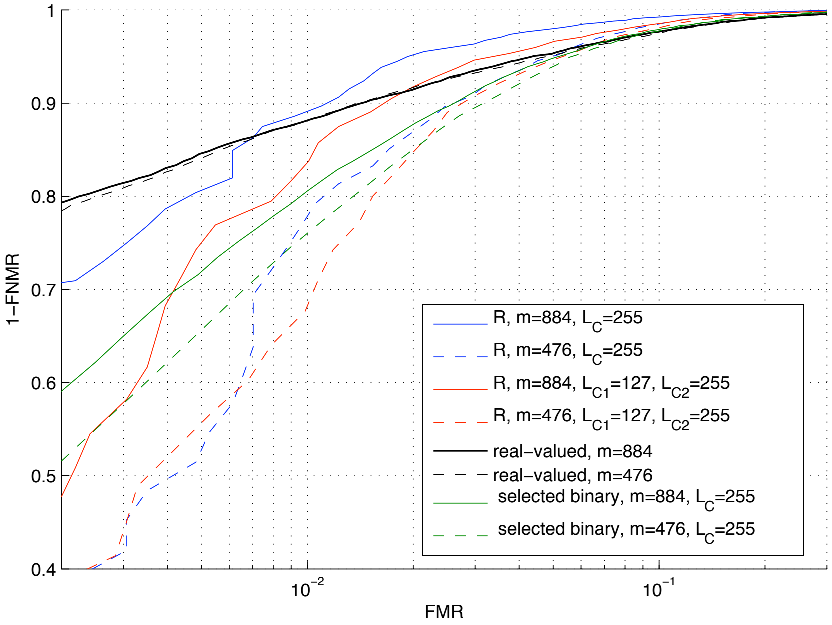


Figure 4.32.: ROC curves using *R*, real-valued features and selected binary features

than $L_C = 127$ or 511. In the region $FMR > 0.7\%$, the performance using R at $m = 884$ and $L_C = 255$ is the best and is even better than that of the real-valued features and the selected binary features. The performance of real-valued and binary features is obtained with 3 enrolled samples and 1 probe sample per comparison. The results using R are from two different enrolment sets, that is comparable with the scenarios using 3 enrolled samples and 3 probe samples in the normal recognition. Additionally, the same samples can be reused in other enrolments. Nevertheless, in the 3D face recognition algorithm, the reliability of individual features is not taken into account. This experiment shows that R contains significant information about the subjects and is very useful for cross matching.

In order to avoid cross matching with the position vector R, we can change feature selection strategy. For instance, the same bits can be chosen for all the subjects in such a way that the general performance is optimized. As a consequence, the performance of individual subject is not optimal and the performance will be reduced in comparison with the current selection method. Alternatively, we can reduce the dimension of the feature to the length of the error correction codeword. However if no position vector is used, fuzzy commitment is vulnerable to indistinguishability attack proposed in [STP09] and the XOR of auxiliary data W of the same subject is decodable. In this case, even if two auxiliary data are generated with different secret size but the same codeword length, this attack is still possible. As shown in Section B.2 the BCH codewords of a short secret length are a subset of the codewords of a long secret length.

As described in Section 4.2.2, the auxiliary data W contains privacy information and can be used to distinguish different subjects. Table 4.6 shows that the maximum InS_{intra} is always smaller than L_C. InS is the number of bits, which are selected in both enrolment processes. The selected features for the same subject are never totally identical and their Hamming distance can be very large due to the shifting of bit positions. Therefore, the indistinguishability attack is no longer feasible. We test this attack for two settings. At $m = 476$, $L_C = 255$, $L_S = 29$, and $L_E = 47$, there are 50.96% genuine subjects, which can not be recognized with the decoding method. At $m = 884$, $L_C = 255$, $L_S = 29$, and $L_E = 47$, it increases to 99.78%. There is no advantage in identifying a subject with the XOR of auxiliary data W. However, if we increase the number of samples used in enrolment, the bit selection becomes more and more stable. If the same reliable bits are selected in every enrolment, the indistinguishability attack of W might be possible.

Additionally since the selected reliable bits in enrolments are different, the secure templates of the same subjects contain the information about different feature part. Combining them can expose more information about biometric features.

4.4. Summary

In this chapter we developed a 3D face recognition system and integrated the fuzzy commitment scheme to protect 3D face features. We applied the evaluation framework on the protected system and assessed strictly its security and privacy performance.

The developed 3D face recognition algorithm uses the distribution of depth values of the face surface to characterize facial geometry. The algorithm is evaluated in the FRGC database. The intraclass variation of the resulting features is small. It enables a smooth integration of the fuzzy commitment scheme and it is easy to find appropriate a coding method. In the fuzzy commitment implementation, the BCH code is used and long secrets can be extracted. The recognition performance is only slightly degraded.

We analyzed the distribution of 3D face features and estimated the probability distribution with the second order dependency tree. The features are highly dependent and their entropy is calculated. Furthermore, we evaluated the security and privacy with information-theoretical metrics. The achieved security is much smaller than the secret size. Since not all the bits in a feature are used in fuzzy commitment, the complexity to retrieve a biometric feature is higher than guessing a secret. Additionally, high privacy leakage exists. Increasing secret size can improve both the security and irreversibility, meanwhile, privacy leakage can be reduced. The position vectors of the selected vectors contain personal identifiable information. Cross matching is possible and evaluated with the recognition performance. Linking the auxiliary data - the XOR of biometric features and codewords -

is infeasible, however, combining two different auxiliary data of the same subject can expose more information about biometric features.

The security of a fuzzy commitment scheme is strongly dependent on the entropy of the auxiliary data. The security can be improved by e.g. permutation of biometric features in such a way that the entropy of the auxiliary data increases. On the other hand, the security is influenced by the selection of binary features. During the feature selection, not only the reliability of features but also the entropy of selected features should be taken into account. Selection of less dependent features can improve the security.

With the evaluation framework, we are able to give a rigorous assessment of the system. We disclosed that the dependency of 3D face features reduces significantly security and privacy. Linkability is a serious problem and is hard to prevent with the current construction.

5. Evaluation of Template Protection for Iris Recognition

In this chapter we demonstrate the developed framework in a template protection system for iris recognition. We first give a brief introduction of iris recognition. Together with face and fingerprint, iris belongs to the biometric modalities recommended by ICAO for the use in biometric passports. Iris patterns contain rich information and enable reliable authentication. Iris features are extracted with an open source algorithm. The feature extraction algorithm used in this chapter is a revised version of the Gabor filter method proposed by Daugman, which is the most important iris recognition algorithm. Additionally, we implement the existing fuzzy commitment algorithm for iris recognition introduced by Hao. The main contribution of this chapter is to evaluate the protected iris recognition system. We analyze the distribution of iris codes and use a Markov model to describe the dependency of iris codes. Furthermore, we measure three protection goals of the protected system, namely security, privacy protection ability and unlinkability. Here we assume the advanced threat model. We also design a cracking algorithm to empirically quantify the complexity of retrieving iris codes. We compare the results of theoretical and practical assessments. A discussion on the possibility to improve the security and the boundary of security performance is given at the end.

5.1. Iris Recognition

5.1.1. An Overview of Iris Recognition

Iris is a part of the eye responsible for controlling diameter and size of pupils [NST06]. It is a biometric modality inside the body and visible from outside. In 1987, Flomand and Safir awarded a patent and proposed the idea of iris recognition. Later in 1994, Daugman awarded a patent with an automatic iris recognition algorithm [tag06]. Thereafter iris recognition technologies are more mature and widely used in border control, access control etc. Many airports in England and the Netherlands chose iris for quick crossing border [HO,Pri]. Due to ethics issues, iris recognition techniques are very popular in Arabian countries [DM04]. Nowadays, iris becomes one of the most important biometric modalities.

The iris appears between pupil and sclera as shown in Figure 5.1. It contains fine patterns and is suitable to distinguish individuals. Most iris capture devices use Near InfraRed (NIR) light in order to avoid reflection of cornea under visible light. After acquirement, the iris region is segmented from the image. Among different iris recognition methods, Daugman's Gabor filter based algorithm is the most common one [Dau03, Dau04]. In the iris detection process, an integrodifferential operator is calculated to find both the pupillary and the outer (limbus) boundaries[1]. Then the detected iris area in a polar coordinate system is projected onto complex-valued 2D Gabor wavelets. The resulting complex values represent the texture information of an iris. Only the phase information of every complex value is used and converted into 2 bits. The feature contains altogether 2048 bits (256 bytes).

[1] The centre of these boundaries is not always the same.

Additionally, a mask vector is generated, which indicates the iris region corrupted by eyelid, eyelash occlusion, specular reflection etc. During comparison, iris codes in the noisy region are not considered.

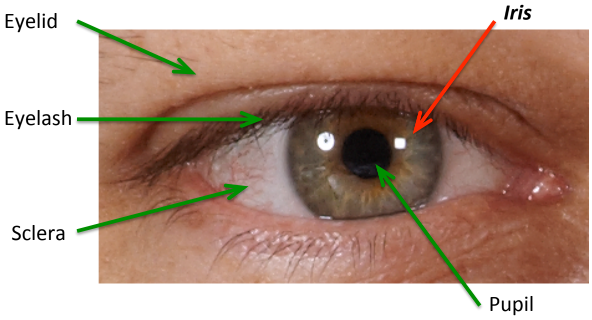


Figure 5.1.: Eye and iris under visible light

Moreover, Daugman analyzed the distinguishing power of the obtained iris features. Individual iris bits are uniformly distributed. The interclass distribution of Hamming distance obtained from 9.1 million comparisons fits perfectly a binomial distribution with $p = 0.5$ and $N = 249$. The entropy of iris features is empirically determined and equal to 249 bits.

Sun et al. proposed an alternative method using ordinal measure [STW04, ST09]. Ordinary measure is an efficient tool for texture classification. Multi-lobe differential filters (MLDF) are applied over iris regions and every filter has a special spatial meaning and represents point, line, edge, corner etc. Every resulting lobe is encoded with one bit according to its sign. This method provided a very good performance. Interestingly, the 2D Gabor wavelet can be seen as a special case of ordinal measure. However, the ordinal measure avoids transformation and is much more efficient than 2D Gabor wavelet. In the next section we show the recognition performance of iris recognition with an open source algorithm.

5.1.2. Experimental Results

Masek developed an open source iris recognition algorithm [Mas03]. The algorithm contains localization and segmentation, normalization, feature extraction and matching process. Figure 5.2 shows the block diagram of the algorithm and intermedian results of individual steps. An input iris image is captured with a NIR device as shown in the left of Figure 5.2. The color information is lost, however, no strong specular reflection occurs in the iris region. For iris localization and segmentation the Hough transformation is used, which is an efficient image analysis tool to detect shapes such as edges, circles, ellipses etc. The circular Hough transform is applied on an iris image to detect the boundaries of iris and pupil. Moreover, the linear Hough transformation finds the upper and lower eyelids. Additionally, the probable eyelid and specular reflection areas are marked black. The localization and segmentation result is depicted in the second left image in Figure 5.2. We denote $I(x,y)$ as the illumination value at pixel (x,y) in the grey level image. In the normalization process, Daugman's rubber sheet model is utilized to convert the iris ring $I(x,y)$ in a Cartesian coordinate system into rectangular form $I(\rho,\phi)$ in a polar coordinate system, where the difference between the centre of the iris and of pupil is taken into account during normalization.

During feature extraction, the 1D log-Gabor filter is applied to each row of the normalized iris region. Masek considered the spatial combination of 1D log-Gabor filters as 2D Gabor filter. In [Kov], it is shown that the log-Gabor filter has two advantages: log-Gabor functions have always zero DC component and they can describe

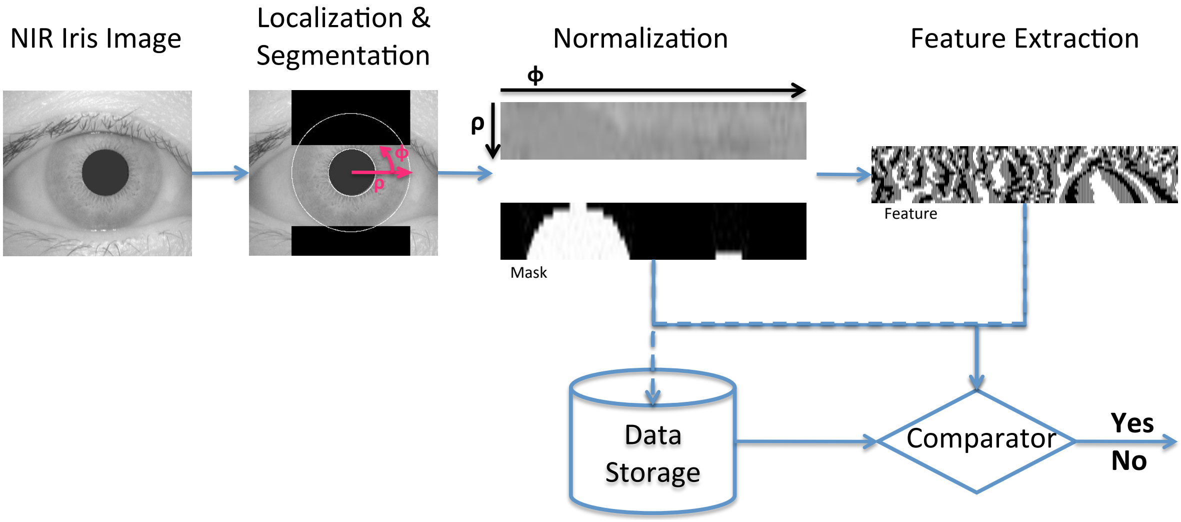


Figure 5.2.: The block diagram of Masek's iris recognition algorithm. (The iris image example is from CASIA-Irisv3 database [CAS])

high frequency regions better. The feature extraction works as follows:

$$F_i(\omega) = \mathcal{I}_i(\omega)G(\omega) \tag{5.1}$$

where i indicates the corresponding row in normalized iris region, $\mathcal{I}_i(\omega) = FFT(I(\rho_i, \phi))$ is the Fourier transformation of the 1D signal of $I(\rho_i, \phi)$ at a fix ρ_i, and $G(\omega)$ is 1D log-Gabor filter, expressed as:

$$G(\omega) = \exp\left(\frac{-[\log(\omega/\omega_0)]^2}{2[\log(\sigma/\omega_0)]^2}\right) \tag{5.2}$$

where ω_0 represents the centre frequency, and σ gives the bandwidth of the filter. The iris features are the sign of the real and imaginary parts of the frequency value after applying the Gabor filter:

$$\mathbf{b_i} = \left[sgn\left\{Re\{F_i\}\right\}, sgn\left\{Im\{F_i\}\right\}\right] \tag{5.3}$$

Every frequency is converted into 2 bits, which is corresponding to one of four quadrants in the phase space $[0, \pi/2), [\pi/2, \pi), [\pi, 3\pi/2), [3\pi/2, 2\pi)$.

The iris template consists of a binary code B and a mask vector Bm. The mask vector shows noisy positions in the iris code. During the enrolment, the template is stored in a data storage. In the verification, the stored iris template is compared with that of a queried iris image. The fractional Hamming distance is used in the comparator. Only the bits in the region which are marked as noiseless are used and the comparison function can be described with:

$$HD = \frac{||(B_1 \oplus B_2) \cap Bm_1 \cap Bm_2||}{||Bm_1 \cap Bm_2||} \tag{5.4}$$

where $[B_1, Bm_1]$ and $[B_2, Bm_2]$ are two iris templates, $||\cdot||$ denotes the Hamming weight, $\oplus$ is the XOR operator, $\cap$ is the Boolean AND operator. During the comparison, the enrolled template is shifted maximum 4 bits to the right and 4 bits to the left. The minimum fractional Hamming distance is returned. In this way the rotation of the eyes is compensated to a certain extent.

We applied Masek's implementation on CASIA-v1.0 and CASIA-Irisv3 [CAS] to generate iris features. We make no change of the original implementation. The CASIA databases were collected by the Chinese Academy of Sciences (CAS), Institute of Automation. CASIA v1.0 contains 756 iris images from 108 subjects captured with a CAS-self-developed iris camera. There are three subsets in CASIA-Irisv3, namely, CASIA-Irisv3-Interval, CASIA-Irisv3-Lamp and CASIA-Irisv3-Twins. The first subset was collected with the CAS-self-developed sensor and the other two were captured with the OKI IRISPASS-h sensor. In our experiments, only CASIA-Irisv3-Interval is used. It contains 2639 images with a resolution of 320 × 280, which are from 395 different eyes of 249 subjects. CASIA-Irisv3-Interval is a superset of CASIA v1.0. The pupil regions of all iris images in CASIA v1.0 were marked black in order to protect the NIR illuminator information of the capture devices due to the patent issue.

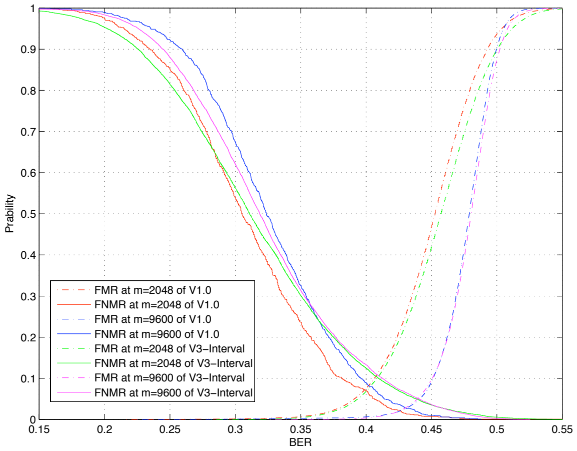


Figure 5.3.: *FMR* and *FNMR* at different m with CASIA databases

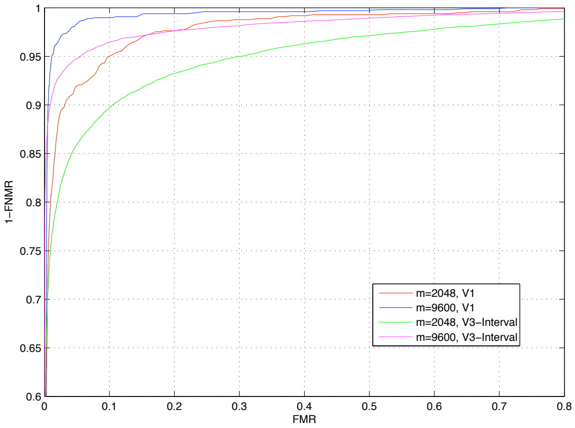


Figure 5.4.: ROC curves at different m with CASIA databases

DB	m	*EER*	@ *BER*
CASIA-v1.0	2048	7.20%	38.85%
CASIA-v1.0	9600	2.78%	43.04%
CASIA-Irisv3-Interval	2048	10.25%	40.87%
CASIA-Irisv3-Interval	9600	5.16%	43.96%

Table 5.1.: *EER* at different m and CASIA databases

Two different settings are tested. For the feature length $m = 2048$, the normalized squared iris region is divided into 8 rows and each row results in 128 1D-Gabor filter coefficients. Every coefficient is converted into 2 bits. For $m = 9600$, 20 rows and 240 coefficients are used. The performance of Masek's algorithm in CASIA-v1.0 and CASIA-Irisv3-Interval is shown in figures 5.3 and 5.4. Figure 5.4 shows that the performance of CASIA-v1.0 is better than that of CASIA-Irisv3-Interval at the same setting. CASIA-Irisv3-Interval contains more challenging iris images than CASIA-v1.0. Increasing feature length m can improve the performance significantly. Figure 5.3

shows that increasing m, the change of $FNMR$ is minor, but FMR is shifted strongly to the right. It indicates small variation of the robustness, but large improvement on the discriminative power. The EER and the corresponding BER are shown in Table 5.1.

The experiment with CASIA-v1.0 database and $m = 9600$ has the best performance. In the previous chapter it was shown that an EER of 5.90% is achieved in the 3D face recognition system at feature length of 804. The recognition performances of both systems are in a comparable level.

5.2. The Fuzzy Commitment Scheme for Iris Recognition

Iris texture is an epigenetic phenotypic characteristics in [DC01]. Even irises sharing identical genetic information have different appearances. Diseases such as free-floating iris cysts can change iris appearance. It is necessary to protect iris features for security and privacy reasons. Hao et al. proposed an algorithm combining cryptography with iris recognition, which is the milestone work in this area [HAD05]. Fuzzy commitment is the basic structure of the algorithm. In order to overcome high intraclass variation, Hao analyzed carefully error patterns of iris codes and applied a two-layer error correction method: Hadamard codes are used to correct random errors caused by acquisition devices or iris distortion; Additionally, Reed-Solomon codes compensate burst errors due to undetected eyelashes and specular reflections. Using this efficient error correction coding, a 140 bit long secret is achieved at FRR of 0.47% and FAR of zero. Furthermore, the security of the proposed scheme was studied regarding the complexity for an adversary to retrieve iris features. The discriminative entropy of iris codes is 249 bits. The coding scheme tolerates up to 27% bit errors. If an attacker knows the correlation properties of iris codes, at least 2^{44} computations need to be tried in an exhaustive search. Hao also suggested a three-factor scheme including biometrics, token and additional passwords, in order to achieve higher security. This system is sufficient for practical use because of the high security and good user convenience.

In [BCC*07], Bringer et al. used the product codes and a two-dimensional iterative min-sum decoding algorithm in the error correction process. They modeled errors between reference and queried iris codes with a binary symmetric channel (BSC) with erasure. A two-dimensional product code is used, where every column and row are a codeword of a linear code. In order to handle burst errors, an interleaver is applied to break the burst errors. During verification, an iterative minimum method is exploited. They showed that the results are close to the theoretical limit of the ideal BSC coding according to Shannon's information theory, which is based on the assumption of independently distributed iris codes. In [VDRY09], Vetro et al. used the syndrome coding to protect iris codes. From the extracted iris codes, only 1806 most reliable bits are utilized. The syndrome of iris features is calculated with the low density parity coding. In the verification, the decoding process uses a belief propagation process. The security of 50 bits can be achieved at $FNMR$ of about 15%, which is comparable with $FNMR$ of the unprotected system.

Iris features are binary vectors and are suitable for the fuzzy commitment scheme, however, the challenge is to correct large amount of intraclass bit errors. In this work we implemented the two layer coding scheme proposed by Hao [HAD05]. Figure 5.5 shows the block diagram. In the enrolment a randomly generated secret S is first encoded with Reed-Solomon (RS) encoder and then with Hadamard encoder. The codeword is XOR-ed with the input iris feature X. The stored secure template consists of the XOR-output W and the hash of the secret $h(S)$. Binary iris features with length of e.g. 2048 fit the code length of many coding methods. In comparison with the 3D face method shown in Section 4.2, neither additional binarization nor selection of the most reliable bits is necessary. During verification, the probe iris feature is XOR-ed with the stored W and a corrupted codeword C' is obtained. By the Hadamard decoder and RS decoder, the errors are corrected. The hash of the estimated secret S' is compared with the stored $h(S)$. If they are identical, a positive result will be given.

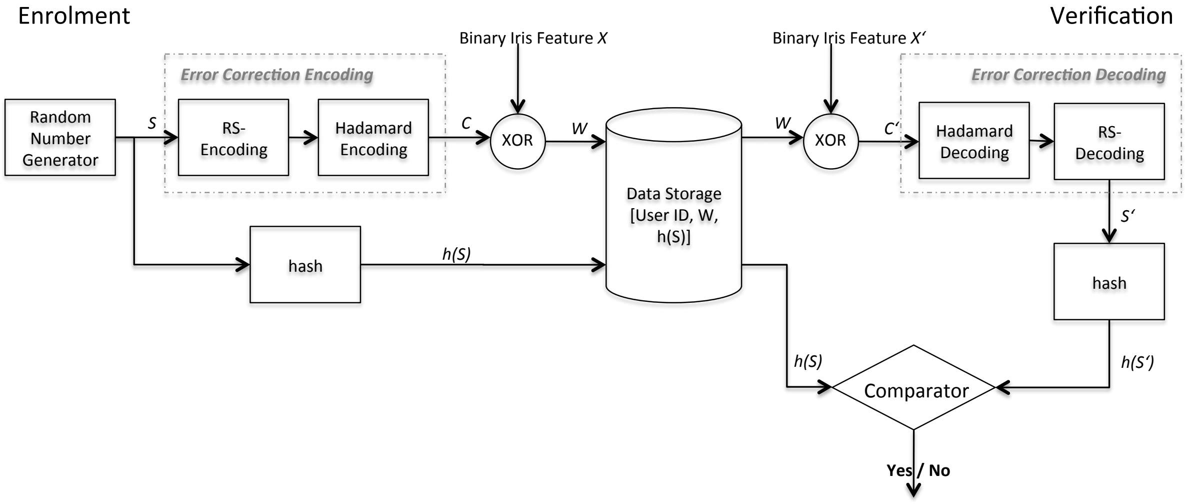


Figure 5.5.: The block diagram of the implemented iris fuzzy commitment algorithm proposed by Hao

The RS code is computed in Galois field $GF(q)$, where $q = 2^u$ and u is a positive integer. An RS code consists of k message symbols and $2t$ parity symbols, where t is the number of correctable symbol errors. Its minimum Hamming distance is $2t+1$. The length of the RS code is not larger than $2^q - 1$. The Hadamard code is a $(2^{l-1}, l, 2^{l-3} - 1)$ binary code[2]. The details of RS code and Hadamard code are shown in Appendixes B.2 and B.3.

Figure 5.6 depicts the coding scheme in details. The L_S bit secret is divided into m_S blocks and each block is l bit long as shown in the first row in Figure 5.6. The RS encoder adds $2t_{RS}$ parity blocks at the end of the secret blocks (see the second row), where t_{RS} is the number of the correctable block errors in an RS code. Then Hadamard encoder extends each block into a 2^{l-1} bit Hadamard code. In the original paper [HAD05], Hadamard code of $(64,7,15)$ and RS code of $(32, m_S, t_{RS})$ are used. Different settings of $m_S \in [6,8,10,\cdots,32]$ are tested. With the database used in their experiment, an FAR of zero can be achieved at $L_S \geq 140$ $(m_S = 20)$ and the minimum FRR of 0.47%.

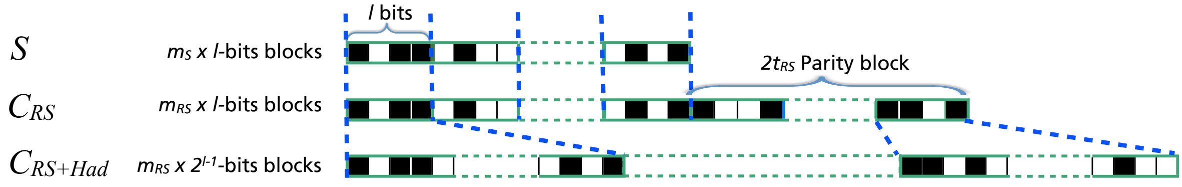


Figure 5.6.: The coding scheme used in the iris fuzzy commitment algorithm proposed by Hao

[2] In this chapter, we denote an error correction code as a (n,k,t) code, where n is the codeword length, k is the number of message bits, and t is the number of correctable bit errors. For instance, in this case, the length of Hadamard codeword is 2^{l-1}, the corresponding message contains l bits and it can tolerate $2^{l-3} - 1$ bit errors.

In our experiment we use the features extracted with Masek's Gabor filter algorithm from the CASIA databases. The fuzzy commitment algorithm is implemented according to Hao's method. Table 5.2 shows the settings with different coding parameters and feature lengths. The Hadamard codeword lengths of $L_{Had} = \{64, 128\}$ are tested, which allow to correct $(2^{n-2} - 1)/2^n \approx 25\%$ bit errors in each Hadamard block. Different numbers of message blocks are also tested in order to change robustness to block errors.

m	9600				2048				
L_S	24	40	56	72	14	16	32	48	64
l	8	8	8	8	7	8	8	8	8
L_{Had}	128	128	128	128	64	128	128	128	128
m_S	3	5	7	9	2	2	4	6	8
m_{RS}	75	75	75	75	32	16	16	16	16
t_{RS}	36	35	34	33	15	7	6	5	4

Table 5.2.: The settings of different coding parameters and feature lengths: m is the feature length, $L_S = m_S \times l$ is the secret length, l is the number of message bits of a Hadamard code, $L_{Had} = 2^{l-1}$ is the Hadamard codeword length, m_S is the number of message blocks in a RS code, m_{RS} is the block length of a RS codeword, and t_{RS} is the number of correctable block errors.

DB	m	L_S	With Mask				Without Mask			
			CER^*_{intra}	CER^*_{inter}	$FNMR$	FMR	CER^*_{intra}	CER^*_{inter}	$FNMR$	FMR
CASIA v1	9600	24	35.67%	50.76%	17.80%	1.59%	36.88%	49.68%	47.43%	0.21%
		40	35.04%	39.51%	19.96 %	0.86%	36.88%	34.78%	49.59%	0.17%
		56	34.54%	32.89 %	21.30%	0.69%	-	-	-	-
		72	34.05%	32.89%	22.74%	0.59%	-	-	-	-
	2048	14	38.67%	51.61%	15.33%	4.86%	41.55%	55.71%	36.73%	1.81%
		16	40.23%	49.41%	10.60%	6.65%	47.46%	56.49%	28.19%	1.49%
		32	36.42%	42.68%	16.56%	3.38%	39.55%	48.68%	41.67%	0.30%
		48	34.13%	35.11%	23.66%	1.80%	38.19%	38.67%	53.19%	0.20%
		64	32.67%	32.96%	34.57%	0.96%	-	-	-	-
CASIA Interval v3	9600	24	44.49%	50.61%	36.29%	0.15%	47.86%	52.97%	47.22%	0.05%
		40	43.46%	32.74%	39.33%	0.08%	45.88%	0	51.21%	0
		72	39.40%	31.43%	43.10%	0.04%	-	-	-	-
	2048	14	46.53%	55.52%	32.50%	2.89%	51.46%	59.28%	41.92%	1.50%
		16	48.39%	54.98%	24.36%	3.61%	52.78%	56.84%	32.30%	1.10%
		32	42.50%	42.19%	35.22%	1.35%	49.85%	47.41%	46.16%	0.11%

Table 5.3.: The recognition performance and the maximum correctable intraclass and interclass bit error rates

The experimental results are shown in Table 5.3. The coding scheme can correct both block errors and bit errors. The maximum number of correctable bit errors, which can be achieved theoretically, may not represent the true error correction ability for this application. We denote CER_{intra} as Correctable bit Error Rate of the intraclass comparisons and CER_{inter} as the one of the interclass comparisons. We empirically measure $CER^*_{intra} = \max\{CER_{intra}\}$ and $CER^*_{inter} = \max\{CER_{inter}\}$, which show roughly the error correction ability at different settings. Obviously, whether the bit errors can be corrected or not, depends on their pattern. Therefore, the maximal correctable bit error rates are not comparable with the threshold of the Hamming distance comparator used in iris recognition.

In the setting with mask, an iris code is firstly XOR-ed with its mask vector before sent to the enrolment or the verification process of fuzzy commitment. In the setting without mask, an iris code is used directly and its mask information is ignored. Mask vectors can filter noisy and invalid regions in an iris code. In CASIA v1 database, the *FNMR* with mask reduces to less than the half of the *FNMR* without mask. In CASIA interval v3 database, the reduction of *FNMR* is about 10% with mask. Meanwhile, *FMR* increases slightly, if the mask is used. Although the mask is not stored, applying the mask can decrease the security of the algorithm. Later in Figure 5.9, it is shown, that appearance of the mask region is quite static and can be predicted. It can provide significant information about the secret to an adversary. Therefore, we do not recommend using mask information for the sake of the security, if *FNMR* is within an acceptable range. Unfortunately, this is not the case in our experiments.

As in other fuzzy commitment algorithms, *FNMR* increases and *FMR* decreases with increasing L_S. Different L_S are used for $m = 9600$ and $m = 2048$. Their recognition performance can not be compared directly. However, we still can see that the results of $m = 9600$ are better than $m = 2048$ in CASIA v1. For instance, lower *FNMR* and *FMR* are achieved at $m = 9600$ and $L_S = 72$ in comparison with the results of $m = 2048$ and smaller $L_S = 64$. The *FNMR* of CASIA v1 is much better than that of CASIA interval v3 at the same setting. The *FMR* of CASIA v1 is only slightly worse than that of CASIA interval v3. The similar results are also observed in the iris recognition experiment without template protection (see Section 5.1.2 and Figure 5.3). $L_S = 14$ is the only setting with $l = 7$ and the corresponding Hadamard block length is 64, which is the half of the block length used

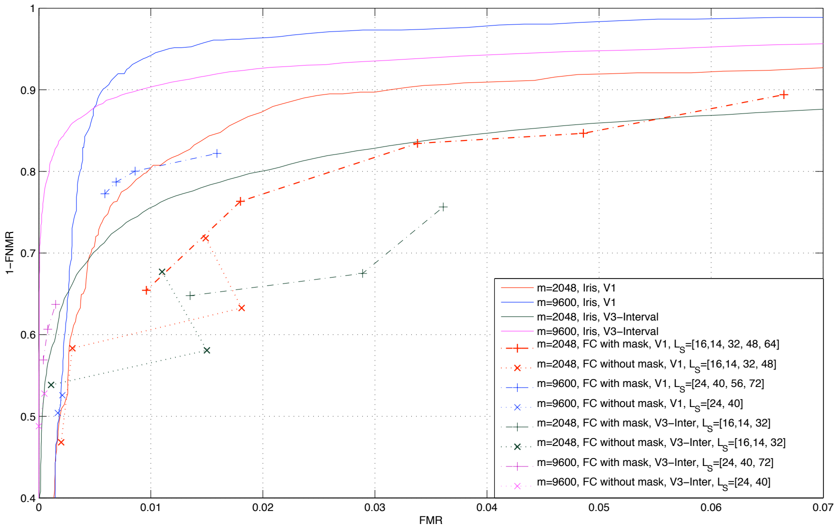


Figure 5.7.: The recognition performance of iris recognition and the fuzzy commitment system: the solid lines are ROC curves of the iris recognition; the lines with markers plot *FMR* and $1 - FNMR$ of the fuzzy commitment system; the dash-dotted lines with plus are the ones of the fuzzy commitment system with mask; the dotted lines with cross are the ones of the fuzzy commitment system without mask; the color shows different feature size $m = \{2048, 9600\}$ and the database (CASIA v1 or CASIA Interval v3);

in other settings. Comparing it with $L_S = 16$, the $FNMR$ of $L_S = 14$ is much worse. Therefore, we choose the block length 128 in the rest of the experiments.

We depict the operational points of the fuzzy commitment system as well as the ROC curves of the original iris recognition in Figure 5.7. In Hao's paper [HAD05], they did not compare the performance of the original iris recognition and fuzzy commitment, because the perfect performance was achieved with fuzzy commitment. However, in our experiments, the performance is far from optimal. We can observe strong performance degradation and all the operational points are below the ROC curves with the same database and feature length. The operational points at the settings without mask are concentrated in the area of low FMR and high $FNMR$. The operational points of the settings with mask show a better trade-off between FMR and $FNMR$. We do not achieve the perfect performance as well as the high secret size as shown in [HAD05]. The secret size in our experiment is limited by the poor recognition performance of the input binary iris features. If the feature extraction algorithm is improved and iris codes are more reliable, both secret size and the recognition performance can be enhanced significantly.

5.3. Privacy and Security Assessment

In this section we investigate the security and privacy of the protected iris recognition system, which is implemented in the previous section. We analyze the statistical properties of iris features. It includes the distribution of intraclass and interclass bit errors, the position of mask region, and the distribution of the iris codes. Later we evaluate the system regarding the three protection goals. Here we assume the *advanced threat model* that an adversary has full knowledge about the system as well as the statistical properties of biometric features. A cracking algorithm to retrieve the secret and iris codes is proposed, which utilizes the security weakness of the system.

5.3.1. Statistical Properties of the Iris Features

The distribution of iris codes plays an important role in privacy and security assessment and is useful prior information for an adversary. In the existing work of Daugman [Dau03], the statistical properties of the iris codes using Gabor filter were investigated with a large database. It is shown that their iris codes contain 249 bit entropy. Since a similar feature extraction algorithm is used in Masek's implementation, we will perform the same analysis on the extracted iris codes.

In the original method of Daugman, the iris codes are uniformly distributed, that an iris bit is equal to zero or one is identically probable. We randomly select one sample from each subject and calculate the interclass mean at every bit position. The bits in the mask region are not taken into account. For a uniform distribution, the interclass mean is expected to be 0.5 (see also the uniform test in Section 4.3.1). Figure 5.8 depicts the interclass mean of individual feature elements for CASIA databases: y-axis shows the number of rows divided in the normalized iris region and x-axis indicates the number of iris bits derived from each row; the color indicates the mean value. If iris features are uniformly distributed, the images in Figure 5.8 would appear light blue for $m = 9600$ or light green for $m = 248$. The colors at many bit positions appear red, orange or dark blue. It indicates that the corresponding bits are not uniformly distributed. Additionally, the spacial correlation of mean values can be observed in vertical direction. The feature of $m = 2048$ has stronger non-uniformity than those of $m = 9600$. As a conclusion, interclass distribution of iris codes can *not* be considered as uniform.

We look at the distribution of mask region, namely the probability that an iris bit is detected as corrupted. We collect all the mask vectors and compute their average, which correspond to the empirical probabilities. The

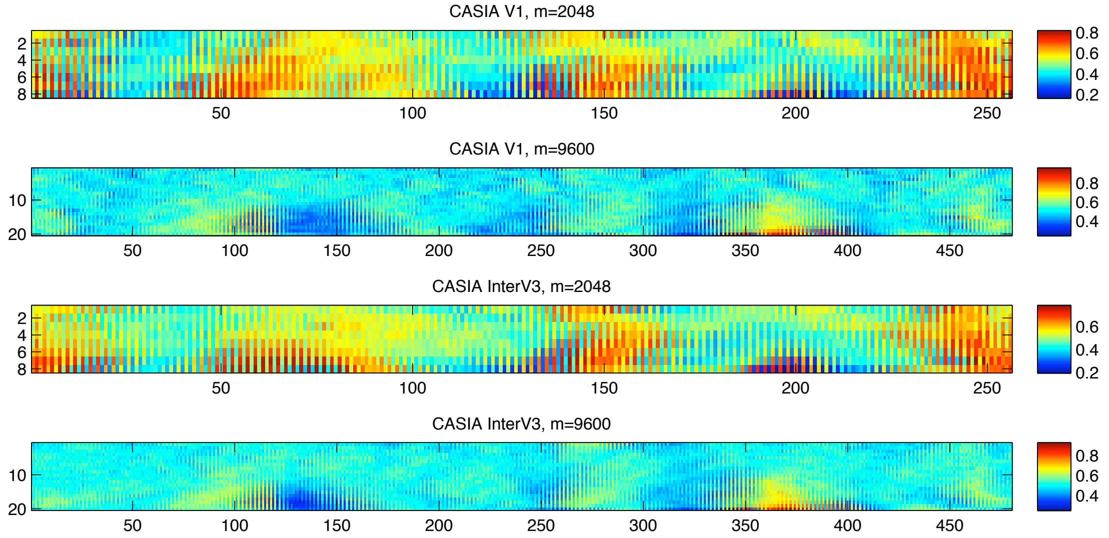


Figure 5.8.: Interclass means of iris features of CASIA databases

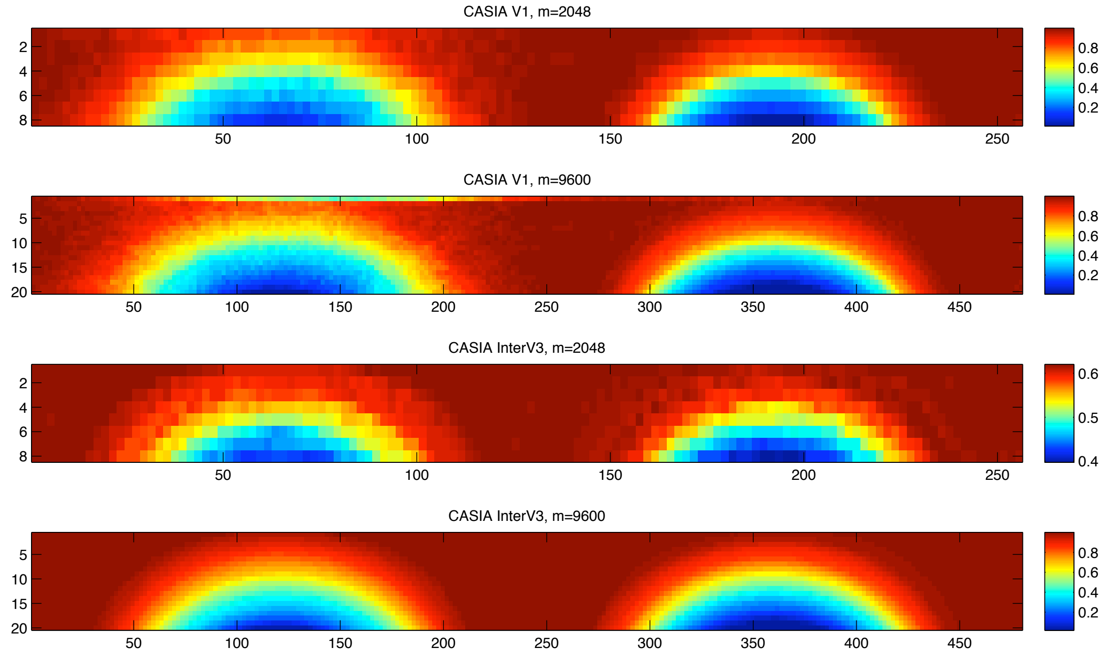


Figure 5.9.: The probability of mask region

result is depicted in Figure 5.9. The dark red region is with high probability marked as valid iris region and the dark blue region is normally marked as invalid region. Two circular sector regions can be recognized obviously and they are caused by eyelids. Most of iris codes outside these sectors are considered as valid. Recall that RS code is used in the fuzzy commitment scheme as shown in Section 5.2. This code is used to correct the burst errors occurring in the iris codes. However, Figure 5.9 shows that the corruption of iris codes does not occur uniformly. It is down to the effect, that obstruction of eyelids is normally on the upper and lower parts of an iris. *We argue that RS coding is not the best choice for these iris codes.*

We also analyze the distribution of intraclass errors. During a comparison, shifting of queried iris codes maximum 4 bits to left and right is used. The error pattern with the minimum Hamming weight is counted. We calculate the error probability at each bit position. The erasures, which are calculated with at least one invalid bit, are not considered. The result is shown in Figure 5.10. The error probability varies from zero (the dark blue color) to one (the dark red color). A light blue green region in a sector form can be recognized on the left side of the first and second images. Similarly a sector region with relatively high noise in red and yellow red color can also be observed on the left of the third and fourth images. These regions correspond to the upper part of iris ring. Generally the lower part of the iris codes has less errors than the upper part. The upper part of iris ring is easily distorted by eyelashes and the error probability is also higher. There is also dark blue appearing on the right of the images in Figure 5.10 (e.g. in the region of $x = [180, 190]$ and $y = [7, 8]$ of CASIA V1, $m = 2048$), which corresponds to the lower part of iris ring. These bits look very stable, because no or very few intraclass errors are observed in this region due to erasures. Therefore, its error probability estimation is not confident. Additionally, the upper part of iris codes has smaller error probability than the lower part. For instance, the region of $y = [1, 5]$ in the first plot of Figure 5.10 for CASIA V1, $m = 2048$ is bluer than the region of $y = [6, 8]$. It means that iris region close to the sclera is noisier than that close to the pupil. Moreover, comparing the error probability of CASIA interval v3 database, the setting of $m = 9600$ is more reliable with less intraclass errors than that of $m = 2048$.

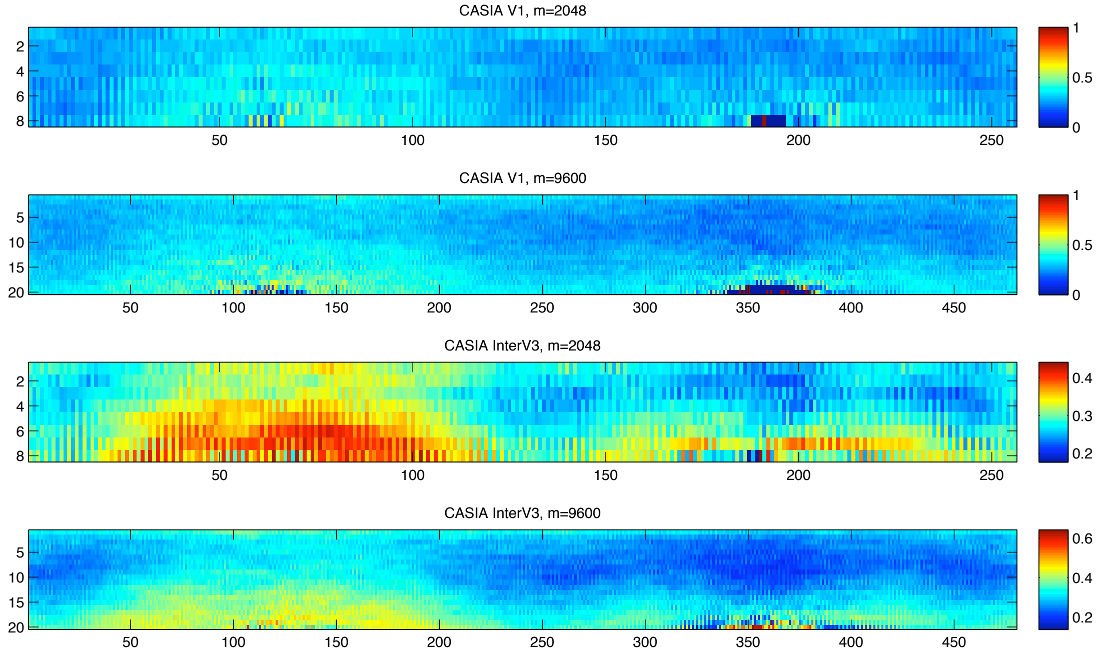


Figure 5.10.: The probabilities of intraclass errors at each bit position

m	2048		9600	
Database	CASIA v1	CASIA Interval v3	CASIA v1	CASIA Interval v3
$\mathbb{E}\{BER_{inter}\}$	0.4506	0.4555	0.4763	0.4780
$var\{BER_{inter}\}$	12.252×10^{-4}	13.019×10^{-4}	4.845×10^{-4}	4.593×10^{-4}
$\frac{0.25}{var\{E_{inter}\}}$	204	192	516	544

Table 5.4.: The statistics of BER_{inter}

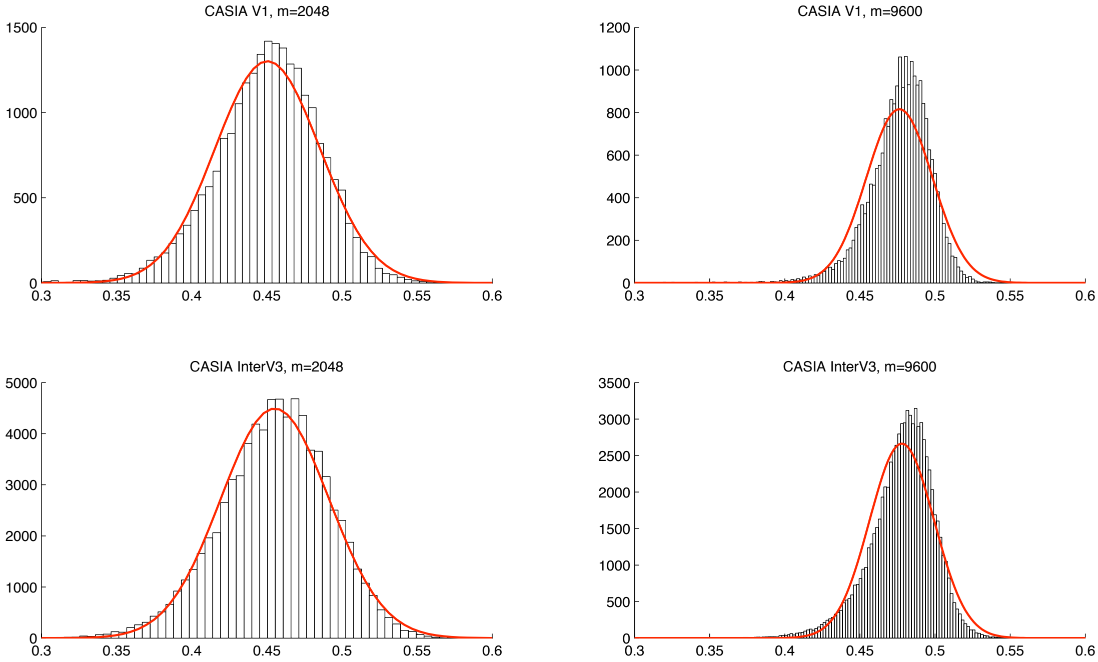


Figure 5.11.: The histogram of interclass BER (black bar) and the ideal binomial distribution with the same mean and variance (red line)

The interclass distribution determines the discriminative power of biometric features. In [Dau03], Daugman showed that the interclass bit errors in their experiments are perfectly binomially distributed. It is proved with a quantile-quantile plot. The observed cumulative distribution of interclass distance is plotted against the ideal cumulative binomial distribution and they lie on a line. He assumed that iris features were derived from a uniformly Bernoulli-distributed source. Then the entropy of iris codes can be calculated with the following equation:

$$H(X) = H(BER_{inter}) = \frac{0.25}{var\{BER_{inter}\}} \tag{5.5}$$

where X is an iris code, BER_{inter} is interclass bit error rate of iris codes and $var\{\cdot\}$ is the variance. The equation is deduced from Eq A.23 and A.25 (see the details in Appendix A.3). It shows the number of independent bits (trials) in the Bernoulli distribution. The 2048 bit long iris code contains 249 bit discriminative entropy.

We apply the similar experiments on our iris features. Table 5.4 shows the statistical results. The expected value of BER_{inter} is not 0.5. It confirms the previous observation that these features are non-uniformly distributed (see Figure 5.8). The variance for $m = 2048$ is much larger than for $m = 9600$. The longer features contain more discriminative information about the iris and the variation of interclass bit error rate is also smaller. Additionally, we display the histogram of the interclass BER_{inter} (black bars) as well as the ideal binomial probability density function with the same mean and variance (red lines) in Figure 5.11. The empirical distributions are skewed to the left and are quite different than the ideal binomial distributions. The assumption and entropy estimation made by Daugman is not valid in this experiment. The reason is the use of different databases and feature extraction algorithms. In our experiments, 23,219 different interclass comparisons of CASIA v1 and 77,814 of CASIA Interval v3 database are performed, which are much smaller than the 9,060,003 comparisons used in Daugman's experiment.

Since the existing model is *not* suitable in our experiment, I start with my own analysis. Every phase of Gabor filter coefficients is converted into two bits. They represent local properties of the iris texture. It is well known that spatial dependency exists in nature images. It inspires me to investigate the properties of iris codes with *Markov model*.

Given X is a 2D binary iris code and each row of X corresponds to the phase information of Gabor filtering of an iris ring with a fix radius to the central of the pupil (see Figure 5.2 in Section 5.1.1). As shown in Eq 5.3, the phase of every complex value of Gabor filtering results is converted into two bits. Therefore, we use four states $\mathcal{Z} = \{Z_i | i \in GF(4)\} = \{[00], [10], [11], [01]\}$ and denote X as a matrix in $\{\mathcal{Z}\}^{m_r \times m_c}$:

$$X = \begin{bmatrix} z_1^1 & \cdots & z_1^{m_c} \\ \vdots & \ddots & \vdots \\ z_{m_r}^1 & \cdots & z_{m_r}^{m_c} \end{bmatrix} \tag{5.6}$$

where $z_u^v \in \mathcal{Z}$, m_r and m_c are the number of rows and columns, GF stands for Galois Field. The length of binary iris codes is $m = 2 \times m_r \times m_c$. For $m = 9600$, $m_r = 20$; for $m = 2048$, $m_r = 8$.

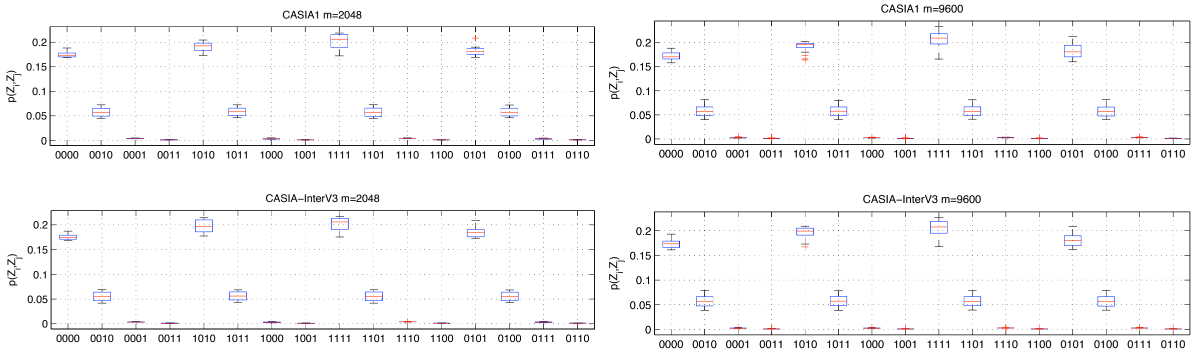


Figure 5.12.: Boxplots of the probability $p(z_u^v = Z_i, z_u^{v+1} = Z_j)$ at different settings

We calculate the joint probabilities of two successive elements in each row. Figure 5.12 shows the boxplots of $p(z_u^v = Z_i, z_u^{v+1} = Z_j)$ at different settings. The four patterns of $[Z_i, Z_i]$, namely $z_u^v = z_u^{v+1}$, have obviously much higher probabilities than others. The pattern $[Z_i, Z_{i+1}]$ is the second most frequently occurring one. It happens rarely that $z_u^v = Z_i$ and $z_u^{v+1} = Z_{i+2}$ or Z_{i+3}. This complies with the typical Markov property and it is observed at all the settings with different feature sizes and different databases.

Additionally, the variation of $[Z_i, Z_{i+2}]$ and $[Z_i, Z_{i+3}]$ is very small. $[Z_i, Z_{i+1}]$ has larger variation and their boxplots with different i are very similar. The variation of $[Z_i, Z_i]$ depends on i, but they are very similar for the same i with different settings. For instance, $[11, 11]$ is highly probable than others and has large variation.

We determine $p(Z_i, Z_j)$ with the mean of the estimation from all four different settings. Based upon this, the state probability $p(Z_i)$ can be calculated with Eq A.3, meanwhile the transition probability $p(z_u^v = Z_i | z_u^{v+1} = Z_j)$ can be derived with Bayesian rule as shown in Eq A.2. The resulting state and transition probabilities are shown in Table 5.5. The state probabilities are almost equal, $p([00]|[00])$ is slightly smaller and $p([11]|[11])$ is slightly larger than others. The transition probabilities on the diagonal in Table 5.5 are larger than 74% and are considerably higher than others. The probabilities $p(z_u^v = Z_{i+1} | z_u^{v+1} = Z_i)$ are larger than 21%. The probabilities $p(z_u^v = Z_{i+2} | z_u^{v+1} = Z_i)$ are the smallest.

Z_i	State Probability	Transition Probability $p(z_u^{v+1} = Z_i \| z_u^v = Z_j)$			
	$p(Z_i)$	$p(Z_i\|[00])$	$p(Z_i\|[10])$	$p(Z_i\|[11])$	$p(Z_i\|[01])$
[0 0]	23.51%	**74.08%**	1.072 %	0.40%	*23.42%*
[1 0]	25.64%	*24.26%*	**76.08%**	1.27%	0.38%
[1 1]	26.53%	0.42%	*22.47%*	**76.75%**	1.19%
[0 1]	24.32%	1.23%	0.38%	*21.58%*	**74.95%**

Table 5.5.: The state and transition probabilities of iris codes

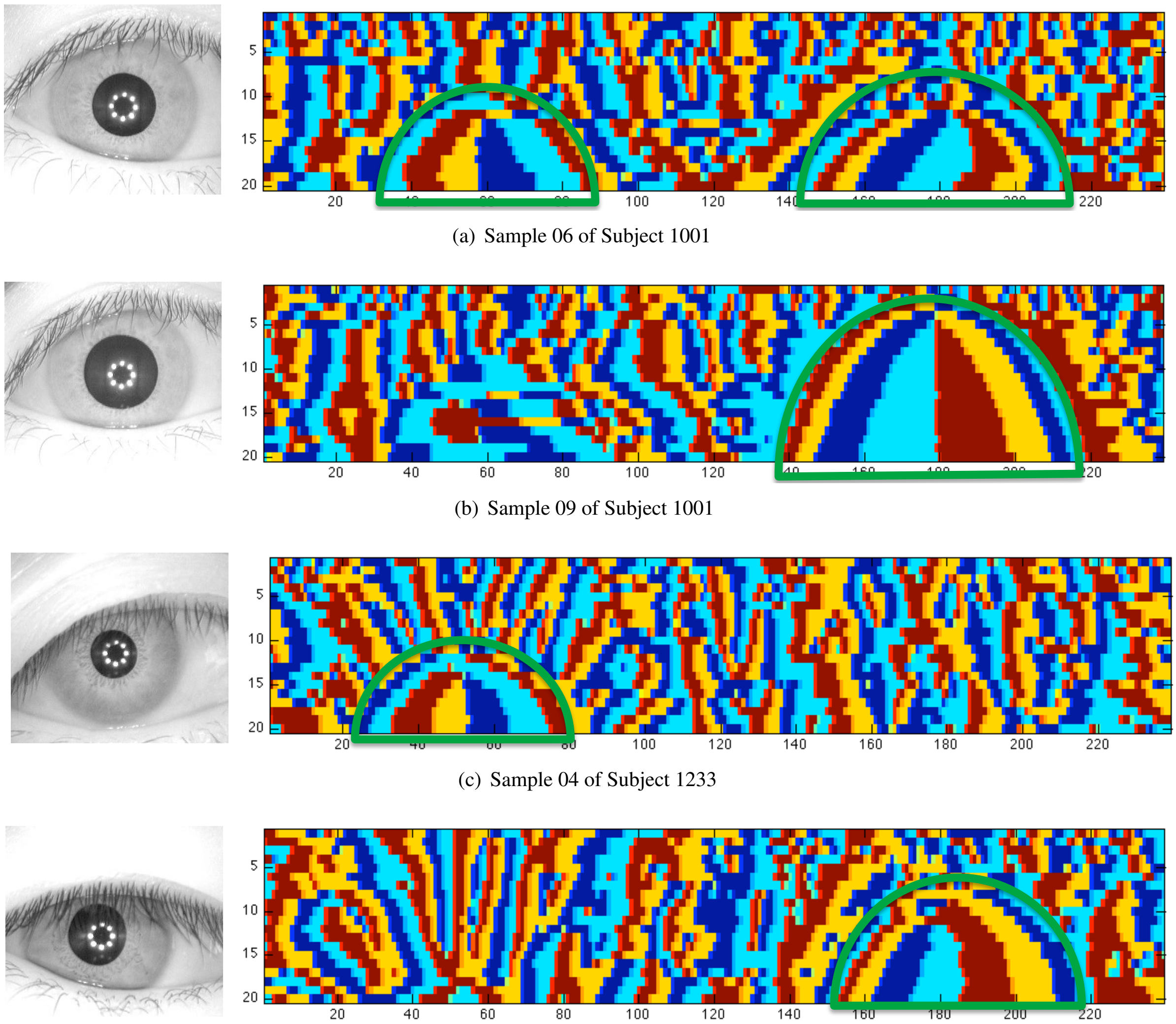
We choose 4 samples from CASIA interval v3 database and represent their iris codes with $[Z_i, Z_j]$ patterns in Figure 5.13. Instead of binary images, iris codes are depicted with 16 different colors. Most of the regions appear mark blue ($[00, 00]$), light blue ($[10, 10]$), red ($[11, 11]$) and yellow ($[01, 01]$). From left to right, the iris codes change in the order of blue→light blue→red→yellow. Small transition areas with the color representing $[Z_i, Z_{i+1}]$ can be recognized between the area of $[Z_i, Z_i]$ and $[Z_{i+1}, Z_{i+1}]$. The patterns $[Z_i, Z_{i+2}]$ and $[Z_i, Z_{i+3}]$ happen rarely and appear randomly. We also mark special patterns in sector form with green curves. Comparing with the iris images on the left, these patterns are derived from the upper and lower eyelids. In these regions, the $[Z_i, Z_i]$ patterns repeat longer and produce large areas in dark blue, light blue, red and yellow. The color patterns in the left sectors (red→yellow→blue→ light blue) and the right sectors (blue→light blue→red→yellow) are different. It seems that the upper eyelid has π-phase shift than the lower eyelid. However, it is not always the case that a sector can be observed. For instance, on the left side in b) and d) of Figure 5.13, such a sector is expected due to the distortion of the eyelids. However, they do not occur on the figures. If the occlusion of eyelid is just under or above the iris, a symmetric structure can be observed inside the sector region (e.g. the sector in a)). The $[Z_i, Z_j]$ patterns are very helpful to analyse the properties of iris codes.

Due to the disturbance of eyelids and eyelashes, it is difficult to evaluate the stationarity and ergodicity of iris codes. Here we make *assumption* that iris codes are *stationary and ergodic* and propose the *Markov model* to describe the distribution of iris codes. The Markov diagram is shown in Figure 5.14. The blue circles show the state $Z_i \in \mathcal{Z}$ for $i \in GF(4)$. With high probability, the adjacent iris elements are the same or change anti-clockwise as the solid blue line shown. With much lower probability, the iris bits change clockwise and with extremely lower probability they change in the diagonal directions. The derived Markov model is quite stable, since the probability estimation of $p([Z_i, Z_j])$ is almost invariant with different databases and feature lengths.

The information rate $H(Z) = 0.901$ of iris code is calculated with Eq A.30. It is much smaller than 2 bits in the case of uniform independent distribution. With Eq A.12, the chain rule of joint probability and Markov properties, the entropy of a Markov sequence can be written as:

$$\begin{aligned} H(Z_1, Z_2, \cdots, Z_n) &= H(Z_1) + H(Z_2|Z_1) + \cdots + H(Z_n|Z_{n-1}) \\ &= H(Z_1) + (n-1) \cdot H(Z) \end{aligned} \tag{5.7}$$

Then the estimated entropy of the iris code $\hat{H}(Z_1, \cdots, Z_{1024}) = 923.72$ for $m = 2048$ and $\hat{H}(Z_1, \cdots, Z_{4800}) = 4325.88$ for $m = 9600$.



(a) Sample 06 of Subject 1001

(b) Sample 09 of Subject 1001

(c) Sample 04 of Subject 1233

(d) Sample 02 of Subject 1223

Figure 5.13.: Iris images from CASIA interval v3 and their iris codes represented with transition patterns

Additionally, the iris entropy derived from Markov model is *quite different* from Daugman's estimation. Despite the differences in the Gabor filter implementation, preprocessing as well as the iris databases, the main

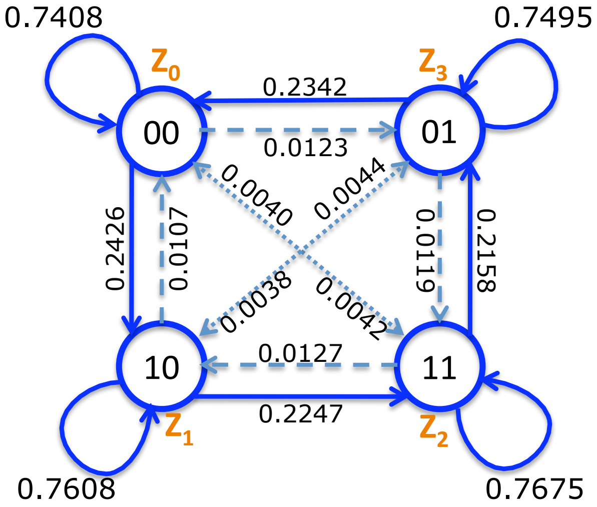


Figure 5.14.: Markov model of iris features

reason is that *only* the horizontal dependency of the adjacent states is analyzed. We investigate only horizontal dependency because of 1D-Gabor filter used in the iris feature extraction. From the examples in Figure 5.13 we can see that the vertical dependency also exists. Moreover, the high order dependency, namely dependency between the second, the third, even higher adjacent states, might also exist. Assumed that Daugman's iris features are also stationary and ergodic, the information rate of his iris codes per elements is $249/2048 \times 2 = 0.2432$, which is much smaller than that obtained in our experiment. If the estimation of the iris code distribution of iris codes can be improved with more general models, for instance, with context-tree weighting [WST95], it can be expected that the entropy of our iris codes reduces and even converges to Daugman's result.

The Markov property of the iris codes is *not a coincidence*. Gabor filters describe the local texture of iris patterns. Due to the inherent dependency in nature image, the adjacent regions can have the same or similar Gabor filter coefficients. It explains the transitions of the Markov model that the adjacent iris states are more frequently the same or the neighboring states. The transition between diagonal opposite directions is very rare. However, it is still unclear, why the iris codes change often in anti-clockwise directions.

As shown in [STW04], Gabor filter is also a kind of local ordinal measure, which describes local relative relationships of adjacent regions. Moreover, the local binary pattern measures directly the local relative relations by comparing the intensity of local region with all its surrounding regions. In [TTMM00], Maenpaa et al. also found out the 9 patterns with very few bit transition in the whole 256 possible patterns are the most informative ones and contribute to more than 90% spatial patterns in the images used in their experiments. Similarly, in our Markov model, some transitions are much more probable than others. The Markov properties of Gabor filter features might be an inherent characteristic of nature images. This can only be further proved with more experiments on iris features extracted from different databases with different Gabor filter implementations.

In this section we analyze the statistical properties of iris codes. We show that iris masks occur at relatively constant areas, which correspond to upper and lower eyelids. The coding method proposed by Hao [HAD05] is not optimal for iris codes. The probabilities of intraclass errors in the upper eyelids are higher than other regions. And the regions close to sclera are more noisy than those close to pupil. Additionally, we also proved that iris codes are not uniformly independently distributed either. The method for estimating the entropy of iris codes proposed by Daugman [Dau03] cannot be applied in iris codes used in our experiments. We propose Markov model to simulate the iris distribution. In the following section we will take a close look at the security and privacy of the fuzzy commitment system for iris recognition.

5.3.2. Assessment of Security and Privacy

In the previous section, we showed that iris codes have the Markov property. It is not a surprise that security and privacy leakage can be measured in the advanced threat model. In this section we give a precise assessment on the privacy and security.

In the fuzzy commitment system, auxiliary data W is the XOR of an iris code and a codeword. Therefore, the security and the irreversibility of PI are equivalent. In the following we make use of all the available information and calculate the complexity to retrieve secrets as well as iris codes from W.

RS code is a systematic code. The first m_s blocks in C are the message blocks. To retrieve the secret, it is sufficient to give a correct estimation of these message blocks. A 2^{l-1} bit Hadamard codeword contains only l bit information. Although Hadamard code is not a systematic code, its code book can be recursively calculated (see Appendix B.3). If $C_1^{2^i}$ is a Hadamard code with length of 2^i, $C_1^{2^{i+1}}$ are also Hadamard codes of length 2^{i+1} with:

$$C_1^{2^{i+1}} = [C_1^{2^i}, \pm C_1^{2^i}] \tag{5.8}$$

where $+C_1^{2^i} = C_1^{2^i}$ and $-C_1^{2^i} = C_1^{2^i} \oplus 1_1^{2^i}$. Here we also define $\pm$ for $Z_j \in \mathcal{Z} = \{[00],[10],[11],[01]\}$:

$$\begin{aligned} +Z_j &= Z_j \\ -Z_j &= Z_{j+2} \end{aligned} \tag{5.9}$$

where $j \in GF(4)$. To estimate a $(2^{l-1}, l, 2^{l-3}-1)$ Hadamard code, it is sufficient to know the two initial bits and the $l-2$ bits at position $2^i+1, i \in [1, \cdots, l-2]$.

We use a recursive method to estimate an iris feature block corresponding to a Hadamard codeword. The auxiliary data W is public. If $X_1^{2^i}$ and $C_1^{2^i}$ are known, there are only two possible candidates of the next iris block, namely $\hat{X}_{2^i+1}^{2^{i+1}} = \pm C_1^{2^i} \oplus W_{2^i+1}^{2^{i+1}}$. Eq 5.8 shows that the sum of the two candidates must be $1_1^{2^i}$. It means that the first two bits of the next subblock, $X_{2^i+1}^{2^i+2}$, are either Z_j or Z_{j+2}. Given the last two bits $X_{2^i-1}^{2^i}$ in the previous iris block and $W_{2^i-1}^{2^i+2}$, the last two bits in the previous auxiliary block and the first two bits in the next auxiliary block, the conditional probabilities of the coming-up two iris bits can be calculated with the following equations:

$$\begin{aligned} p(X_{2^i+1}^{2^i+2} = Z_k | X_{2^i-1}^{2^i} = Z_j, W_{2^i-1}^{2^i+2}) &= \frac{p([Z_j, Z_k])}{p([Z_j, Z_k]) + p([Z_j, Z_{k+2}])} \\ p(X_{2^i+1}^{2^i+2} = Z_{k+1} | X_{2^i-1}^{2^i} = Z_j, W_{2^i-1}^{2^i+2}) &= 0 \\ p(X_{2^i+1}^{2^i+2} = Z_{k+2} | X_{2^i-1}^{2^i} = Z_j, W_{2^i-1}^{2^i+2}) &= \frac{p([Z_j, Z_{k+2}])}{p([Z_j, Z_k]) + p([Z_j, Z_{k+2}])} \\ p(X_{2^i+1}^{2^i+2} = Z_{k+3} | X_{2^i-1}^{2^i} = Z_j, W_{2^i-1}^{2^i+2}) &= 0 \end{aligned} \tag{5.10}$$

For instance, given $W_{2^i-1}^{2^i+2} = [Z_{j_1}, Z_{j_2}]$, then $C_{2^i-1}^{2^i} = Z_{j+j_1}$ and $k = j + j_1 + j_2$, where $k, j, j_1, j_2 \in GF\{4\}$.

Now we are able to calculate the conditional entropy $H(X_{2^i+1}^{2^i+2} | X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2})$. According to Eq A.8, it can be computed with:

$$H(X_{2^i+1}^{2^i+2} | X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2}) \quad = \quad - \sum_{X_{2^i-1}^{2^i+2}, W_{2^i-1}^{2^i+2}} p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2}) \log p(X_{2^i+1}^{2^i+2} | X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2}) \tag{5.11}$$

The joint probability $p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2})$ can be derived from the distributions of $[X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}]$ and the bits $C_{2^i-1}^{2^i+2}$ in a Hadamard codeword:

$$\begin{aligned}
p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2}) &\overset{(a)}{=} p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}, C_{2^i-1}^{2^i+2}) \\
&\overset{(b)}{=} p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}) p(C_{2^i-1}^{2^i+2}) \\
&\overset{(c)}{=} \frac{1}{8} p(X_{2^i+1}^{2^i+2}, X_{2^i-1}^{2^i}) \qquad (5.12)
\end{aligned}$$

Step (a) follows from the effect that $W = X \oplus C$ and each combination of X and C gives a unique W; step (b) follows from the independency of X and C; step (c) follows from the rekursive properties of C and information rate of $H(C_{2^i-1}^{2^i+2}) = 3$ for any $i \in \mathcal{N}$. With Eq 5.11, 5.10 and 5.12, we can obtain:

$$H(X_{2^i+1}^{2^i+2} | X_{2^i-1}^{2^i}, W_{2^i-1}^{2^i+2}) = 0.1051 \qquad (5.13)$$

It is much smaller than $H(C_{2^i+1}^{2^{i+2}} | C_1^{2^i}) = 1$ and $H(Z) = 0.901$. It shows that uncertainty about the iris as well as secret reduces rapidly given the iris distribution and W.

We give an estimation of the uncertainty about a whole iris block corresponding to a Hadamard of length 2^{l-1}:

$$\begin{aligned}
\hat{H}(X_{j\gamma+1}^{j\gamma+\gamma} | W_{j\gamma+1}^{j\gamma+\gamma}) &= H(X_{j\gamma+1}^{j\gamma+2}) + \sum_{i=2}^{l-1} H(X_{j\gamma+2^i+1}^{j\gamma+2^i+2} | X_{j\gamma+2^i-1}^{j\gamma+2^i}, W_{j\gamma+2^i-1}^{j\gamma+2^i+2}) \qquad (5.14) \\
&= 2 + (l-2) \cdot 0.1051 \qquad (5.15)
\end{aligned}$$

for any $j \in \{0, 1, 2, \cdots, m_{RS} - 1\}$. Here $\gamma = 2^{l-1}$ and m_{RS} is the symbol length of an RS code. Eq 5.14 only makes use of the bits around the informative positions in the Hadamard code. It is a close approximation of the real $H(X_{j\gamma+1}^{j\gamma+\gamma} | W_{j\gamma+1}^{j\gamma+\gamma})$. According Eq A.12, the chain rule of joint information:

$$\begin{aligned}
H(X_{j\gamma+1}^{j\gamma+\gamma} | W_{j\gamma+1}^{j\gamma+\gamma}) &= \sum_{i=1}^{l-1} H(X_{j\gamma+2^i+1}^{j\gamma+2^{i+1}} | X_{j\gamma+1}^{j\gamma+2^i}, W_{j\gamma+1}^{j\gamma+\gamma}) \\
H(X_{j\gamma+2^i+1}^{j\gamma+2^{i+1}} | X_{j\gamma+1}^{j\gamma+2^i}, W_{j\gamma+1}^{j\gamma+\gamma}) &\overset{(a)}{=} H(X_{j\gamma+2^i+1}^{j\gamma+2^i+2} | X_{j\gamma+1}^{j\gamma+2^i}, W_{j\gamma+1}^{j\gamma+\gamma}) \\
&\leq H(X_{j\gamma+2^i+1}^{j\gamma+2^i+2} | X_{j\gamma+2^i-1}^{j\gamma+2^i}, W_{j\gamma+2^i-1}^{j\gamma+2^i+2})
\end{aligned}$$

Step (a) is valid, since the knowledge of any bit in $X_{j\gamma+2^i+1}^{j\gamma+2^{i+1}}$ can expose the rest of the block. If the whole block $W_{j\gamma+1}^{j\gamma+\gamma}$ is taken into account by estimating $X_{j\gamma+2^i+1}^{j\gamma+2^i+2}$, the uncertainty about $X_{j\gamma+2^i+1}^{j\gamma+2^i+2}$ might further reduce.

In our experiment, two settings of Hadamard code are used: $\hat{H}(X_{j\gamma+1}^{j\gamma+2^{l-1}} | W_{j\gamma+1}^{j\gamma+2^{l-1}}) = 2.523$ at $l = 7$ and $\hat{H}(X_{j\gamma+1}^{j\gamma+2^{l-1}} | W_{j\gamma+1}^{j\gamma+2^{l-1}}) = 2.631$ at $l = 8$. Eq5.15 shows that the uncertainty about X increases very slowly with l. Enlarging l, the real gain on the security is very poor.

The complexity to estimate the whole iris code is:

$$\begin{aligned}
\hat{H}(X|W) &= \hat{H}(X_1^{\gamma}|W_1^{\gamma}) + \sum_{j=1}^{m_S-1} \hat{H}(X_{j\gamma+1}^{j\gamma+\gamma}|X_{j\gamma-\gamma+1}^{j\gamma}, W_{j\gamma-\gamma+1}^{j\gamma+\gamma}) \\
&= \hat{H}(X_1^{\gamma}|W_1^{\gamma}) + \sum_{j=1}^{m_S-1} \Big(H(Z) + \sum_{i=2}^{l-1} \hat{H}(X_{j\gamma+2^i+1}^{j\gamma+2^i+2}|X_{j\gamma+2^i-1}^{j\gamma+2^i}, W_{j\gamma+2^i-1}^{j\gamma+2^i+2})\Big) \qquad (5.16) \\
&= 2 + (m_S-1)0.901 + m_S \cdot (l-2) \cdot 0.1051 \\
&= 1.099 + 0.6908 \cdot m_S + 0.1051 \cdot L_S \qquad (5.17)
\end{aligned}$$

where m_S is the number of message blocks in the RS code and $L_S = m_s \cdot l$ is the secret length. The second term in Eq 5.16 is different from Eq 5.14. The reason is that if the previous Hadamard code is known, the next Hadamard block can be initialised with dependency of the iris code.

Table 5.6 shows $\hat{H}(X|W)$ at different settings. Since $\hat{H}(X|W) = \hat{H}(S|W)$, the values in Table 5.6 represent both the security and irreversibility of protected templates. The previous section shows that it is not difficult to learn the statistics of iris codes. An experienced attacker can exploit Markov property of the iris codes to crack the system. Section 5.3.4 will show a method to crack the fuzzy commitment algorithm.

m	9600				2048				
L_S	24	40	56	72	14	16	32	48	64
m_S	3	5	7	9	2	2	4	6	8
$\hat{H}(X\|W)$	5.6938	8.7570	11.8202	14.8834	3.9520	4.1622	7.2254	10.2886	13.3518

Table 5.6.: $\hat{H}(X|W)$ of the fuzzy commitment system for iris recognition at different settings

In the last section we show that $\hat{H}(X_1^{9600}) = 4325.88$ and $\hat{H}(X_1^{2048}) = 923.72$. The current fuzzy commitment scheme has more than 4300 bits privacy leakage for $m = 9600$ and 900 bits for $m = 2048$. We know that privacy leakage is unavoidable. If W is unknown, the uncertainty of X is equal to its entropy. The privacy leakage shows the reduction of the complexity to estimate the iris features in comparison with a blind estimation. Additionally, the dependency of iris codes reduces the security significantly and $\hat{H}(X|W)$ is much smaller than L_S. High secret leakage also exists.

In the original paper [HAD05], Hao et al. also gave a lower boundary of the security. An iris code has 2^{249} possible candidates. They empirically measured that their coding algorithm can correct up to 27% of the bit errors, which is about 67 bits in a 249 bits code. If all the bit strings in a sphere within the Hamming distance of 67 bits can be mapped to the same key as well as the same iris code, the searching effort is at least $2^{249}/\sum_{i=0}^{67}\binom{249}{i} \approx 2^{249}/\binom{249}{67} = 2^{44}$. They claimed that it is the worst case scenario. They also claimed that "with our current state of knowledge we really do not know how to correlate someone's iris bits unless we know their iris code anyway."

We argue that their security assessment is too optimistic. Their estimated entropy is 249 bits, which is much smaller than the feature size 2048 bits. It means that their iris codes are also strongly correlated. Additionally, the equation they used to estimate the searching effort is the Hamming bound of linear block codes. It means that the achievable secret size of a 249 bit codeword with 67 bit error tolerance is at most 44, which is much smaller than the secret size of 140 in their system. The secret leakage also exists in their system.

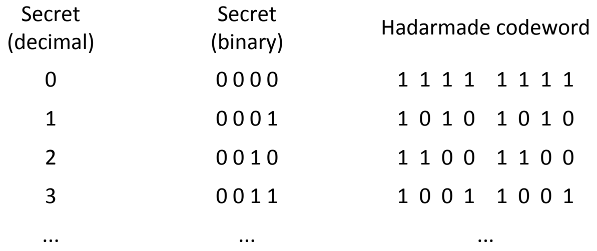
Section 5.3.1 explored the distribution of iris codes and proved that distribution estimation is possible for iris codes. In this section we gave an alternative to quantify the security, which is based on the knowledge of the coding scheme and the distribution of iris codes. We found out that Hadamard codes mismatch the iris code structure. It causes high security leakage.

5.3.3. Assessment of Unlinkability

In this section we evaluate the unlinkability of the algorithm regarding cross matching and leakage amplification. The previous section showed that high privacy leakage exists in the helper data W, therefore, the protected system is definitively vulnerable to cross matching. Figure 5.5 in Section 5.2 shows the coding scheme used in the protected system. This scheme is vulnerable to the decodability attack proposed in [STP09]. The final codeword C_{RS+Had} consists of m_{RS} Hadamard codeblocks and $W = C_{RS+Had} \oplus X$. Like all linear block codes, the sum of two Hadamard codewords is still a codeword. The sum of two auxiliary data generated from the same subject is decodable with higher probability than those from different subjects. On the other hand, the decodability attack can further be applied on the RS coding layer, only if linearity between secrets and encoded codewords exists: given $C_1 = Enc(s_1)$ and $C_2 = Enc(s_2)$ are two codewords, s_1 and s_2 are their secrets, $C_1 \oplus C_2$ is also a codeword with $s_1 \oplus s_2 = Dec(C_{Had,1} \oplus C_2)$.

Hadamard code is a kind of linear block code. However, the linearity is not required in the Hadamard encoding and decoding algorithms shown in Appendix B.3. The codebook used in our experiment is the Hadamard matrix given in Appendix B.3. Each row in the matrix is coded with a bit string converted from a decimal number. The decimal number starts from zero and increases with the number of the rows. Figure 5.15 shows an example of the codebook used in our experiment. The sum of two codewords is also a valid codeword, but it is not the codeword corresponding to the sum of their secrets. The linearity between secrets and encoded codes does not exist. Therefore, the decodability attack is not feasible in the RS coding layer. But if the Hadamard codebook is not carefully designed, the decodability attack on RS coding layer is possible.

We evaluate the recognition performance with the decodability attack. The number of decodable Hadamard blocks is the corresponding comparison score. The length of Hadamard block is 128. The number of Hadamard blocks is 16 for $m = 2048$ and 75 for $m = 9600$. The Hadamard code has the fixed code rate given the block length. Therefore, the performance is independent of the secret size in the protected system. The corresponding FMR and $FNMR$ are shown in Figures 5.16 and 5.17. The blue lines are the results from CASIA v1 database using mask; the green lines are from CASIA interval v3 with mask; the red lines are from CASIA interval v3 without mask. The number of decodable blocks of CASIA interval v3 without mask is much smaller than the other two. The FMR of CASIA v1 and CASIA interval v3 with mask is very similar. However the $FNMR$ of CASIA v1 is much better than of CASIA interval v3. Table 5.7 shows the recognition performance, where FMR is approximately equal to $FNMR$. The ROC curves of this attack is plotted in Figure 5.18 and compared with



Secret (decimal)	Secret (binary)	Hadarmade codeword
0	0 0 0 0	1 1 1 1 1 1 1 1
1	0 0 0 1	1 0 1 0 1 0 1 0
2	0 0 1 0	1 1 0 0 1 1 0 0
3	0 0 1 1	1 0 0 1 1 0 0 1
...	...	...

Figure 5.15.: Example of a Hadamard codebook used in our experiment with the message length of 4 and codeword length of 8

the performance of the fuzzy commitment algorithm. The dashed lines are the curves of $m = 2048$ and the solid lines are the curves of $m = 9600$. The ROC curves of the fuzzy commitment algorithm are marked with '+' and they are on the upper left of the ROC with decodability attack. The resulting recognition performance is comparable with that of the protected system using only one layer coding with the Hadamard code. Therefore, the performance with decodability attack is worse than the original fuzzy commitment algorithm with the two layer coding scheme.

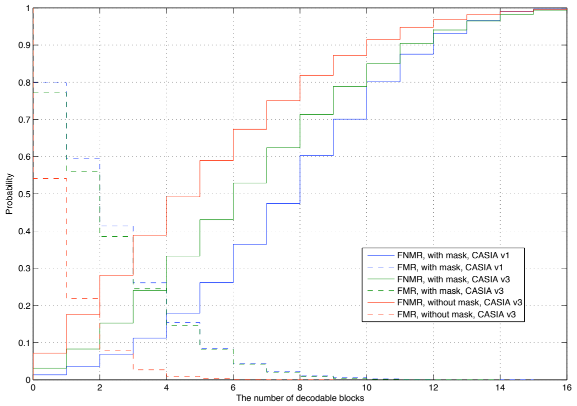


Figure 5.16.: *FMR* and *FNMR* with decodability attack at $m = 2048$

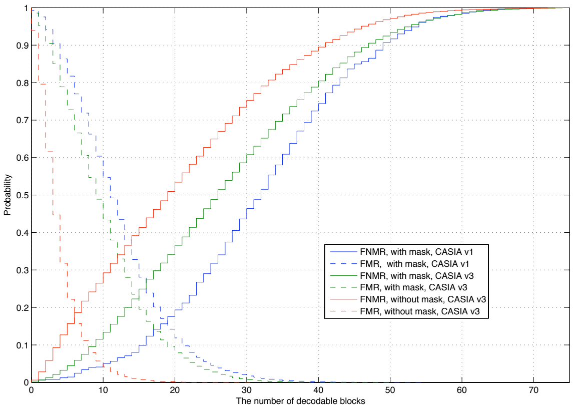


Figure 5.17.: *FMR* and *FNMR* with decodability attack at $m = 9600$

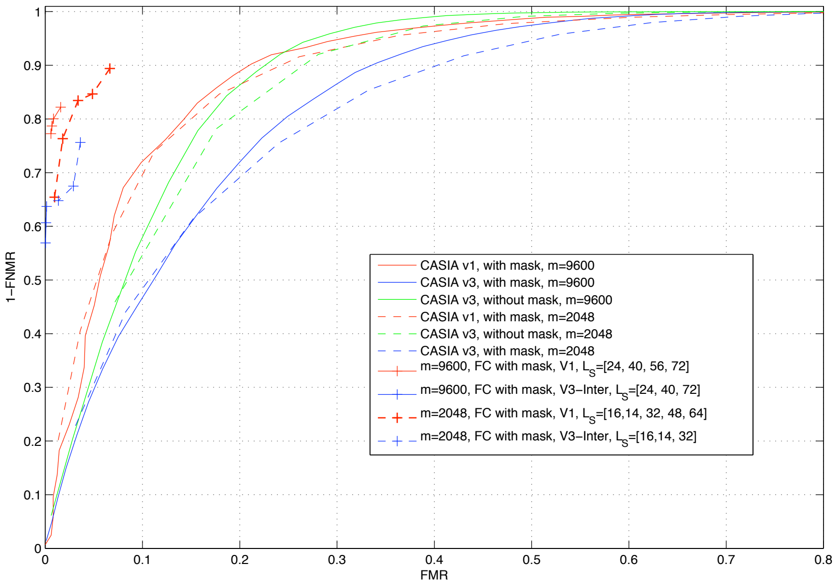


Figure 5.18.: ROC curves of the fuzzy commitment algorithm and the decodability attack

	$m = 2048$			$m = 9600$		
	CASIA v1	CASIA v3		CASIA v1	CASIA v3	
	mask	mask	no mask	mask	mask	no mask
FMR	15.37%	24.49%	21.85%	17.05%	23.54%	15.68%
$FNMR$	17.9%	24%	17.58%	15.64%	22.28%	18.64%
# of decodable blocks	4	3	1	18	14	7

Table 5.7.: The recognition performance with the decodability attack

The privacy leakage caused by Hadamard codes is dependent on their codeword length γ. The shorter γ is, the smaller the privacy leakage rate is. Increasing the codeword length (with decreasing code rate) can reduce $FNMR$ and increase FMR.

Although this algorithm is vulnerable to cross matching, it has good resistance to leakage amplification. If two secure templates are generated with the same coding parameters, leakage amplification is impossible. Even if different coding parameters are used, leakage amplification is still infeasible. Theorem 1 in Appendix B.2 shows that an RS codeword of short secret length is also a codeword of the same codeword length but large secret length. Additionally, the Hadamard codebook with long codeword length can be derived by concatenating the codebook of smaller codeword length. For instance, given $\mathcal{C}^{\gamma}$ is the Hadamard code book of the block length γ and $\tilde{\mathcal{C}}^{\gamma}$ is a set consisting of all the codes with the same block length, which are concatenated with two codewords from $\mathcal{C}^{\gamma/2}$. Obviously, $\mathcal{C}^{\gamma}$ is a subset of $\tilde{\mathcal{C}}^{\gamma}$. Changing the secret length in the fuzzy commitment algorithm can not bring additional information about secret or biometric features. Therefore, privacy amplification is impossible.

5.3.4. Cracking the Fuzzy Commitment for Iris Recognition

The assessment in Section 5.3.2 showed poor security and irreversibility of secure templates. In this section we prove that retrieval of iris codes as well as secrets is indeed feasible with low lost. Here we assume the advanced threat model and make use of knowledge about the distribution of iris codes and the details of the protected iris systems. The idea behind is to exploit all available information and to find out the most likely iris codes or secrets.

We propose the following estimation method. A secure template $[h(S),W]$ is generated from iris feature X. The set $\mathfrak{X} = \{\mathcal{X}_1, \mathcal{X}_2, \cdots, \mathcal{X}_N\}$ consists of all the possible candidates of X given W. Since the distribution of the features X is known, it is possible to calculate the probability $p(X = \mathcal{X}_i|W)$ for $X_i \in \mathfrak{X}$. We rank $\mathcal{X}_i$ with decreasing $p(X = \mathcal{X}_i|W)$ and start the estimation with the most probable sequences.

We denote $X_{j\gamma+1}^{j\gamma+\gamma} = [x_{j\gamma+1}, x_{j\gamma+2}, \cdots, x_{j\gamma+\gamma}]$ as a subblock of X, for $j \in \{0,1,2,\cdots,m_S-1\}$, which corresponds to a Hadamard codeword. $W_{j\gamma+1}^{j\gamma+\gamma}$ is the corresponding subblock in W. The Hadamard codebook $\mathcal{C}^{\gamma} = \{C_1, C_2, \cdots, C_N\}$ with the message length of l consists of $N = 2^l$ Hadamard codewords. Every codeword is $\gamma = 2^{l-1}$ bit long. For all $C_i \in \mathcal{C}^{\gamma}$, $\mathcal{X}_i$ is a candidate of $X_{j\gamma+1}^{j\gamma+\gamma}$ with:

$$\mathcal{X}_i = W_{j\gamma+1}^{j\gamma+\gamma} \oplus C_i \tag{5.18}$$

$\mathfrak{X} = \{\mathcal{X}_i | i \in [1,2,\cdots,N]\}$ contains exactly N candidates. The search space of $X_{j\gamma+1}^{j\gamma+\gamma}$ is limited only to the N possible candidates. Since we use Markov model to simulate iris features, the probability $p(X_{j\gamma+1}^{j\gamma+\gamma} = \mathcal{X}_i | W_{j\gamma+1}^{j\gamma+\gamma})$

can be calculated with:

$$p(X_{j\gamma+1}^{j\gamma+\gamma} = \mathcal{X}_i | W_{j\gamma+1}^{j\gamma+\gamma}) \quad = \quad p(z_1^i) \cdot p(z_2^i | z_1^i) \cdots p(z_{\gamma/2}^i | z_{\gamma/2-1}^i) \tag{5.19}$$

where $\mathcal{X}_i = [z_1^i, z_2^i, \cdots, z_{\gamma/2}^i]$ and $z_j^i \in \mathcal{Z} = \{[00], [10], [11], [01]\}$. Then we create a ranking list by sorting $p(X_{j\gamma+1}^{j\gamma+\gamma} = \mathcal{X}_i | W_{j\gamma+1}^{j\gamma+\gamma})$ in descending order for all $i \in [1, 2, \cdots, N]$. $\mathcal{X}_T = argmax_{\mathcal{X}_i \in \mathfrak{X}} \{p(X_{j\gamma+1}^{j\gamma+\gamma} = \mathcal{X}_i | W_{j\gamma+1}^{j\gamma+\gamma})\}$ is the most probable one. Guessing $X_{j\gamma+1}^{j\gamma+\gamma}$ should start with the first one in the ranking list, and then the second and so on, till the correct one is found.

A secure template contains the hash of the whole secret. We are not able to check the correctness of the estimated individual subblocks. Therefore, we apply this process to all the subblocks corresponding to the message blocks of RS codes and recalculate the probabilities of all the possible combinations of the iris bits:

$$p(X_1^{m_S\gamma} | W_1^{m_S\gamma}) = \prod_{j=0}^{m_S-1} p(X_{j\gamma+1}^{j\gamma+\gamma} | W_{j\gamma+1}^{j\gamma+\gamma}) \tag{5.20}$$

For every possible $X_1^{m_S\gamma}$, a corresponding secret can be estimated by decoding Hadamard codes and concatenating the secret bits of individual Hadamard codes. Now we can rank $p(X_1^{m_S\gamma} | W_1^{m_S\gamma})$ and start the estimation with the most probable ones. If the hash of the estimated secret candidate is exactly matched with the stored hash value, then the correct secret is found.

Additionally, in order to speed up the searching process, we use the following logarithmic representation of the probabilities so that multiplications are converted into additions:

$$\log(p_1 \cdot p_2 \cdots, p_n) = \log(p_1) + \log(p_2) + \cdots + \log(p_n) \tag{5.21}$$

We test our cracking algorithm in CASIA interval v3 database with 2639 different iris images. The Hadamard code of (128, 8, 31) is used. We try to estimate the subblocks of iris codes and secrets corresponding to individual Hadamard code blocks with Eq 5.19. The results of different settings are shown in Figure 5.19. The x-axis indicates R, the number of performed attempts till the correct secret is found; the y-axis shows the probability, that the R-th attempt is successful. Comparing with low conditional entropy $H(X_{j\gamma+1}^{j\gamma+\gamma} | W_{j\gamma+1}^{j\gamma+\gamma}) = 2.532$, it is not surprising that the most Hadamard blocks can be cracked with only two attempts. Without mask, more than 58% blocks can be successfully estimated at the first attempts and more than 36% at the second attempts. With mask, more than 56% blocks are correctly guessed at the second attempts and more than 32% at the first attempts. The success probability at the first attempt in the case without mask is higher than that with mask, because our Markov model is trained with the iris features without mask. Moreover, if iris masks are used, iris bits in the marked regions are all zeros, which also belong to the highly probable state transition. Therefore, a lot of blocks can be cracked after the second attempts in the case with mask. The guessing entropy of Hadamard blocks can be calculated with Eq A.18. Based on our test results, it is less than 1.5 attempts.

When estimating the whole secret, the conditional probability can be calculated sequentially with Eq 5.20. If a candidate list of $X_1^{j\gamma}$ is with the size of U, the new candidates list of $X_1^{j\gamma+\gamma}$ including the next subblock increases to $U \times N$. The size of the candidate list increases exponentially with m_S, the number of the message blocks in an RS code. It can block the memory very fast. We use the following sub optimal solutions to reduce the memory size as well as the computational power required.

In the first implementation we use the *Viterbi algorithm* and give a limit on the length of the candidate list. If the number U of the candidates exceeds a predefined limit, the rest of the candidates will be deleted from the sorted candidate list. In the second implementation, we change the ranking strategy and choose the first V

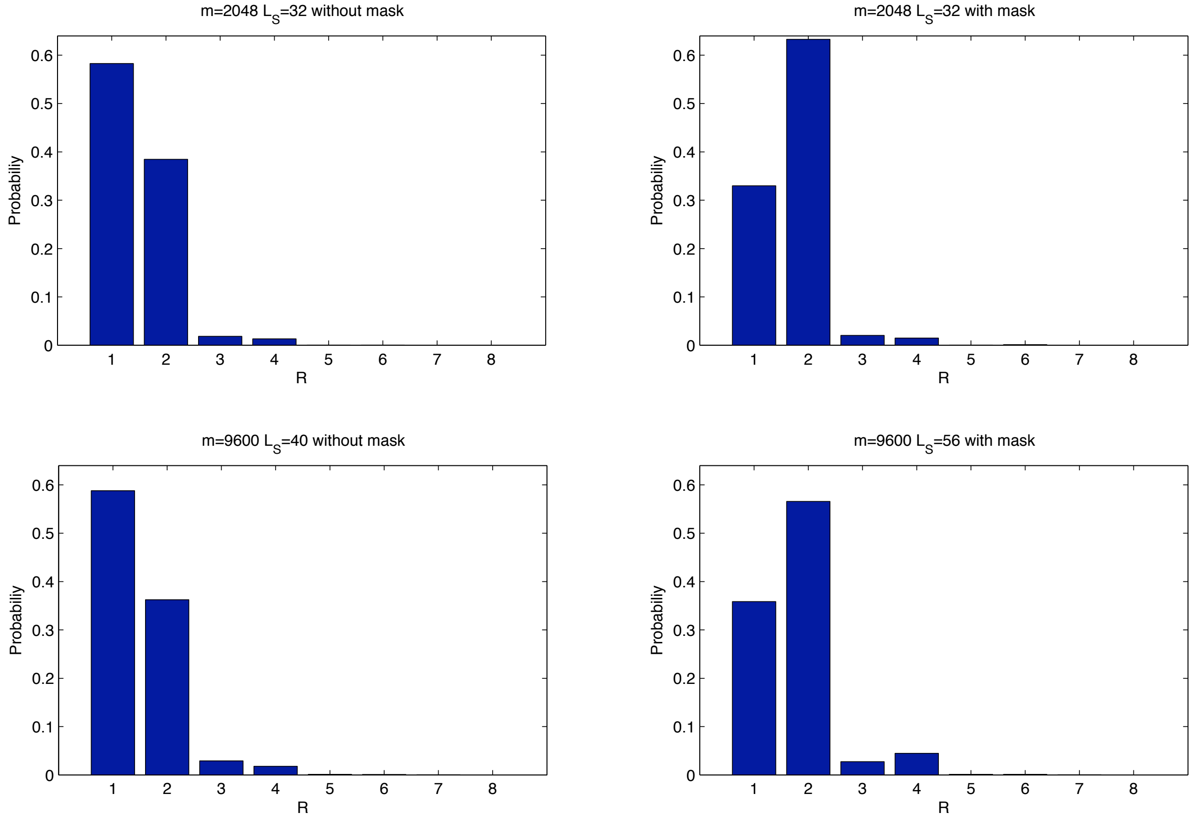


Figure 5.19.: The number of attempts and their corresponding successful rate

candidates of every Hadamard block. For instance, if the candidate list of $X_1^{j\gamma}$ is with the size of U, the new candidate list of $X_1^{j\gamma+\gamma}$ is extended with the first V candidates of $X_1^{j\gamma}$. And the size of the new list increases to $U \times V = V^{j+1}$. We denote the first implementation as Algo 1 and the second implementation as Algo 2.

In the experiment with Algo 1, the candidate list length never exceeds the length of the Hadamard codebook, namely 256 for the128 bit long Hadamard codewords. The number of the candidates to be calculated during ranking is never larger than 256×256, which corresponds to 16 bits. The estimation results are plotted in Figure 5.20. This setting works very well with the short L_S. However, as L_S grows, not all features can be successfully estimated. For $L_S = 40$, 99.85% secure templates without mask can be cracked with up to 10.52 bit attempts and 99.51% with mask can be retrieved with up to 9.66 bit attempts. For $L_S = 56$, 91.22% protected templates without mask and 91.68% with mask can be cracked with maximum 10.38 bit attempts. The success probabilities reduce strongly at $L_S = 72$. Only 44.19% secure templates without mask and 45.71% with mask can be estimated with maximum 9.98 bit attempts. We also try to increase the length of the candidate list to improve the number of crackable templates. However, the success rate increases very slowly with the length of the list.

In the experiment with Algo 2, only the first 4 most probable candidates of individual codeblocks are taken into account. The maximum number of attempts is $4^{m_{RS}}$. The results are plotted in Figure 5.21. For $L_S =$

$\{40, 56, 72\}$, the maximum attempts are 10, 14, 18 bits. The maximum success rates are 96.59%, 98.59% and 99.09% respectively.

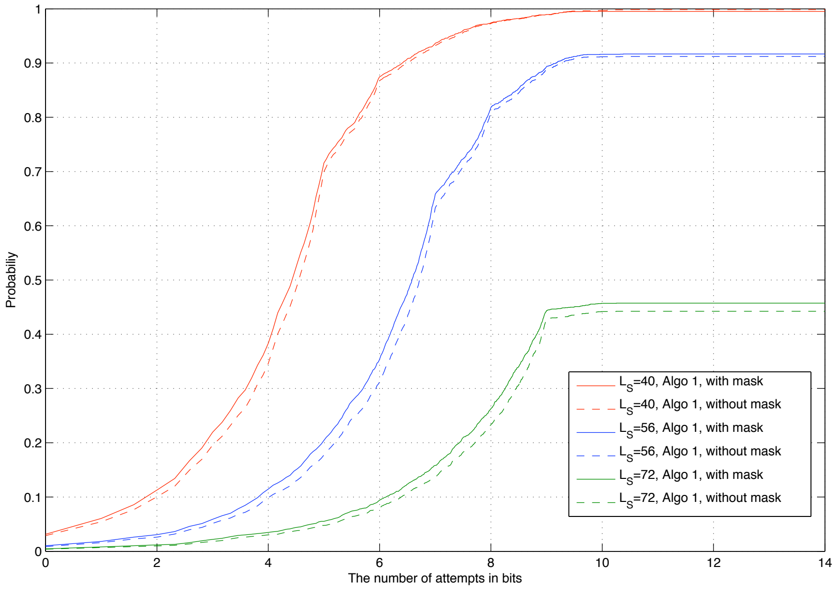


Figure 5.20.: The success rate of cracking secure templates from CASIA v3 Interval Database with Algo 1

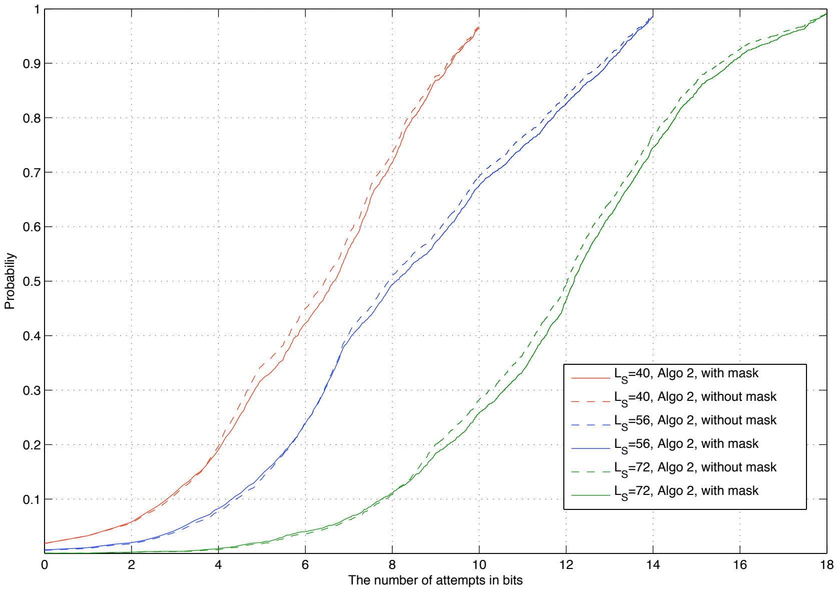


Figure 5.21.: The success rate of cracking secure templates from CASIA v3 Interval Database with Algo 2.

Except the setting of $L_S = 40$, Algo 2 is generally better than Algo 1. The memory and computational power required in Algo 2 grow with the secret size. This avoids the waste of the resource by estimating short secrets. The success rate curves of Algo 1 grow faster than those of Algo 2, however, they reach saturation also earlier than Algo 2. Additionally, Algo 2 shows a better performance for long secret. In Algo 1, the candidates in the previous block are weighted more than that in the later blocks. However, the success of estimation is dependent on the correctness of every subblock. Figure 5.19 already shows that the correct secret of individual subblocks is with high probability in front of the ranking list. Therefore, Algo 2 is more efficient than Algo 1.

The algorithms with the current settings can not crack all the secure templates. Those unsuccessfully estimated templates need more than N_T attempts, where N_T is the maximum number of attempts used in a setting. We assign N_T to those unsuccessful templates and calculate the average number of attempts needed to reconstruct iris codes with Algo 2 for $m = 9600$ in CASIA interval v3 database. The results are shown in Table 5.8. The number of attempts for those unsuccessful templates might be larger than N_T. Therefore, the results are a lower bound of the average number of attempts and the risk of overestimation on the security is avoided.

L_S	Average # of attempts	
	no mask	mask
40	7.73	7.65
56	11.06	10.93
72	14.42	14.25

Table 5.8.: The average number of attempts (in bits) needed to reconstruct iris codes with Algo 2 for $m = 9600$ in CASIA interval v3 database

5.3.5. Discussions

In Section 5.3.2 we measured the security and privacy protection ability of the protected iris recognition system with mutual information and conditional entropy. It was shown that the uncertainty of iris code X as well as secret S given auxiliary data W is much smaller than the secret length. The security and irreversibility of secure templates are very poor. In Section 5.3.4, we proposed a cracking algorithm, which exploits the distribution of iris codes and the detail of the coding method. We show that cracking protected templates is possible with low complexity. It confirms the results obtained in our theoretical analysis. An adversary can really use the security and privacy leakage of the system and perform a practical attack. The cracking algorithm requires certain memory and computational power. In Section 5.3.4, the calculation of candidate list was based on a recursive method, which is not time consuming. However, temporary storage of the list needs huge memory. We solved this problem by limiting the length of the candidate list. It is a sub optimal solution with quite high success rate and only several secure templates can not be cracked successfully.

In Section 5.3.3, we analyzed the unlinkability. The system is resistant to leakage amplification, but vulnerable to cross matching. Cross matching is caused by high privacy leakage and a decodability attack can be performed at Hadamard coding layer. With the cracking method, it is easy to explain the effect of leakage amplification. If W_1 and W_2 are the helper data generated from features X_1 and X_2 of the same subject using the same coding method, they result in the similar candidate lists with a linear shift of $X_1 - X_2$. Linking W_1 and W_2 will not give any additional information about X_1 or X_2. However if different coding schemes are used, two different candidate lists can be produced. The ranking can be further optimized with the similarity between the candidates in two different lists. It means that the real X_1 and X_2 are in two candidate lists and their distance is smaller than those between other candidates. This causes leakage amplification. However, if the noise between X_1 and X_2 is too high and their distance is too large, then there is no advantage combining two templates and leakage amplification is impossible. It also supports the analysis in [STP09] (see also Section 3.4.2).

The security and privacy leakage is a serious problem in the system. Hadamard code has good error correction ability, however, its code construction strengthens the leakage. A subblock of a Hadamard code is a repetition or an inversion of its previous block. It complies with the path with the lowest probability in the Markov chain of iris codes. Therefore, the possible candidates of an iris codes are far from a uniform distribution given the helper data. It is possible to improve the security of the system by changing the coding scheme. We can modify iris encoding process so that a state and its inversion on the Markov chain are not in the diagonal positions, e.g switching the state [01] and [11] in Figure 5.14. Unfortunately, the error probability will increase, since the Hamming distance between adjacent quantization areas grows from 1 bit to 2 bit. Alternatively permutation is also a useful tool. We can change iris codes or Hadamard code such that the distribution of iris candidates given the helper data looks more uniform. It is also possible to scramble the whole iris codes and the complexity of calculating the ranking list can increase strongly and more memory is required. But this method will break burst error patterns in iris codes and RS code will be no longer useful. The potentials to improve security exist by designing more adequate coding scheme.

On the other hand, if iris features are stationary and ergodic, secrecy leakage is unavoidable with the fuzzy commitment scheme. In [Ign09], Ignatenko gave a lower bound of the entropy $H(W)$ for this case:

$$H(W) \geq n \cdot h\big(h^{-1}(H(X)) * h^{-1}(\frac{L_S}{n})\big) \tag{5.22}$$

where h is binary entropy function, h^{-1} is the inverse function of h, and the operator $*$ is defined for $0 \leq a, b \leq 1$ as $a * b = a(1-b) + (1-a)b$. The achievable secret size of the system $H(S|W)$ can not be larger than $H(X) + L_S - n \cdot \big(h^{-1}(H(X)) * h^{-1}(\frac{L_S}{n})\big)$. For $L_S = 72$ and $m = 9600$, $H(S|W)$ is at most 54.4234 bits. In order to prevent security leakage inherently, either iris codes should be decorrelated or alternative template protection construction should be used.

5.4. Summary

In this chapter, we continued the evaluation and gave a rigorous assessment on a template protection system for iris recognition. Iris is a widely used biometric modality. Most of iris recognition algorithms describe the local pattern of iris textures. We introduced briefly iris recognition and extracted the iris features from CASIA database with an open source Matlab code using 1D log-Gabor filter. We implemented the fuzzy commitment algorithm proposed by Hao et al. which is a fundamental work of protecting iris features. Iris codes have high discriminative power, however, the intraclass errors are also quite high. The two layer coding scheme including Hadamard code and RS code is used to achieve good robustness. Comparing with results in the original paper, we can not obtain the same recognition performance and the secret size. The reason is the use of different databases and feature extraction algorithms. However, it does not affect our work on the security and privacy assessment.

We evaluated the implemented template protection system based on our framework. We analyzed the distribution of iris codes and found out that they can be well characterized with a Markov model. It is shown that iris codes are strongly dependent. With high probability the adjacent states in an iris code are the same or change anti-clockwise along the Markov model. Based on this, we quantify the security and privacy protection ability of the system with information theoretical metrics such as mutual information and conditional entropy. Due to the dependency of iris codes as well as the coding scheme, the security and irreversibility are very poor. Especially, the Hadamard code has an opposite pattern to iris codes and decreases the security significantly. As a consequence of high privacy leakage, the system is also vulnerable to cross matching. Although the performance linking secure templates is much worse than the protected system, it is still a serious security weakness. The advantage of this construction is the resistance to leakage amplification.

We did not limit our evaluation to the theoretical assessment and designed a cracking algorithm to retrieve secrets and iris codes from secure templates. We exploited the knowledge about the coding scheme and the properties of iris codes. It is shown that both secrets and iris codes can be successfully estimated with low complexity. It confirms the results of the theoretical assessment. It is possible to improve the security to a certain extent by changing the coding scheme. However, it is already proved in the literature that the secret leakage is unavoidable as long as iris codes are non-uniform stationary and ergodic sequences.

6. Extended Analysis

In Chapter 3, we proposed a generalized evaluation framework for privacy and security assessment. In Chapters 4 and 5, we applied this framework on the template protection system for 3D face recognition and iris recognition using fuzzy commitment. Their privacy and security performance were *strictly* investigated under the advanced threat model. In this chapter, we complete the evaluation including the assessment in the naive and collision models. Furthermore, we take a look at the existing security analyses on the fuzzy vault system for fingerprint recognition and show that these analyses fit perfectly into the proposed framework. With the help of the framework as well as the definitions of security and privacy, we are able to compare three different template protection systems regarding their security and privacy performance.

Both fuzzy commitment and fuzzy vault belong to biometric cryptosystems. Additionally, we validate the framework on the transformation-based approaches. In contrast to biometric cryptosystems, their evaluation is based on individual attacks. We investigate and extend the existing security analyses. These analyses can map well to the framework and measure different protection goals, namely security, privacy protection ability and unlinkability under special threat models.

6.1. Biometric Cryptosystems

6.1.1. Assessment of the Fuzzy Commitment Scheme in Different Threat Models

In Section 3.4 as well as Chapters 4 and 5, we concentrated on the assessment of fuzzy commitment in the advanced threat model. In this section, we generalize our assessment to all three threat models including the naive and collision models.

As shown in Section 3.4, a protected template in a fuzzy commitment scheme consists of PI and $\mathbb{W}$, where $PI = h(S)$ is the hash of a randomly generated secret S and $\mathbb{W}$ includes all auxiliary data, for instance, the XOR of the codeword and biometric feature and the positions of the most reliable bits used in the fuzzy commitment system for 3D face recognition as shown in Section 4.2.1. In the *naive* threat model, we assume that an adversary has no information about the system. The only attack, which he can perform, is to invert the hash $h(S)$. For a perfect hash function there exists no useful inversion function. Since S is a L_S-bit long uniformly distributed string (property of random number), the brute force on $h(S)$ requires 2^{L_S-1} trials on average. The secret length, which can be achieved currently with fuzzy commitment, is relatively short. In this case, the computational time required to calculate a hash is very small. We consider it as a constant and denote $O(1)$ to measure the computational time of the hash function. Recalling the security definition Def 1 given in Section 3.2.3, fuzzy commitment is $(\mathcal{T}, \varepsilon)$- secure in the naive model with $\mathcal{T} = O(1)$ and $\varepsilon = L_S - 1$. In this threat model, an adversary can only retrieve the secret. He can, for instance, reuse this secret and try to be verified as an authorized subject. However, neither privacy information can be learned nor any linkage attack is possible.

In the *advanced* model, more information is available to an adversary and the assessment is much more rigorous than in the naive model. In Chapters 4 and 5, information-theoretical metrics are used to evaluate the security and privacy preserving ability. A perfectly secure fuzzy commitment scheme requires independently uniformly distributed features and does not leak information about the secret. Our evaluation results on 3D face and iris recognition show that serious privacy and security leakage exists, if the requirement of independency is not fulfilled.

Dependency of features is very common in biometric systems. Especially, those feature extraction algorithms based on local patterns preserve more or less the inherent correlation present in biometric modalities. On the one hand, we can use additional processes such as random projection or independent component analysis, to reduce the dependency of biometric features. On the other hand, we show that coding algorithms have a strong influence on security. Although security leakage can not be eliminated with coding algorithms, a well-designed method can be adapted to statistical properties of biometric features and minimize secret leakage and an improper coding method can enlarge the leakage. For instance, we show in Section 5.3.5 that the achievable security of the iris fuzzy commitment system is $H(S|W) = 54.42$ bits at $L_S = 72$ according to our iris model. The really achieved security with Hadamard code and RS code is only 14 bits (see Section 5.3.2). We can also use Def 1 and 2 in order to measure the security and privacy. A fuzzy commitment scheme is $(\mathcal{T},\varepsilon)$- secure in the advanced model with $\mathcal{T} = O(1)$ and $\varepsilon = \log_2 G(S|W)$, where $G(S|W)$ is the conditional guessing entropy of S given W and implies the average number of guesses required to successfully estimate S. The hash function is necessary in the reconstruction and we use the computational time of a perfect hash to quantify $\mathcal{T}$. From the privacy point of view, a fuzzy commitment scheme is $(t,\mathcal{T},\varepsilon)$- preserving in the advanced model with $t = 0$, $\mathcal{T} = O(1)$ and $\varepsilon = \log_2 G(X|W)$. Here t is equal to zero, because the biometric feature is linked with the secret through W and the corresponding features can be totally recovered with known secrets.

In both theoretical and practical analyses with possible attacks, the distribution of binary biometric features is the key in the assessment. Without knowing their probability distribution, it is not possible to compute the information-theoretical metrics. An adversary can perform an efficient attack with the help of information about the distribution. Therefore, we made an effort in Chapters 4 and 5 to study the distribution of the features. We used two models, the second order dependency tree and the Markov model for the 3D facial features and the iris features, respectively. The use of statistical models can limit the estimation complexity. The challenge is to find an appropriate model for the biometric features. Sometimes further assumptions and simplifications are necessary such that features can be fitted to the chosen model. The empirical non-parametric methods are more accurate, however, their complexity can grow very fast with the dimensionality of the features and they are hard to use in practice.

In Section 5.3.4, we used a cracking algorithm to reconstruct the iris features from their secure templates. In the non-perfectly secure systems, the computational time of one reconstruction attempt is larger than that of the hash function. In this case, the secret is no longer uniformly distributed given the auxiliary data and the number of necessary reconstruction attempts is much smaller than that in the case of perfect secure systems. The candidates of a secret need to be stored and their probabilities must be calculated and ranked. More computational power is required. Here we use $O(1)$ to give a very loose lower bound of the required computational time. The required memory can be quantified with $H(S|W)$.

Linkability is a serious problem in the fuzzy commitment scheme. It is caused by the inevitable privacy leakage and possible personal identifiable information in protected templates. The resistance to linkability can be improved, if an optimal coding method is used and privacy leakage is minimized. Moreover, it should be avoided to store any personal identifiable information. Ideally, protected templates are totally random.

In the *collision* model, the security is dependent on the *FAR* of a system. An adversary can perform a *FAR* attack and find biometric data in his database, that can pass the pseudonymous identifier verification process. Here the search space is limited to the database of an adversary. The average success rate is equal to the *FAR* and the average number of guesses needed is $1/FAR$. The fuzzy commitment scheme is $(\mathcal{T},\varepsilon)$- secure in the collision model, where $\varepsilon = -\log_2 FAR$ and $\mathcal{T}$ depends on the complexity of the whole pseudonymous identifier verification process including feature extraction and pseudonymous identifier recorder. The data found in the adversary's database is also close to the biometric data of the target person. Therefore, this attack also harms privacy. We can use the same metrics of the security definition to measure the privacy preserving ability. In this case, the accuracy of the reconstruction of biometric data is equal to the tolerance of the *PI* verification process by default. In this threat model, linking different applications is not possible due to the lack of system information. Of course, the similar biometric data, that an adversary finds, can be falsely accepted in other applications. The security performance is strongly related to recognition performance, namely the achieved *FAR*.

We showed the evaluation of the fuzzy commitment scheme for different threat models. The evaluation results are strongly dependent on the information and resources available to an adversary. Therefore, the evaluation results of distinct models can be quite different. A system designer should choose a threat model subject to the security and privacy requirements of the application at hand. By designing an algorithm, a rigorous assessment is recommended. Assessment of only the naive model is not sufficient. Both the advanced and collision models need to be taken into account. Especially in the advanced model, all protection goals identified in Section 3.2.2 can be assessed, which is very helpful for an algorithm developer to find weaknesses or potential flaws.

6.1.2. Comparison of Different Biometric Cryptosystems

The proposed framework is helpful to give a rigorous assessment of a template protection system. Additionally, it creates a basis to compare different systems regarding security and privacy. In this section, we compare fuzzy commitment for 3D face recognition and iris recognition using the evaluation results obtained in Chapters 4 and 5. In order to demonstrate the generalizability, an existing security assessment on the fingerprint fuzzy vault system is also included.

The details of the fuzzy vault algorithm and the security analysis are given in Section 3.5. We use the results of Nandakumar et al. in [NJP07] with the FVC2002-DB2 database. In their experiment, 24 minutiae points are used in the enrolment, the degree of the polynomial $d = 8$, and 224 chaff points are generated. The length of the secret is 128 bits. The *FAR* of 0.01% at *FRR* of 9% is achieved with one reference and one query fingerprint image per comparison. With Eq 3.20, they calculated the expected number of combinations, which is needed to be evaluated in order to find the genuine points and retrieve the secret. These are 2.5×10^9 combinations corresponding to 31.24 bits.

For the 3D face recognition system, we use the results with the FRGC database including version 1.0 and 2.0. The feature length of 476 and the length of BCH-codeword of 255 are chosen. For the iris recognition system, the results with CASIA-V1.0 database and the feature length of 9600 with iris mask are utilized.

According to the evaluation framework proposed in Section 3.2.4, we analyse three template protection systems regarding the protection goals, namely security, privacy protection ability and unlinkability in different threat models. In order to compare different algorithms, *generally applicable* evaluation metrics are necessary. In Section 3.2.4 we give Def 1 and 2 to quantify the security of *PI* and the irreversibility of biometric features. The advantage is that the metrics can be calculated empirically as well as theoretically. In the following, we will make use of these definitions and the metrics measuring privacy leakage and unlinkability (see Sections 3.2.3, 3.4 and 3.5). The differences of the three systems in privacy and security performance are shown.

6.1.2.1. Comparison of Security

In Def 1, the metrics ε and $\mathcal{T}$ are proposed, which show the average number of attempts needed to guess a pre-image of *PI* and the computational time required for one attempt. They represent average computational complexity required in an attack scenario. These unified metrics allow the comparison of different template protection systems. In Table 6.1, the security assessment using Def 1 in three threat models is displayed. Both fuzzy commitment and fuzzy vault belong to biometric cryptosystems and the *PI* in their systems is the hash of randomly generated secret. In the naive model, an adversary can only guess the plain text of the hash. Therefore, ε is dependent on the secret size and $\mathcal{T}$ corresponds to the computational time of the hash function. The assessment in the naive model indicates the computational complexity of a brute force attack on the *PI*.

In the advanced threat model, ε reduces strongly, since the estimation of secrets becomes easier with knowledge about the system and biometric features. As shown in the previous section, ε is the logarithmic representation of the conditional guessing entropy $G(S|W)$. In both the 3D face and the iris recognition systems, we can not measure $G(S|W)$ directly. However, in the face recognition system, the BCH-coding is used. A lower bound of $G(S|W)$ can be calculated with Eq 4.21 and ε in Table 6.1 shows this lower bound. For the iris recognition system, we empirically calculate the average number of attempts needed by the cracking algorithm. This result is dependent on the cracking algorithm and its settings. It is an approximation of ε. The result of fingerprint recognition is calculated with Eq 3.20 and cited from [NJP07]. Eq 3.20 is based on the assumption that an adversary can not distinguish the chaff points from genuine ones. The chaff points and genuine points should have the same statistical properties and all the combinations of subsets should be equally probable minutiae sets. Otherwise Eq 3.20 will overestimate the security. In fuzzy commitment, the reconstruction still relies on the hash function, therefore, $\mathcal{T}$ is the same as in the naive model. In fuzzy vault, polynomial reconstruction is the dominant operation in the reconstruction. Its $\mathcal{T}$ shows the computational time of a polynomial reconstruction, which is equal to $O(nlog^2(n))$ [Sha79].

As shown in the previous section, ε and $\mathcal{T}$ in the collision model depend on the *FAR* and the computational time of the whole verification process. Table 6.1 shows ε of three systems, and ε varies from 5.18 bits to 13.29 bits. We can reduce the *FAR* to achieve higher security, however, *FRR* will increase and the system will become inconvenient. The best way is to design a better feature extraction algorithm and a better template protection algorithm to improve the recognition performance.

In the naive model, the fingerprint fuzzy vault system has the largest secret size. In the advanced model, it also has the highest ε and $\mathcal{T}$. In the collision model, its ε is equal to 13.29 bits with the smallest *FRR*. Therefore the fingerprint system is the most secure one in all threat models. Similarly, we can recognise that the iris fuzzy commitment system is the second secure one.

System	L_S	Naive Model		Advanced Model		Collision Model
		$\varepsilon = L_S - 1$	$\mathcal{T}$	ε	$\mathcal{T}$	$\varepsilon = -\log_2 FAR$ $(FAR@FRR)$
Fuzzy Commitment for 3D face	47	46	$O(1)$	5.20	$O(1)$	5.18 (2.75%@9.64%)
	55	54	$O(1)$	6.79	$O(1)$	6.24 (1.32%@17.68%)
	71	70	$O(1)$	11.13	$O(1)$	6.48 (1.12%@19.97%)
Fuzzy Commitment for Iris	40	39	$O(1)$	7.65	$O(1)$	6.86 (0.86%@19.96%)
	56	55	$O(1)$	10.93	$O(1)$	7.18 (0.69%@21.30%)
	72	71	$O(1)$	14.25	$O(1)$	7.41 (0.59%@22.74%)
Fingerprint Fuzzy Vault	128	127	$O(1)$	31.24	$O(nlog^2(n))$	13.29(0.01%@9%)

Table 6.1.: Security assessment of the three template protection systems in the naive, advanced and collision threat models

If a fuzzy commitment scheme is perfectly secure, the security assessment with the naive model is equal to that with the advanced model. Due to strong dependency of 3D face features and iris features, ε in the naive model is much larger than in the advanced model. Although ε increases with the secret length, the secret length can not represent the security in the advanced and collision model. In many papers, only the secret length is given for the security assessment, which is definitively not proper in a rigorous analysis. The security of fuzzy vault is determined by the hardness of polynomial reconstruction among numerous chaff points. The complexity of the reconstruction should be high enough to guarantee computational security.

6.1.2.2. Comparison of Privacy Protection Ability

We analyze the privacy protection ability. In the naive model, an adversary can not obtain information about biometric data lacking of knowledge about the systems. In the collision model, he can only find biometric data, from which the same or a similar *PI* as that of the target person can be generated. Therefore, it makes more sense to assess privacy protection ability in the advanced model. The results are shown in Table 6.2. The privacy leakage measures the amount of information about biometric features contained in protected templates. The irreversibility of *PI* is measured with Def 2. The threshold t in the definition is equal to 0.

System	Uncertainty of bio. features	L_S	Privacy Leakage	Irreversibility	
				ε	$\mathcal{T}$
Fuzzy Commitment for 3D face	153.7	47	84.3	67.4	$O(1)$
		55	82.1	69.6	$O(1)$
		71	77.5	74.2	$O(1)$
Fuzzy Commitment for Iris	4325.88	40	4317.12	7.65	$O(1)$
		56	4314.06	10.93	$O(1)$
		72	4311.00	14.25	$O(1)$
Fingerprint Fuzzy Vault	923.83	128	892.59	31.24	$O(nlog^2(n))$

Table 6.2.: Privacy assessment of the three template protection systems in advanced model

The privacy leakage of the fuzzy commitment schemes is evaluated as $H(X|W)$. The entropy of the 3D facial features is 153.7 at a feature length of 476. In the 3D face recognition system, only 255 elements of the whole feature vector are used in the fuzzy commitment system. If the secret is compromised, still 221 bits of the features need to be estimated. Therefore, the 3D facial feature has less privacy leakage in comparison with the other two systems. In addition, its irreversibility is higher than the security of *PI* in the advanced model[1]. In contrast, all bits in the iris features are used in the fuzzy commitment scheme. The irreversibility is equal to the security in the advanced model. The entropy of iris features is 4325.88 at a feature length of 9600. The privacy leakage is extremely high.

All these results are based on the statistical models, which are utilized to simulate the distribution of biometric features. A more accurate estimation is possible, if better methods can be found for modeling the distributions. Additionally, it is shown that the privacy leakage increases when decreasing the secret size in fuzzy commitment. This confirms the similar conclusion drawn in [Ign09].

[1] The threshold t in Def 2 shows how precise an adversary wants to reconstruct biometric features. If a larger t is chosen, the irreversibility of the protected 3D face system becomes smaller.

The irreversibility of the fuzzy vault scheme is also equal to the security, since the compromise of the secret is accomplished with exposure of minutiae information. In [NJP07], a minutia is represented by a 16 bit feature, 6 bit for the vertical dimension, 5 bit for the horizontal dimension and 5 bit for the orientation. As shown in Section 3.5, the uncertainty of a feature set containing 24 minutiae is equal to $\log_2\left(2^5 \cdot \binom{2^{11}}{24}\right) = 923.83$. [2] Given a vault set containing 224 points, the uncertainty reduces to the complexity of finding 24 genuine points among the vault set. We use Eq 3.21 and obtain the privacy leakage of 892.59 bit.

Comparing the uncertainty of biometric features with the privacy leakage in Table 6.2, the 3D face system has the smallest privacy leakage. The iris system has the worst privacy preserving ability. The iris system and fingerprint system expose more than 96% biometric information.

6.1.2.3. Comparison of Unlinkability

Finally we investigate the unlinkability. In Chapters 4 and 5 we showed that both fuzzy commitment systems are vulnerable to cross matching. In the 3D face system, an *EER* of 5% can be obtained by linking the position vectors. In the iris system, an *EER* of 16.34% is achieved with the decodability attack. The 3D face system is vulnerable to privacy leakage amplification, however, the iris system is resistant to the leakage amplification. The fuzzy vault system is unprotected to both cross matching and privacy leakage amplification. As shown in [SB07], linking protected templates of the same subject can retrieve the genuine minutiae in the vault set. Unfortunately, no assessment on the linkability is given in the cited fuzzy vault paper [NJP07]. The feasibility of linkage attack was proved by Kholmatov et al. in [KY08]. The databases and implementation used in their fuzzy vault scheme are not exactly the same as in [NJP07]. Therefore, we can not use it in our comparison. Nevertheless linkage is a serious problem for fuzzy vault.

In this section we analyzed the security, privacy protection ability as well as unlinkability of three template protection systems. From the security point of view, the fingerprint fuzzy vault system has the best performance. However it has large privacy leakage and is unresistant to the linkage attack. The security of the iris fuzzy commitment system is slightly better than that of the 3D face system. However, its privacy leakage is quite high. All these three systems can not fulfill all the protection goals. Further improvement is necessary.

6.2. Transformation-Based Algorithms

Till now we investigated the security and privacy of biometric cryptosystems. Transformation-based algorithms are also an important category of template protection. Biometric cryptosystems can generate distinct secrets from biometric data. In contrast, transformation-based methods either distort or randomize biometric data such that the original data can not be recognised any more. In these algorithms, user- and application-specific transformation parameters are used, which are the auxiliary data (AD) and parts of protected templates as described in Section 2.2.2. Normally they need to be kept *secret*.

The main focuses of transformation-based algorithms are to enable renewability and the non-invertibility with good recognition performance: Changing transformation parameters should result in different transformed data (*PI*), which do not match each other even if they are derived from the same subject; it is hard to derive the original data from its transformed template; additionally, transformation functions should preserve the recognition performance of the original biometric system.

[2] The real entropy of minutiae features is lower than the estimated result, since the position of a minutiae is correlated with its angle information. The encoding of minutiae in [NJP07] contains redundancy and is not optimal. However, our assessment is based on the assumptions and parameters used in [NJP07] and the correlation is ignored.

In Table 6.3 we give the examples of some important transformation-based algorithms and show their *AD* and *PI*. In this section we focus on transformation-based algorithms and *validate* the evaluation framework proposed in Section 3.2. We will define the different threat models and analyze the corresponding protection goals for different algorithms.

	Algorithm	*AD*	*PI*
Cancelable Biometrics	Face image morphing [RCB01]	Morphing parameters	Transformed image
	Cartesian transformation of minutiae [RCCB07]	Transformation parameters	Transformed minutiae
	Polar transform of minutiae [RCCB07]	Transformation parameters	Transformed minutiae
	Surface folding transformation of minutiae [RCCB07]	Transformation parameters	Transformed minutiae
Biohashing	Random projection& binarization [JLG04, TJC*06, CTGN05]	Projection matrix	Binary vector
	Complex number randomization & phase binarization	Randomization vector	Binary vector
	Random binarization [AL09]	Randomization threshold	Binary vector
Cancelable biometrics filters	Convolution with a random kernel & MACE [SKK04]	–	Encrypted MACE filter

Table 6.3.: Examples of transformation-based algorithms

6.2.1. The Threat Models

The threat models are the important precondition for the assessment and can influence the evaluation results. In this section we define different threat models for transformation-based algorithms.

Evaluation of transformation-based algorithms in the naive model is not necessary, since protected templates mean nothing outside the algorithms and an adversary cannot perform any attack. In the rest of the section we skip the assessment with the naive model.

The assessment with the advanced model assumes that an adversary knows the template protection algorithms. Secret auxiliary data is an important security and privacy factor. The advanced model can be further refined with following assumptions:

- AM1: An adversary has no access to *AD*.
- AM2: An adversary has indirect access to *AD*. He can make use of *AD* as well as the transformation functions without knowing *AD* exactly.
- AM3: An adversary has direct access to *AD*. He knows *AD* and can use both *AD* and the transformation functions.

From AM1 to AM3, the complexity for an adversary to calculate a pre-image or to retrieve biometric features decreases.

Similarly, the assessment in the collision model can be divided into the cases with or without *AD*. We also define the two sub models:

- CM1: An adversary has no access to *AD*.

- CM2: An adversary has access to *AD*.

Neither CM1 nor CM2 requires the detailed information about *AD*. However, CM2 assumes that an adversary can use the *AD* of the target person during a collision attack, while in CM1 he cannot.

Based on the threat models we can design an evaluation process to measure the protection goals. In practical evaluation an attack algorithm can be used and its efficiency quantifies the protection goals. During experiments we can define different kinds of genuine and impostor comparisons to evaluate the efficiency of an attack algorithm. In Table 6.4 we give an overview of possible comparisons and the corresponding protection goals, which can be assessed. Genuine comparisons using the same *AD* show the usability (robustness) of transformed features (*PI*) and those using different *AD* represent the unlinkability of CM1. Impostor comparisons with stored *AD* show the discriminative power of *PI*s in the same transformed feature space, while impostor comparisons with different *AD* show the general discriminative power of *PI*s. Impostor comparisons also represent the security in different collision models. Genuine comparisons between biometric data and the data reconstructed from *PI* with stored *AD* display the security in advanced model AM2 or AM3. Those with different *AD* show the accuracy of a reconstruction function and can evaluate irreversibility in advanced model AM2 or AM3. A generalized reconstructed datum can be matched with protected templates of the same subject and accepted in other applications. Table 6.4 is helpful for the design of evaluation processes. In the following we analyze achievements of the protection goals for transformation-based algorithms in different threat models.

Comparison		stored *AD*	different *AD*
Genuine	biometric vs. biometric data	usability of *PI* (performance) security (collision model CM2)	unlinkability (collision model CM1)
	biometric vs. reconstructed data	security (advanced model AM2, AM3)	Irreversibility (advanced model AM2, AM3)
Impostor		discriminability (performance) security (collision model CM2)	discriminability (performance) security (collision model CM1)

Table 6.4.: The different kinds of comparisons and the assessment of corresponding protection goals

6.2.2. Security Assessment

According to Section 3.2.3, the security of template protection is determined by the complexity to construct a pre-image $\hat{M}$, which can pass through the *PI* verification process, $PIC(PIR(AD,\hat{M},AD)),PI) = 1$. Under threat model AM1, the reconstruction of a pre-image is hard. Under threat models AM2 and AM3, most of the transformation-based algorithms are reversible.

The *cancelable biometrics* for fingerprint minutiae applies different (many-to-one) functions to change minutiae. In [NJ09], Nagar et al. investigated its security. The important step is the calculation of the pre-image of each minutia. The pre-image is a set of candidate minutiae, which can produce the same transformed minutiae as those stored in a protected template. They computed the transformed positions of all pixels in the fingerprint area and found the candidate positions of a particular transformed minutia. Obviously, any combination of the minutiae in the individual pre-images is a valid $\hat{M}$. As calculating the pre-image, it is not necessary to know the transformation parameter, namely *AD* exactly. It is sufficient for an adversary to use the transformation function. It corresponds to the assessment in threat model AM2.

In *biohashing* based on random mapping as shown in [CTGN05, JLG04], a biometric feature M is projected onto randomly generated basis vectors and the new feature is binarized. The algorithm is conducted in the following steps:

1. Generate n orthogonal normalized random vectors with length m ($n \leq m$), $\mathbf{R} = \{\mathbf{r}_j | j \in [1, \cdots, n]\}$ with $\mathbf{r}_j^T \cdot \mathbf{r}_{j'} = 0$ for $\forall j \neq j'$; $\mathbf{r}_j^T \cdot \mathbf{r}_j = 1$ [3].
2. Calculate the inner product $\tau = [\tau_1, \cdots, \tau_n]\}$ of the biometric feature $M = [\mathsf{m}_1, \cdots, \mathsf{m}_m]$ and the random vectors. $\tau_j = M \cdot \mathbf{r}_j$.
3. Calculate $\mathbf{b} = [b_1, \cdots, b_n]$, by comparing τ with the binarization thresholds. $\mathbf{b} \in \{0, 1\}^n$ is the pseudonymous identifier and also called biohash.

In [CKYZ05] Cheung et al. evaluated the non-invertibility of this algorithm. They assumed that the projection matrix $\mathbf{R}$ and the biohashes $\mathbf{b}$ are available to an adversary. $\mathbf{b}'$ is a modified version of $\mathbf{b}$: $b'_j = 1$, if $b_j = 1$; or $b'_j = -1$, if $b_j = 0$. By $\tau = 0$. A valid $\hat{M} = \mathbf{b}' \cdot \mathbf{R}^*$, where $\mathbf{R}^*$ is a pseudo inverse of $\mathbf{R}$. It can be easily proved that any $\hat{M}$ fulfilling the following equation is a valid pre-image:

$$\hat{M} = (\tau + \Delta) \cdot \mathbf{R}^* \tag{6.1}$$

where $\Delta = [\delta_1, \cdots, \delta_n]$ with $\delta_i > 0$ for $b_i = 1$ and $\delta_i < 0$ for $b_i = 0$. Since $\mathbf{R}$ consists of pair wise orthogonal rows, its pseudo inverse exists (the definition of pseudo inverse can be found in [MV99]):

$$\mathbf{R}^* = \mathbf{R}^T \tag{6.2}$$

$\mathbf{R}^*$ has the property that $\mathbf{R}^* \cdot \mathbf{R} = 1$ and $\mathbf{R} \cdot \mathbf{R}^* \cdot \mathbf{R} = \mathbf{R}$, then:

$$\hat{M} \cdot \mathbf{R} = (\tau + \Delta) \cdot \mathbf{R}^* \cdot \mathbf{R} = \tau + \Delta \tag{6.3}$$

The binarization of $\hat{M}$ can give the same biohash $\mathbf{b}$ and $\hat{M}$ can pass through the verification process. This attack algorithm and security analysis correspond to the assessment with threat model AM3.

For the *cancelable biometric filter*, Adler proposed a hill climbing attack to find an operative image [Adl04], which corresponds to threat model AM1. Although there is no real implementation shown, he said that the comparison score of the queried and stored *PI* can be utilized in a recursive algorithm to improve the similarity between the reference image and the image submitted by an adversary. The detail of the algorithm is described in Section 3.1.2.

In the collision model, the security also depends on *FAR*. Normally FAR_{CM1} with threat model CM1 becomes smaller and a transformation-based algorithm can improve the dissimilarity between *PI* of different subjects. It is due to the use of user-specific *AD*. The threat model CM2 is stricter. A well-designed transformation function should not degrade recognition performance and preserve the same discriminative power even if *AD* is known to an adversary. The assessment with CM1 shows the renewability of an algorithm and the evaluation with CM2 shows the resistance against collision. For instance, Kong et al. showed in [KCZ*06] that zero *EER* can be achieved by biohashing algorithms with CM1. However, they demonstrated the decreasing of the recognition performance with CM2.

6.2.3. Privacy Assessment

Privacy assessment includes the privacy leakage and irreversibility of biometric information. The essential part is irreversibility, which is defined as the complexity to reconstruct a datum $\hat{M}$ close to biometric datum M of the target person. The privacy assessment requires more precise estimation of biometric data.

[3] A simple way to generate orthogonal random vectors is to apply Gram-Schmidt process to a set of random numbers.

The privacy performance of *cancelable biometrics* for fingerprint minutiae was evaluated in [RCCB07,NJ09]. In [RCCB07], Ratha et al. calculated the number of possible pre-images given the transformed features. It is the assessment based on a brute force attack with threat model AM1.

In [NJ09], Nagar et al. analyzed further the irreversibility. The pre-image of a transformed minutia is calculated, which may contain more than one candidates. With the general distribution of fingerprint minutiae, the candidate minutiae in the pre-image are ranked and an adversary can guess the original minutia based on the ranking list. They plotted the *effort*, namely the number of guesses, versus the *coverage*, the probability of the success retrieval. Their experiments showed that the coverage and effort also depend on the transformation parameters. It is also a drawback of this cancelable biometrics algorithm that the irreversibility varies with different parameters. Given v_i is a transformed minutiae, $i \in [1, \cdots, m]$ and m is the number of transformed minutiae. V_i is the pre-image of v_i, which contains l_i candidate minutiae and $\mathsf{m}_i \in \mathsf{V}_i$ is the original one. $H(\mathsf{m}_i|v_i)$ is the uncertainty about m_i given its transformed one v_i. The equation calculating $H(\mathsf{m}_i|v_i)$ was proposed in [NJ09]: $H(\mathsf{m}_i|v_i) = -\sum_{j=1}^{l_i} p(\mathsf{v}_{i,j}|v_i) \cdot \log(p(\mathsf{v}_{i,j}|v_i))$. It is a metric to quantify the irreversibility based on threat model AM3.

In [NNJ10], Nagar et al. also proposed an algorithm attacking *biohashing*, which can give more precise estimation of biometric features than Cheung' algorithm [CKYZ05]. In their algorithm, several features in a dataset are chosen in such a way that their biohashes with the projection matrix of the target person are very similar to the biohashes of that person. The optimization algorithm for constrained linear least-squares problems is used to find a biometric feature $\tilde{M}$, which has the minimum distance to a selected biometric feature and can result in exactly the same biohashes as the target one. The final estimation is an average of all $\tilde{M}$ calculated from the selected features.The experimental results on facial database showed significant similarity between the original images and reconstructed images. In order to improve the irreversibility, they also proposed a new binarization method, which adds two more binarization thresholds at λ and $100 - \lambda$ - quantile. The value in the first and the third quantiles is signed into 0 and the rest is signed to 1. With the factor λ, the continuity of the reconstructed images is broken and the uncertainty about the original images increases. However, they also showed that this algorithm reduces the recognition performance. The analysis is also based on threat model AM3.

We cannot find analysis on privacy protection ability of the face image morphing algorithm and cancelable biometric filters. The cancelable biometric filter has the advantage that random kernel used in enrolment is not stored. It increases the difficulty of reconstruction. More investigation on privacy is necessary for these algorithms. Additionally, a distance function as described in Def 2 is very helpful to quantify the accuracy of reconstruction.

6.2.4. Assessment of Unlinkability

In transformation-based algorithms, cross matching is avoided by using different transformation parameters. A transformed feature, PI, should have enough dissimilarity to the original feature as well as those transformed features generated from the same subject but with different parameters. For instance, the results in [RCCB07] show that the performance of genuine comparisons with different parameters is very similar to impostor comparisons of the original untransformed features with the cancelable biometrics for minutiae. In [TJC*06], Teoh et al. showed that Hamming distance of impostor biohashes approaches to binomial distribution. It indicates that the resulting biohashes are perfectly random bit strings. In [SKK04], Savvides et al. also visualised the original and transformed MACE filters with cancelable biometric filter. Convolution with different kernels changes strongly MACE filters.

Moreover, leakage amplification needs to be analyzed. As shown in the previous section, the inversion algorithm proposed in [NJ09] can estimate the candidate minutiae from a transformed one. The original minutia can be simply retrieved by overlapping pre-images of different secure templates generated from the same user. Similarly, the reconstruction algorithm in [NNJ10] can give more accurate estimation with more biohashes and the projection matrixes. In these algorithms, combining more protected templates of the same subjects can cause more privacy leakage. In the following we show another example of the biohashing using scalar randomization.

The Biohashing based on scalar randomization is introduced in [AL09], where biometric features are binarized with randomly generated thresholds. Assume that $\mathbf{x}_k = [x_{k,1}, \cdots, x_{k,n}]$ is a biometric feature of subject k. The interclass probability density function of x_i is denoted as p_{x_i}, where x_i is the i-th element of $\mathbf{x}$. The cumulative function of p_{x_i} is $f_{x_i}(\tau) = \int^{\tau} p_{x_i}(\varepsilon)d\varepsilon$ with $f_{x_i -} = 0$ and $f_{x_i +} = 1$. The binarization threshold of $x_{k,i}$ is $\mathbf{t}_{k,i} = [t^1_{k,i}, \cdots, t^m_{k,i}]$, which is randomly generated with the distribution $p_{t_i} = p_{x_i}$. Biohash $\mathbf{b}_{k,i} = [b^1_{k,i}, \cdots, b^m_{k,i}]$ is the binarized feature of $x_{k,i}$:

$$b^j_{k,i} = \begin{cases} 1 & \text{if} \quad x_{k,i} \geq t^j_{k,i} \\ 0 & \text{if} \quad x_{k,i} < t^j_{k,i} \end{cases} \tag{6.4}$$

Multiple bits can be extracted from a single element in a feature vector. The resulting biohashes have the following properties:

- For a bit b^j_i of a unknown user, the probability $p(b^j_i = 1)$ is:

  $$\begin{aligned} p(b^j_i = 1) &= \int p_{x_i}(x_i) \int^{x_i} p_{t_i}(t^j_i) dt^j_i \cdot dx_i \\ &= \int \int^{x_i} p_{t_i}(t^j_i) dt^j_i \cdot df_{x_i}(x_i) = \int f_{x_i}(x_i) df_{x_i}(x_i) \\ &= (\frac{1}{2} f_{x_i}(x_i)^2)^+_- = \frac{1}{2} \end{aligned} \tag{6.5}$$

  It indicates that the bits from different subjects are uniformly distributed, since the binarization thresholds have the same distribution as the biometric features.

- $p(b_{k,i} = 1)$ is the probability that a bit in biohash $\mathbf{b}_{k,i}$ of subject k is equal to 1:

  $$\begin{aligned} p(b_{k,i} = 1) &= \int^{x_{k,i}} p_{t_i}(t^j_{k,i}) dt^j_{k,i} = f_{x_i}(x)^{x_{k,i}}_- \\ &= f_{x_i}(x_{k,i}) \end{aligned} \tag{6.6}$$

  It shows that the bits in $\mathbf{b}_{k,i}$ of subject k are identically and independently distributed with the probability of $f_{x_i}(x_{k,i})$. The distribution of $\mathbf{b}_{k,i}$ is dependent on $x_{k,i}$. $H(\mathbf{b}_{k,i})$ is the entropy of $\mathbf{b}_{k,i}$:

  $$H(\mathbf{b}_{k,i}) = m \cdot H(f_{x_i}(x_{k,i})) \tag{6.7}$$

  For all users, the average entropy of $\mathbf{b_i}$ is calculated as:

  $$H(\mathbf{b}_i) = m \cdot \int^+_- p(x_{k,i}) H(f_{x_i}(x_{k,i})) dx_{k,i} = m \cdot \int^1_0 H(f_{x_i}(x_{k,i})) df_{x_i}(x_{k,i}) \approx 0.74 \cdot m \tag{6.8}$$

  It shows the randomization ability of this Biohashing algorithm.

- The probability $p(b^j_{k,i} = b^j_{k',i})$ that the j-th bits from different users are equal can be calculated:

  $$\begin{aligned} p(b^j_{k,i} = b^j_{k',i}) &= f_{x_i}(x_{k,i}) f_{x_i}(x_{k',i}) + (1 - f_{x_i}(x_{k,i}))(1 - f_{x_i}(x_{k',i})) \\ &= 2 f_{x_i}(x_{k,i}) f_{x_i}(x_{k',i}) - f_{x_i}(x_{k,i}) - f_{x_i}(x_{k',i}) + 1 \end{aligned} \tag{6.9}$$

  Dependency between the bits from different subjects exist. They are independent only if $f_{x_i}(x_{k,i}) = 0.5$ or $f_{x_i}(x_{k',i}) = 0.5$ (Eq 6.9 is equal to 0.5).

Combining biohashes of the same subject helps to precisely retrieve biometric features. Assume that an adversary collects m bit biohashes of $x_{k,i}$. The Hamming weight of these bits equals l. Then l is binomially distributed with m and $f_{x_i}(x_{k,i})$. From the properties of binomial distribution, we obtain:

$$E\{\frac{l}{m}\} = f_{x_i}(x_{k,i}) \tag{6.10}$$

$\hat{f}_{x_i}(x) = \frac{l}{m}$ is an estimation of $f_{x_i}(x)$. The larger m is, the more reliable is the estimation. Depending on whether $\hat{f}_{x_i}(x)$ is close to 0 or 1, a prediction of new biohashes extracted from x is possible. Moreover, if $f_{x_i}(x)$ is known, an estimation of x_i can be given. Biohashes with scalar randomization have poor randomness and poor resistance to leakage amplification. The proposed attack can be performed in threat model AM2.

6.3. Summary

In this chapter we firstly analyzed and compared the security and privacy performance of three different biometric cryptosystems, the fuzzy commitment scheme for 3D face recognition, the fuzzy commitment scheme for iris recognition and the fuzzy vault algorithm for fingerprint recognition with the help of the evaluation framework. It not only allows a systematic assessment of individual algorithm but also enables the comparison of different protected biometric systems.

We investigated the protection goals for three main threat models. It is shown that privacy and security assessment are strongly dependent on the threat models. For instance the security of the 3D face and iris systems in the naive model is much higher than in the advanced model. The naive model is based on a simple assumption that an adversary knows nothing about systems. In a rigorous assessment, advanced model and collision model are indispensable. Our proposed security and privacy definitions provide unique metrics, which allow both empirical and theoretical measurement on security of *PI* and irreversibility of biometric features. We used these metrics to compare three template protection systems and showed that the fuzzy vault algorithm for fingerprint recognition has the best security and irreversibility.

A disadvantage of these systems is the high privacy leakage. Although the privacy leakage in fuzzy commitment is unavoidable, the dependency in the 3D face features and iris features strengthens the privacy leakage. The 3D face system has less privacy leakage than the iris system, since not all bits in the 3D features are used in fuzzy commitment. However, the position of selected features must be stored as a part of secure templates in the protected 3D face system. It causes the serious cross matching problem. The protected iris recognition system is also vulnerable to cross matching of the auxiliary data due to high privacy leakage. In the cited paper of the fuzzy vault implementation, no evaluation on linkability is given. But fuzzy vault is not resistant to cross matching either and shown in other literatures. All these systems can not fulfill the requirement of unlinkability.

In the second part of this chapter we validated the evaluation framework in transformation-based template protection algorithms. It was shown that our identified protection goals cover the security and privacy requirements on transformation-based as well. In contrast to biometric cryptosystems, the evaluation of transformation-based algorithm relies on practical attacks. The theoretical metrics are only limitedly utilized in the analysis of special attacks. Naive model is not applicable, since only experienced adversary or someone owning a large biometric database can perform an attack. The advanced and collision models can be further divided into the sub models depending on access to *AD* (secret transformation parameters), since *AD* is crucial by calculating a pre-image of *PI* or retrieving biometric features. The security in collision model is determined by *FAR*. However, it should be evaluated with two collision threat models: a unauthorized subject uses the *AD* of authorized subject and a unauthorized subject uses his own *AD* and wants to be verified as an authorized subject.

Additionally, if the transformation functions as well as their parameters are compromised, it is straightforward to reconstruct a datum, which can spoof the verification process. However, retrieving the original biometric data is more complicated. The transformation functions used in cancelable biometrics have many-to-one property. In biohashing, biometric data is randomized. Cancelable biometric filter makes biometric data extremely noisy. These increase the difficulty to reconstruct the original biometric data. Furthermore, there is no references linked directly to biometric data and a precise reconstruction is hard. Transformation-based algorithms have good privacy protection ability. However, more investigation on privacy especially with quantitative assessment is necessary.

Due to user-specific transformation parameters, these algorithms have good resistance to cross matching. However, the risk of leakage amplification is high. Combining secure templates of the algorithms such as cancelable biometrics and biohashing with random projection can strengthen privacy leakage, if *AD* is known. In some algorithms such as biohashing using scalar randomization can expose information and leakage amplification is possible, even if *AD* is not explicitly given.

As conclusions, the proposed evaluation framework is a useful evaluation tool for both biometric cryptosystems and transformation-based algorithms. The existing security analysis measured one or more protection goals in the framework. More assessment of different algorithms is still necessary.

7. Conclusions and Future Work

Biometrics provides the nice security property of binding an identity to its owner and is therefore an important tool to fight identity fraud. Nevertheless, the related potential privacy and security risks should not be underestimated. Biometrics can not be applied at the cost of sacrificing user's privacy. Biometric data should be safeguarded against internal and external attackers in order to prevent identity theft and cross matching. Biometric template protection techniques have been developed to overcome these privacy and security drawbacks.

The research interests in this area should not be limited to a successful integration of template protection with good recognition performance. It is also important to prove that these algorithms can really improve security and privacy. Practical applications need a comprehensive rigorous assessment with quantitative measurements. This thesis meets the challenge of quantifying the security and privacy of biometric template protection.

The research question "*how can we make a comprehensive and systematic assessment of the privacy and security performance of biometric template protection algorithms*" is solved. The essential steps of an assessment, determining evaluation criteria and threat models, and designing evaluation process were identified. The formal definitions of privacy and security were given and a basis of ranking different algorithms was provided. My concept of systematic evaluations was validated with rigorous assessments of different template protection systems. Their privacy and security performance are compared.

7.1. Conclusions

The main contribution of this thesis is to propose a *generalized evaluation framework* for privacy and security assessment. It answers the main research question. The framework supports a systematic assessment of different algorithms. Its essential components include protection goals, threat models and evaluation metrics. Protection goals represent the objectives which we want to achieve with template protection. Three protection goals namely security, privacy preserving ability and unlinkability, were proposed. The security represents the hardness for an adversary to generate a datum, which can fool the verification process. Privacy preserving ability measures the hardness to retrieve biometric data and information about biometric data contained in a protected template. The unlinkability measures whether a protected template contains personal identifiable information and whether combining protected templates can reduce the security or privacy preserving ability. The protection goals cover thoroughly the requirements on template protection and are the *evaluation criteria*.

In order to measure the attainment of the protection goals, the ability of an adversary regarding information and computational resources available for him are defined with the threat models. They are the prerequisites for an evaluation. Without them, the security measurement is meaningless, since the validated scenario is not clear. We propose three threat models: The naive model assumes that adversaries have very limited information about the system. The advanced model applies Kerckhoffs' principle, that adversaries know details of the system and properties of biometric features. The collision model assumes that adversaries own a large biometric database and exploit inaccuracies of a biometric system. The threat models also determine which system parameters can be accessed during an assessment or an attack.

If protection goals and threat models are determined, the metrics measuring protection goals and the corresponding evaluation process can be developed. On the one hand, theoretical analyses can be used to measure the protection goals directly with e.g. information-theoretical metrics. On the other hand, practical analyses based on individual attacks are also possible to show security and privacy performance in practice. Theoretical and practical analyses complement each other. The framework describes the formal workflow for an evaluation. It is an indispensable tool for privacy and security assessment.

Additionally, we define $(\mathcal{T},\varepsilon)$-secure and $(\mathcal{T},\varepsilon,t)$- preserving for template protection, which describe security and irreversibility of protected templates respectively. The metric $\mathcal{T}$ shows the computational time required of one attack attempt and the metric ε shows the average number of attempts needed to achieve an attack objective. Together, they quantify the computational complexity of attacks. The metric t determines the desired reconstruction accuracy of biometric data. These unified metrics enables comparison of different protected systems regarding their security and irreversibility.

The second contribution is to validate the framework and to assess strictly two biometric template protection systems, the fuzzy commitment scheme for 3D face recognition and the fuzzy commitment scheme for iris recognition. A novel algorithm utilizing the histogram of the depth information is developed to characterize the 3D face surface. It is successfully integrated in fuzzy commitment. The experimental results using the FRGC databases show a good recognition performance while achieving a high secret size. Additionally, an open source iris recognition algorithm with Gabor filter is used and the protection scheme proposed by Hao is implemented, which is a fundamental work protecting iris data.

I carefully analyzed the statistical distribution of 3D face features and iris features as well as the interclass and intraclass error patterns. The intraclass bit errors are not uniformly distributed in a feature vector. The coding methods used in fuzzy commitment are not optimal. Additionally, strong dependencies exist in these features, since they describe the local characteristics of a 3D face or an iris. A second order dependency tree is used to simulate the dependency of 3D features. Iris features can be well described with a Markov model. Based on this, the security and privacy were measured with information-theoretical metrics. Two cross matching attacks were applied to link the protected templates. In both systems, the achieved security is very poor and high privacy leakage is observed in the advanced threat model. The results showed that the feature dependency has strong influence on security and privacy. In the security analysis of fuzzy commitment, any assumption on the distribution of biometric features must be made very carefully. If dependency of features is ignored, security can be highly overestimated. Moreover, both protected systems suffer from cross matching. In the protected 3D face system, privacy leakage can be amplified by combining two protected templates of the same subject.

The security and privacy performance of both systems are not satisfactory. The reason is that the optimal performance of a fuzzy commitment scheme can only be achieved, if binary biometric features are uniformly and independently distributed. It is a very strict condition, which is hard to fulfill. The thesis shows that there exists the possibility to improve the security by changing the coding methods. However, in order to prevent security leakage inherently, better binarization processes or alternative template protection schemes are necessary.

The third contribution is to compare two fuzzy commitment systems with a fuzzy vault system for fingerprint recognition using the framework. In order to enable a comparison, the security and privacy definitions quantifying security and privacy from computational complexity point of view were used. The fuzzy vault system outperforms the other two algorithms in security and irreversibility. However, high privacy leakage exists in all the systems and they are vulnerable to cross matching.

In order to prove the generality, the framework was also validated using the transformation-based algorithms. The existing security analyses of these algorithms measure one or more protection goals based on corresponding threat models. The proposed framework is also suitable to evaluate these algorithms.

The assessment is very important for template protection to check security and privacy performance. The proposed framework enables rigorous assessments in practical applications. The security and privacy performance can be quantified. With the framework, potential weaknesses of an algorithm can be identified. It provides an overview of the privacy and security requirements. Algorithm designers can adopt a defensive perspective in the development and consider all the aspects in advance. It is much more efficient than current reactive perspective. It is essential for technology innovation. To promote and popularize these techniques, a provable security and privacy analysis is necessary and this framework is an indispensable tool. Additionally, it creates a basis for benchmarking and certification. The framework is flexible and system designers can derive different evaluation processes for specific applications to select a suitable algorithm for their needs.

7.2. Future Work

In the future, the framework can be extended further. Potential directions are e.g. the enrichment of the evaluation metrics. The protection goals proposed in this work give only necessary criteria and the definitions of security and privacy are kinds of evaluation metrics. Universal and constructive criteria, which can guarantee security and privacy performance of template protection, are required.

Additionally, we can use the framework to evaluate more template protection algorithms regarding all protection goals. On the one hand, the achievement of the security and privacy requirements can be inspected; on the other hand, potential weaknesses can be detected. The distribution of biometric features plays an essential role in the assessment. More general models for distribution estimations can be used.

It is shown in this thesis that coding algorithms and binarization process strongly influence the security and privacy performance of fuzzy commitment. The future research directions are how to binarize dependent biometric features into uniformly independent binary features, and how to design appropriate coding methods. The theoretical analysis of helper data scheme predicts better security and privacy performance than fuzzy commitment. A better alternative to protect biometric features can be developed.

Unique metrics enable comparisons of different template protection algorithms regarding individual protection goals. However, in order to give an overall ranking including all protection goals, additional functions combining different evaluation metrics are necessary. Security and privacy are an important part for evaluation of biometric template protection systems. Moreover, a general evaluation should also include the recognition performance. The relation between recognition performance and security should be further analyzed.

A. Probability and Information Theory

A.1. Probability and Entropy

The probability shows the likelihood of occurrence of an event. Assume that X and Y are two discrete random variables. $\mathcal{X}$ and $\mathcal{Y}$ are the collections of all the possible X and Y. The probability that X is equal to x is denoted as:

$$p(x) = Pr\{X = x\} \quad \text{for} \quad x \in \mathcal{X} \tag{A.1}$$

$p(X,Y)$ is the joint probability of X and Y. $p(X|Y)$ is the conditional probability. The *Bayesian rule* can be expressed:

$$\begin{aligned} p(X|Y) &= \frac{p(X,Y)}{p(Y)} = \frac{p(Y|X) \cdot p(X)}{p(Y)} &\text{(A.2)} \\ p(X) &= \sum_{Y \in \mathcal{Y}} p(X,Y) &\text{(A.3)} \end{aligned}$$

Assume that X is a binary string of length N and $X = [\mathrm{x}_1, \mathrm{x}_2, \cdots, \mathrm{x}_N]$. X is statistically *independently distributed*, if $p(X) = \prod_{i=1}^{N} p(\mathrm{x}_i)$. X is *identically independently distributed*, if X is independently distributed and $p(\mathrm{x}_1) = p(\mathrm{x}_2) = \cdots = p(\mathrm{x}_N) = p$, where p is a constant. X is *uniformly independently distributed*, if X is identically independently distributed and $p = 0.5$.

The *entropy* shows the amount of information contained in a random variable. The entropy of X is defined as:

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x) \tag{A.4}$$

Similarly the *joint entropy* $H(X,Y)$ is defined as:

$$H(X,Y) = -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p(x,y) \log p(x,y) \tag{A.5}$$

Their *conditional probability* $H(Y|X)$ is defined as:

$$\begin{aligned} H(Y|X) &= \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) &\text{(A.6)} \\ &= -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log p(y|x) &\text{(A.7)} \\ &= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log p(y|x) &\text{(A.8)} \end{aligned}$$

The *mutual information* $I(X;Y)$ is defined as:

$$I(X;Y) = \sum_{x \in \mathcal{X}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \tag{A.9}$$

If $X_1, X_2, \cdots, X_n$ are n discrete random variables, the chain rule exist:

$$\begin{aligned}
I(X_1;X_2) &= H(X_1) - H(X_2|X_1) && \text{(A.10)}\\
H(X_1,X_2,\cdots,X_n) &= \sum_1^n H(X_i|X_{i-1},\cdots,X_1) && \text{(A.11)}\\
&= H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_{n-1},X_{n-2},X_1) &&\\
I(X_1,X_2,\cdots,X_n;Y) &= \sum_1^n I(X_i;Y|X_{i-1},\cdots,X_1) && \text{(A.12)}\\
H(X_1,X_2|X_3) &= H(X_1|X_3) + H(X_2|X_1,X_3) && \text{(A.13)}\\
I(X_1;X_2|X_3) &= \sum_{x_1,x_2,x_3} p(x_1,x_2,x_3)\log\frac{p(x_1,x_2|x_3)}{p(x_1|x_3)\cdot p(x_2|x_3)} &&\\
&= H(X_1|X_3) - H(X_1|X_2,X_3) && \text{(A.14)}
\end{aligned}$$

Relative entropy, also called Kullback-Leibler distance, KL-divergence is an efficient method to measure the difference of two probabilities. If $p(x)$ and $q(x)$ are two probability functions, Kullback-Leibler distance is defined as follows:

$$\begin{aligned}
D(p||q) &= \sum_{x\in\mathbf{x}} p(x)\log\frac{p(x)}{q(x)} && \text{(A.15)}\\
&= \mathbb{E}_p\{\log\frac{p(x)}{q(x)}\} &&
\end{aligned}$$

A.2. Min-Entropy and Guessing Entropy

Min-entropy and guessing entropy are often used in cryptography for security assessment. Min-entropy characterizes the most probable occurrence of a random variable:

$$H_\infty(X) = -\log\big(\max_{x\in\mathcal{X}}\{p(x)\}\big) \tag{A.16}$$

Obviously, $H_\infty(X)$ is *always* smaller or equal to $H(X)$. The equality is valid, only if X is perfectly uniformly and independently distributed.

The average min-entropy is defined as the average min-entropy of X given Y:

$$\tilde{H}_\infty(X|Y) = -\log\Big(\sum_{y\in\mathcal{Y}} p(y)\cdot max_x\{p(x|y)\}\Big) \tag{A.17}$$

Min-entropy and average min-entropy represent security performance in the *worst case* scenario. They are indispensable metrics for rigorous security assessment.

The guessing entropy is eligible to measure the average number of guesses required to find a random variable successfully. Assuming that X is chosen from $\{x_1, x_2, \cdots, x_{|X|}\}$ with the probability $p(x_1), p(x_2), \cdots, p(x_{|X|})$, where $|X|$ is the number of possible X and $p(x_1) \geq p(x_2) \geq \cdots \geq p(x_{|X|})$. The best guessing strategy of an adversary is to start with the most probable occurrence. The *guessing entropy* $G(X)$ is defined as:

$$G(X) = \sum_{i=1}^{|X|} i\cdot p(x_i) \tag{A.18}$$

Here i indexes the number of the attempts and the probability that the i-th attempt is successful is equal to $p(x_i)$ according to this guessing strategy. If an adversary can try maximum K attempts, his successful rate is $\sum_1^K p(x_i)$. Guessing entropy is related with entropy, which shows minimum average coding length for a random variable. In [Mas94], Massey gave a lower bound of guessing entropy regarding to entropy:

$$G(X) \geq 2^{H(X)-2} + 1 \tag{A.19}$$

for any variable X with $H(X) \geq 2$. Similarly the conditional guessing entropy $G(X|Y)$ is defined as the average number of attempts required to estimate X given Y:

$$G(X|Y) = \sum_{y \in Y} p(Y) \sum_{i=1}^{|X|} i \cdot p(x_i|Y) \tag{A.20}$$

A.3. Binomial distribution

The binomial distribution is widely used to model distributions of binary variables. Binomial distribution can be seen as discrete Poisson distribution. It describes the statistics of a Bernoulli sequence, which can be defined as [Bur99]:

- Each trial results in one of only two possible outcomes.
- The trials are *statistically identical* so that the probability p of an event's occurrence is *constant* for each trial.
- The trials are *statistically independent*.

Under these conditions, the probability of obtaining k occurrences in n Bernoulli trials is given by:

$$b(k, p, n) = \begin{pmatrix} n \\ k \end{pmatrix} p^k (1-p)^{n-k} \tag{A.21}$$

The expected value and variance of a Binomial variable are given by:

$$\mathbb{E}\{k\} = n \cdot p \tag{A.22}$$

$$var\{k\} = n \cdot (1-p) \cdot (p) \tag{A.23}$$

where $\mathbb{E}\{\cdot\}$ and $var\{\cdot\}$ denote expected value and variance. When the sample size n is large enough, the Binomial distribution approximates to Gaussian distribution. Additionally, the entropy of the corresponding independently identically distributed sequence is equal to $n \cdot h(p)$, where $h(p)$ is the binary entropy function.

If X and Y are two uniformly independently distributed binary vectors with the length n and $E = X + Y$ is the bit error vector comparing X and Y, then E is also uniformly independently distributed. The Hamming distance of E is binomially distributed with parameter n and $p = 0.5$. The bit error rate $BER = ||E||/n$ has the following properties:

$$\mathbb{E}\{BER\} = \frac{n \cdot p}{n} = 0.5 \tag{A.24}$$

$$var\{BER\} = \frac{n \cdot p \cdot (1-p)}{n^2} = \frac{0.25}{n} \tag{A.25}$$

All X, Y and E contain n bits entropy.

A.4. Markov Chain

The Markov chain is appropriate to describe dependency of random variables. Let $\{X_i\}$ be a sequence generated from a stochastic source with $x_i \in \mathcal{X}$. A stochastic process is called *stationary*, if the joint distribution of any subset is invariant to shifting:

$$Pr\{X_1 = x_1, X_2 = x_2, \cdots, X_n = x_n\} = Pr\{X_{1+l} = x_1, X_{2+l} = x_2, \cdots, X_{n+l} = x_n\} \quad \forall\, n,\, l \tag{A.26}$$

A discrete stochastic processing $X_1, X_2, \cdots$ has *Markov* properties, if for all $n \in \mathcal{N}$ and all $x_1, x_2, \cdots, x_n \in \mathcal{X}$:

$$Pr\{X_n = x_n | X_{n-1} = x_{n-1}, X_{n-2} = x_{n-2}, \cdots, X_1 = x_1\} = Pr\{X_n = x_n | X_{n-1} = x_{n-1}\} \tag{A.27}$$

The variable X_n is only dependent on its previous variable X_{n-1} not on other previous states. The joint probability $p(x_1, x_2, \cdots, x_n)$ of Markov chain can be written as:

$$p(x_1, x_2, \cdots, x_n) = p(x_1) \prod_{i=2}^{n} p(x_i | x_{i-1}) \tag{A.28}$$

The information rate of a stochastic process X_i is defined as [CT91]:

$$H(\mathcal{X}) = \lim_{n \to \infty} \frac{1}{n} H(X_1, X_2, \cdots, X_n) \tag{A.29}$$

if the limit exists. The information rate of Markov chain is:

$$H(\mathcal{X}) = - \sum_{i,j \in [1,\cdots,n]} p(X_m = \mathrm{x_j}) p(X_{m+1} = \mathrm{x_i} | X_m = \mathrm{x_j}) \log p(X_{m+1} = \mathrm{x_i} | X_m = \mathrm{x_j}) \tag{A.30}$$

where $\mathcal{X} = \{\mathrm{x_i} | i \in [1, \cdots, n]\}$.

B. Error Correction Code

B.1. Linear Block Code

Coding theory is the fundamental of modern digital techniques. It enables reliable data transmission and efficient data storage. Linear block code is an important code class. For instance, a message block S of k symbols can be extended into a codeword C of n symbols with a linear coding method and the codeword can correct t errors. We denote this code as a (n,k,t) block code. If d is the minimum Hamming distance of the codewords, $d \geq 2t+1$.

A $k \times n$ generation matrix G can be used to produce a codeword with $C = S \cdot G$. Every row of G is a valid code. If C is corrupted with an error E and the Hamming weight of E is not larger than t, the errors can be corrected with the parity check matrix H. H is an $r \times n$ matrix, where $r \leq n-k$. It is orthogonal to G and codeword space, namely $G \cdot H^T = 0$. The syndrome of a code V is defined as $syn(V) = v \cdot H^T$. The codes with the same syndrome share the unique error pattern E, whose Hamming weight is smaller than $d/2$.

The Hamming (sphere-packing) bound of a (n,k,t) block code over a q symbol space exists:

$$q^k \leq \frac{q^n}{\sum_{i=1}^{t} \binom{n}{i} (q-1)^i} \tag{B.1}$$

Instead of coding in a vector space, the polynomial coding in Galois field is an efficient alternative. A Galois field $GF(q)$ contains q symbols, where $q = p^m$, p is a prime number and $m \in \mathcal{N}$ is a natural number. A (n,k) linear block code is a block code with length n and consists of q^k codewords, "if and only if these codewords from a k- dimensional subspace of all the n- tuples vector space over the field $GF(q)$" (definition 3.1 in [LC83]). Obviously these q^k codewords form also a vector space in $GF(q)$. A (n,k) codeword $C = [c_0, c_1, c_2, \cdots, c_{n-1}]$ with $C \in GF(q^n)$ can be described as a polynomial $c(X)$ of degree $n-1$ in $GF(q)$. A (n,k) cyclic code can be generated by a multiplication of a generator polynomial $g(X)$ with degree of $n-k$ and an arbitrary polynomial $u(X)$ with degree not larger than $k-1$.

$$\begin{aligned} c(X) &= c_0 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1} \\ &= u(X) \cdot g(X) \\ &= (u_0 + u_1X + \cdots + u_{k-1}X^{k-1})(1 + g_1X + \cdots + g_{n-k}X^{n-k}) \end{aligned}$$

where $X \in GF(q)$.

In the following we show some important polynomials over $GF(2)$ with special properties (the detailed description can be found in section 2.3 and 2.5 in [LC83]):

- *Irreducible polynomial*: A polynomial $f(X)$ over $GF(2)$ of degree m is irreducible, if it can not be divided by any polynomial over $GF(2)$ with degree smaller than m and greater than 0
- *Primitive polynomial*: An irreducible polynomial $f(X)$ of degree m is called primitive, if it is divisible by a $X^n + 1$ and the smallest n is equal to $2^m - 1$. The number of irreducible polynomials of degree m can be more than one.

- *Minimal polynomial*: The minimal polynomial $\phi(X)$ of β is the polynomial with the smallest degree of $GF(q)$, that $\phi(\beta) = 0$ and $\beta \in GF(2^m)$.

It can be proven that the minimal polynomial $\phi(X)$ of β is unique and irreducible. Any $f(X)$ over $GF(2)$ is divisible by $\phi(X)$, if β is a root of $f(X)$.

B.2. BCH and RS Codes

The Bose, Chaudhuri and Hocquenghem (BCH) codes are the generalised Hamming codes. It is not only qualified for binary codes, but also non-binary codes. Reed-Solomon codes are one of the most important subclasses of non-binary BCH codes. In the following we introduce the properties of BCH and RS codes.

For any positive integer m, t with $m \geq 3$, a binary BCH code exists:

$$\begin{array}{rl} \text{Codeword length} & n = 2^m - 1 \\ \text{Number of correctable bit errors} & t < 2^{m-1} \\ \text{Number of parity bits} & n - k \leq mt \\ \text{Minimum Hamming distance} & d_{min} \geq 2t + 1 \end{array}$$

A BCH code is a polynomial code (also a cyclic code). Let $\phi_i(X)$ be the minimal polynomial of α^i for $i \in \{0, 1, \cdots, 2^n - 1\}$. Then the generator polynomial $g(X)$ of the BCH-code is:

$$g(X) = LCM\{\phi_1(X), \phi_3(X), \phi_5(X) \cdots, \phi_{2t-1}(X)\} \tag{B.2}$$

where LCM is the least common multiple. In other words $g(X)$ is the lowest-degree of polynomial, which has roots of $\alpha, \alpha^2, \cdots, \alpha^{2t}$. [1]

The above described binary BCH code can be extended into non-binary Galois field $GF(q)$ (i.e., $q = 2^m$). A q-array (n, k) BCH code can also be generated with a generation polynomial $g(X)$ of degree $n - k$ over $GF(q)$. And such a BCH code exists for t correctable symbol errors and $n = q^s - 1$, where s and t is positive integers. The Reed-Solomon (RS) Code is an important subclass of non-binary BCH code in $GF(q)$ with $s = 1$. The *RS* code has the following parameters:

$$\begin{array}{rl} \text{Codeword length} & n = q - 1 \\ \text{Number of parity digits} & n - k = 2t \\ \text{Minimum distance} & d_{min} = 2t + 1 \end{array}$$

Please note that a RS code is a sequence in $\{GF(q)\}^n$.

Theorem 1. *A (n, k_1) BCH code is also a (n, k_2) BCH code, if $k_1 < k_2$.*

Proof. Let $c_1(X)$ be a (n, k_1) BCH code. $g_1(X)$ and $g_2(X)$ are the generator polynomials for the BCH codes of (n, k_1) and (n, k_2). If t_1 and t_2 are the corresponding number of correctable errors. And $t_1 > t_2$, since $k_1 < k_2$.

$$\begin{aligned} g_2(X) &= LCM\{(X - \alpha)(X - \alpha^3) \cdots (X - \alpha^{2t_2 - 1})\} \\ g_1(X) &= LCM\{((X - \alpha)(X - \alpha^3) \cdots (X - \alpha^{2t_2 - 1}) \cdot (X - \alpha^{2t_2 + 1}) \cdots (X - \alpha^{2t_1 - 1})\} \end{aligned}$$

[1] $LCM\{\phi_1(X), \phi_3(X), \phi_5(X) \cdots, \phi_{2t-1}(X)\} = LCM\{\phi_1(X), \phi_2(X), \phi_3(X), \cdots, \phi_{2t}(X)\}$, since the odd power sequence and even power sequence have the same minimal polynomial (section 6.1 in [LC83]).

Therefore $g_1(X)$ is divisible by $g_2(X)$ and a quotient $v(X)$ exists so that $g_1(X) = g_2(X) \cdot v(X)$. Then

$$\begin{aligned} c_1(X) &= g_1(X) \cdot u_1(X) \\ &= g_2(X) \cdot v(X) \cdot u_1(X) \end{aligned}$$

where $u_1(X)$ is a polynomial over $GF(q)$ with the degree not greater than $k_1 - 1$ and is the corresponding message of $c_1(X)$. Therefore $c_1(X)$ is also a (n, k_2) BCH codeword and its message code is $v(X) \cdot u_1(X)$. □

The BCH code and RS code are the widely used error correction codes. They are also kinds of cyclic codes that shifting the symbol in a code words results also a codeword. They can correct a certain amount of errors and the occurring error at each position is supposed to be equally probable.

B.3. Hadamard Code

The Hadamard code is the first order Reed-Muller code. Hadamard codes can be derived from a Hadamard matrix. A Hadamard matrix is a $2^k \times 2^k$ squared matrix consisting of 1 and -1, where k is a positive integer.

$$Hd_1 = [1], \quad Hd_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad Hd_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

The Hadamard matrix can be generated recursively with increasing k:

$$Hd_{2^k} = \begin{bmatrix} Hd_{2^{k-1}} & Hd_{2^{k-1}} \\ Hd_{2^{k-1}} & -Hd_{2^{k-1}} \end{bmatrix} = Hd_2 \otimes Hd_{2^{k-1}} \tag{B.3}$$

where $\otimes$ is the Kronecker product, also called tensor product or the direct product [Mal]. Any two different rows in Hd are orthogonal [Mal] (with normal arithmetic operation not arithmetic operation in e.g. Galois Field).

Given the codeword length $n = 2^k$, the Hadamard code book can be derived with Hadamard matrix by replacing -1 with 0:

$$C^n_{Hd} = \begin{bmatrix} Hd^*_n \\ -Hd^*_n \end{bmatrix} \tag{B.4}$$

The length of message code is $k+1$. The minimum Hamming distance of the codewords is 2^{k-1}. The maximum number of correctable bit error is $2^{k-2} - 1$. The codeword length increases exponentially with k, while the secret length increases linearly with k. The code rate is relatively poor, however, it can correct $(2^{n-2} - 1)/2^n \approx 25\%$ bit errors.

Assuming that a sequence C' is observed in the decoding process. The zero components in C' are replaced with -1 and the resulting code $\tilde{C}$ multiplied with the Hadamard matrix. If the number of bit errors is not larger than $2^{n-2} - 1$, a unique maximum absolute value of the multiplication exists. The corresponding row in the code book with the maximum value is the decoding output, if the value is positive; the inverse of the corresponding row is taken, if the value is negative.

Notations

$\{0,1\}^m$	m-dimensional binary feature space
$\|\|\cdot\|\|$	Hamming weight
$D(p(X)\|\|q(X))$	Kullback-Leibler distance of distributions $p(X)$ and $q(X)$
$E\{\cdot\}$	Expected value
$G(X)$	Guessing entropy of a random variable X
$G(X\|Y)$	Conditional guessing entropy of random variable X given Y
GF	Galois Field
$h(p)$	Binary entropy function, $h(p) = -p\log(p) - (1-p)\log(1-p)$
$H(X)$	Entropy of a random variable X
$H_\infty(X)$	Min-entropy of a random variable X
$H(X\|Y)$	Conditional entropy of a random variable X given Y
$\tilde{H}_\infty(X\|Y)$	Average min-entropy of a random variable X given Y
$I(X,Y)$	Mutual information of random variables X and Y
$\mathcal{N}$	Natural number
$\oplus$	XOR operator
p	Probability density function

Abbreviations

AD	Auxiliary Data
BSC	Binary symmetric channel
BER	Bit error rate
BCH code	Bose, Chaudhuri and Hocquenghem code
EER	Equal Error Rate
FAR	False Accept Rate
FNMR	False Non-Match Rate
FMR	False Match Rate
FRGC	Face Recognition Grand Challenge
FRR	False Reject Rate
FTA	Failure to Acquire
FTE	Failure to Enrol
ICAO	International Civil Aviation Organization
IDA	Independent Component Analysis
i.i.d	identically independently distributed
LDA	Linear Discriminate Analysis
NIR	Near InfraRed
PCA	Principle Component Analysis
PIE	Pseudonymous Identifier Encoder
PIR	Pseudonymous Identifier Recorder
PIC	Pseudonymous Identifier Comparator
PI	Pseudonymous Identifier
ROC	Receiver Operation Characteristics
RS code	Reed-Solomon code
SD	Statistical Distance

Bibliography

[AC93] AHLSWEDE R., CSISZÁR I.: Common randomness in information theory and cryptography part ii: Cr capacity. *IEEE Trans. Inform. Theory 39* (1993), 1121–1132. 16

[Adl03] ADLER A.: Sample images can be independently restored from face recognition templates. In *Proceedings of Canadian Conference on Electrical and Computer Engineering* (Montreal, Canada, 2003), pp. 1163–1166. 6

[Adl04] ADLER A.: Reconstruction of source images from quantized biometric match score data. In *In Biometrics Conference, Washington, DC* (September 2004). 18, 43, 98

[Adl05] ADLER A.: Vulnerabilities in biometric encryption systems. In *Audio- and Video-based Biometric Person Auth.* (Tarrytown, NY, USA, 2005). 18

[AJB97] ACHERMANN B., JIANG X., BUNKE H.: Face recognition using range data. In *Proc. International Conference on Virtual Systems and Multimedia* (Geneva, Switzerland, 1997), IEEE Press, pp. 129– 136. 37

[AL09] AO M., LI S. Z.: Near infrared face based biometric key binding. In *ICB'09: Proceedings of the Third International Conference on Advances in Biometrics* (Berlin, Heidelberg, 2009), Springer-Verlag, pp. 376–385. 9, 96, 100

[ART03] *Working document on biometrics*. Tech. rep., ARTICLE 29 Data Protection Working Party, 2003. 6

[Bal08] BALLARD L. K.: *Robust Techniques for Evaluating Biometric Cryptographic Key Generators*. PhD thesis, The Johns Hopkins University, Baltimore, Maryland, March 2008. 18, 22

[BCC*07] BRINGER J., CHABANNE H., COHEN G., KINDARJ B., ZÉMOR G.: Optimal iris fuzzy sketches. In *First IEEE International Conference on Biometrics: Theory, Applications, and Systems BTAS 2007* (May 2007), vol. 705. 26, 66

[BDH*08] BUHAN I., DOUMEN J., HARTEL P., TANG Q., VELDHUIS R.: Embedding renewable cryptographic keys into continuous noisy data. In *Information and communications security, 10th international conference ICICS* (UK, 2008), pp. 294–310. 10

[Bro06] BROMBA M.: On the reconstruction of biometric raw data from template data. *Bromba Biometrics* (2006). 6

[Bur99] BURY K.: *Statistical Distributions in Engineering*. Cambridge University Press, 1999. 108

[BV99] BLANZ V., VETTER T.: A morphable model for the synthesis of 3d faces. *Proc. of the SIGGRAPH'99 Los Angeles, USA* (1999), 187–194. 37

[BYS05] BAI X.-M., YIN B.-C., SUN Y.-F.: Face recognition using extended fisherface with 3d morphable model. In *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics* (2005), pp. 4481–4486. 37

[CAS] CASIA iris image database. collected by the Chinese Academy of Sciences' Institute of Automation (CASIA), http://biometrics.idealtest.org/. 64, 65

[CCCe04] CHAOS COMPUTER CLUB E.V.: How to fake fingerprints? 6

[CKYZ05] CHEUNG K. H., KONG A. W.-K., YOU J., ZHANG D.: An analysis on invertibility of cancelable biometrics based on biohashing. In *CISST'2005* (2005), pp. 40–45. 98, 99

[CL68] CHOW C., LIU C.: Approximating discrete probability distributions with dependence trees. In *IEEE Transactions on Information Theory, IT-14* (1968), pp. 462–467. 51

[CS07] CAVOUKIAN A., STOIANOV A.: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*. Tech. rep., Information and Privacy Commissioner/Ontario, March 2007. 7, 13

[CS08] CARTER F., STOIANOV A.: Implications of biometric encryption on wide spread use of biometrics. In *EBF Biometric Encryption Seminar* (June, 2008). 29

[CT91] COVER T. M., THOMAS J. A.: *Elements of information theory*. Wiley-Interscience, New York, NY, USA, 1991. 109

[CTGN05] CONNIE T., TEOH A., GOH M., NGO D.: Palmhashing: a novel approach for cancelable biometrics. In *Information Processing Letters* (2005), vol. 93, pp. 1–5. 9, 96, 98

[Dau03] DAUGMAN J.: The importance of being random: Statistical principles of iris recognition. In *Pattern Rec. 36* (2003), pp. 279–291. 62, 70, 73, 77

[Dau04] DAUGMAN J.: How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on 14*, 1 (2004), 21 – 30. 62

[DC01] DAUGMAN J., C C. D.: Epigenetic randomness, complexity, and singularity of human iris patterns. In *Proceedings of the Royal Society, B, 268, Biological Sciences* (2001), pp. 1737 – 1740. 66

[Dir95] Directive 95/46/ec of the european parliament and of the council. *Offical Journal of the European Communities*, L 281 (1995). 6

[DM04] DAUGMAN J., MALHAS I.: Iris recognition border-crossing system in the uae. *International Airport Review, Issue 2* (2004). 62

[DORS08] DODIS Y., OSTROVSKY R., REYZIN L., SMITH A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing 38* (2008). 10, 16, 22, 43

[DRS04] DODIS Y., REYZIN L., SMITH A.: Fuzzy extractors: How to generate strong secret keys from biometrics and other noisy data. In *In Advances in cryptology - Eurocrypt'04* (2004), 3027 L., (Ed.), pp. 523–540. 10

[DSB07] *Report of the Defense Science Board Task Force on Defense Biometrics*. Tech. Rep. 20301-3140, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Washington, D.C., March 2007. 7

[EFG*09] ERKIN Z., FRANZ M., GUAJARDO J., KATZENBEISSER S., LAGENDIJK I., TOFT T.: Privacy-preserving face recognition. In *Privacy Enhancing Technologies, 9th International Symposium, PETS 2009* (2009), vol. 5672 of *Lecture Notes in Computer Science*, Springer, pp. 235–253. 7

[HAD05] HAO F., ANDERSON R., DAUGMAN J.: *Combining cryptography with biometrics effectively*. Tech. Rep. 640, Univesity of Cambridge, Computer Laboratory, July 2005. 66, 67, 70, 77, 80

[HHB03] HUANG J., HEISELE B., BLANZ V.: Component-based face recognition with 3d morphable models. *Proc. of the 4th International Conference on Audio- and Video-Based Biometric Person Authentication AVBPA 2003* (2003), Guildford, UK, 27–34. 37

[Hil01] HILL C. J.: *Risk of Masquerade Arising from the Storage of Biometrics*. Master's thesis, The Department of Computer Science, Australian National University, November 2001. 6, 18

[HLLS01] HETZEL G., LEIBE B., LEVI P., SCHIELE B.: 3d object recognition from range images using local feature histograms. In *IEEE International Conference on Computer Vision and Pattern Recognition (CVPR'01)* (2001), vol. 2, pp. 394–399. 38

[HO] HOME OFFICE U. A.: The nationality, immigration and asylum act 2002, physical data: voluntary provision, iris recognition immigration system (iris) scheme definition document. *Nationality, Immigration and Asylum Act 2002*. 62

[HPA04] HESELTINE T., PEARS N., AUSTIN J.: Three-dimensional face recognition: An eigensurface approach. In *Proc. IEEE International Conference on Image Processing* (Singapore, 2004), pp. 1421–1424. 37

[Ign09] IGNATENKO T.: *Secret-Key Rates and Privacy Leakage in Biometric Systems*. PhD thesis, Eindhoven University of Technology, 2009. 16, 20, 28, 55, 88, 94

[ISO11] ISO/IEC 24745 Information technology - Security techniques - Biometric template protection. ISO/IEC JTC 1/SC 27, June 2011. 11, 13, 19, 42

[JLG04] JIN A. T. B., LING D. N. C., GOH A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition Issue 11 37* (November 2004), 2245–2255. 9, 96, 98

[JNN08] JAIN A. K., NANDAKUMAR K., NAGAR A.: Biometric template security. In *EURASIP Journal on Advances in Signal Processing, , Special Issue on Biometrics* (January 2008). 7, 13

[JS02] JUELS A., SUDAN M.: A fuzzy vault scheme. In *IEEE International Symposium on Information Theory* (2002). 10, 32, 33

[JTK07] JIN A. T. B., TOH K.-A., KUAN Y. W.: 2^n discretisation of biophasor in cancellable biometrics. In *ICB* (2007), pp. 435–444. 9

[JW99] JUELS A., WATTENBERG M.: A fuzzy commitment scheme. In *6th ACM Conference on Computer and Communications Security* (1999), pp. 28–36. 10, 27, 28, 42

[KCZ*06] KONG A., CHEUNG K.-H., ZHANG D., KAMEL M., YOU J.: An analysis of biohashing and its variants. *Pattern Recognition 39*, 7 (2006), 1359 – 1368. 9, 98

[Kel10] KELKBOOM E. J. C.: *On the Performance of Helper Data Template Protection Schemes*. PhD thesis, University of Twente, 2010. 29, 30, 31

[Ken64] KENNEY J. F.: *Mathematics of statistics*, 3 ed. Van Nostrand, 1964. 49

[KKM*10] KEVENAAR T., KORTE U., MERKLE J., NIESING M., IHMOR H., CHRISTOPH B., ZHOU X.: A reference framework for the privacy assessment of keyless biometric template protection systems. In *BIOSIG 2010: Biometrics and Electronic Signatures* (2010). 13

[Kov] KOVESI P.: What are log-Gabor filters and why are they good? 63

[KY08] KHOLMATOV A., YANIKOGLU B.: Realization of correlation attack against fuzzy vault scheme. In *Proceedings of SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents X* (2008), vol. 6819. 95

[LC83] LIN S., COSTELLO D. J.: *Error Control Coding: Fundamentals and Applications*. Pearson Education, 1983. 110, 111

[LPV03] LU J., PLATANIOTIS K., VENETSANOPOULOS A.: Face recognition using lda-based algorithms. In *IEEE Trans. on Neural Networks* (January 2003), vol. Vol. 14, pp. 195–200. 36

[LT03] LINNARTZ J. P., TUYLS P.: New shielding functions to enhance privacy and prevent misuse of biometric templates. In *4th international conference on audio- and video-based biometric person authentication* (2003). 16

[LVB*93] LADES M., VORBRUGGEN J., BUHMANN J., LANGE J., VON DER MALSBURG C., WURTZ R., KONEN W.: Distortion invariant object recognition in the dynamic link architecture. In *IEEE Trans. Computers, 42* (1993), pp. 300–311. 36

[LWC99] LIU C., WECHSLER H., COMPARATIVE: Assessment of independent component analysis (ICA) for face recognition. In *Proc. of the Second International Conference on Audio- and Video-based Biometric Person Authentication AVBPA'99* (Washington D.C., USA, March 1999), pp. 211–216. 36

[Mal] MALEK M.: *Hadamard Codes*. California State University. 112

[Mas94] MASSEY J. L.: Guessing and entropy. In *Proceedings of the 1994 IEEE International Symposium on Information Theory* (1994), p. 204. 108

[Mas03] MASEK L.: Recognition of human iris patterns for biometric identification, 2003. 63

[Mau99] MAURER U.: Information-theoretic cryptography. In *Advances in Cryptology — CRYPTO '99* (Aug. 1999), Wiener M., (Ed.), vol. 1666 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 47–64. 23

[MMYH02] MATSUMOTO T., MATSUMOTO H., YAMADA K., HOSHINO S.: Impact of artificial "gummy" fingers on fingerprint systems. In *Optical Security and Counterfeit Deterrence Techniques IV* (2002), vol. SPIE Vol. 4677, pp. 275–289. 6

[MP01] MOON H., PHILLIPS P.: Computational and performance aspects of pca-based face recognition algorithms. In *Perception* (2001), vol. Vol. 30, pp. 303–321. 36

[MV99] MEYBERG K., VACHENAUER P.: *Hoehere Mathematik 1*. Springer, 1999. 98

[NJ09] NAGAR A., JAIN A. K.: On the security of non-invertible fingerprint template transforms. In *IEEE Workshop on Information Forensics and Security (WIFS)* (2009). 21, 22, 97, 99

[NJP07] NANDAKUMAR K., JAIN A. K., PANKANTI S.: Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security 2*, 4 (2007), 744–757. 10, 33, 34, 92, 93, 95

[NNJ07] NANDAKUMAR K., NAGAR A., JAIN A. K.: Hardening fingerprint fuzzy vault using password. In *International conference on biometrics 2007* (2007). 34

[NNJ10] NAGAR A., NANDAKUMAR K., JAIN A. K.: Biometric template transformation: a security analysis. In *SPIE Media Forensics and Security Media Forensics and Security II* (2010). 99, 100

[NST06] NSTC SUBCOMMITTEE ON BIOMETRICS AND IDENTITY: *Iris Recognition*, 2006. 62

[Pat96] Fingerprint controlled public key cryptographic system. US patent, U.S. 5,541,994, 1996. 8

[Pat97] Biometric controlled key generation. US patent, U.S. 5,680,460,, 1997. 8

[Pat01] Method for secure generation using a biometric. US patent, US 6,219,794,, 2001. 8

[PFS*05] PHILLIPS P. J., FLYNN P. J., SCRUGGS T., BOWYER K. W., CHANG J., HOFFMAN K., MARQUES J., MIN J., WOREK W.: Overview of the face recognition grand challenge. In *IEEE CVPR* (http://face.nist.gov/frgc/, June 2005), vol. 2, pp. 454–461. 39, 44

[Pri] Fast border passage with the iris scan. Schiphol, Amsterdam Airport. 62

[PSO*07] PHILLIPS P. J., SCRUGGS W. T., O'TOOLE A. J., FLYNN P. J., BOWYER K. W., SCHOTT C. L., SHARPE M.: *FRVT 2006 and ICE 2006 Large-Scale Results*. Tech. rep., National

Institute of Standards and Technology and SAIC and School of Behavioral and Brain Sciences and Computer Science & Engineering Depart., U. of Notre Dame, Notre Dame and Schafer Corp., March 2007. 36

[PW03] PAN G., WU Z.: Automatic 3d face verification from range data. In *ICASSP* (2003), pp. 193–196. 37

[PWWL03] PAN G., WU Y., WU Z., LIU W.: 3D face recognition by profile and surface matching. In *Proc. International Joint Conference on Neural Networks* (Portland, Oregon, 2003), pp. 2168–2174. 37

[RCB01] RATHA N., CONNELL J., BOLLE R.: Enhancing security and privacy in biometrics-based authentication system. *IBM Systems Journal 40*, 3 (2001), 614–634. 9, 96

[RCCB07] RATHA N. K., CHIKKERUR S., CONNELL J. H., BOLLE R. M.: Generating cancelable fingerprint templates. In *IEEE Transactions on Pattern Analysis and Machine Intelligence* (April 2007), vol. 29. 9, 96, 99

[RSGK99] ROBERGE C. S. D., STOIANOV A., GILROY R., KUMAR B. V.: Biometric encryption. *ICSA Guide to Cryptography, Chapter 2* (1999). 8

[RSN*08] RUKHIN A., SOTO J., NECHVATAL J., BARKER E., LEIGH S., LEVENSON M., BANKS D., HECKERT A., DRAY J., VO S., RUKHIN A., SOTO J., SMID M., LEIGH S., VANGEL M., HECKERT A., DRAY J., BASSHAM III L. E.: *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Tech. rep., National Institute of Standards and Technology, 2008. 29

[SB07] SCHEIRER W. J., BOULT T. E.: Cracking fuzzy vaults and biometric encryption. In *Proceedings of the Biometrics Symposium* (Baltimore, Md, USA, 2007). 17, 34, 95

[Sei06] SEIDEL J.: Zusatzinformationen in fingerbildern. 6

[Sha79] SHAMIR A.: How to share a secret. In *Communications of the ACM 22*. 1979, pp. 612–613. 93

[SKK04] SAVVIDES M., KUMAR B. V., KHOSLA P.: Cancelable biometric filters for face recognition. In *Proceedings of the 17th International Conference on Pattern Recognition ICPR 2004* (2004), vol. 3, pp. 922 – 925. 8, 96, 99

[Smi04] SMITH A. D.: *Maintaining Secrecy when Information Leakage is Unavoidable*. PhD thesis, Massachusetts Institute of Technology, August 2004. 20, 28

[Sou02] SOUTAR C.: Biometric system security. In *Information Technology Security Symposium* (2002). 43

[ST09] SUN Z., TAN T.: Ordinal measures for iris recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2009). 63

[STP09] SIMOENS K., TUYLS P., PRENEEL B.: Privacy weaknesses in biometric sketches. In *the 2009 IEEE Symposium on Security and Privacy, IEEE Computer Society* (2009), pp. 188–203. 17, 22, 29, 30, 60, 81, 88

[STW04] SUN Z., TAN T., WANG Y.: Robust encoding of local ordinal measures: A general framework of iris recognition. In *Proc. BioAW Workshop* (2004), pp. 270–282. 63, 77

[tag06] Iris recognition takes steps into a brave new world. *Biometric Technology Today 14*, 2 (2006), 1–2. 62

[Tak07] TAKARAGI D. K.: Security techniques for next generation applications - cancelable bio and post-quantum. presentation on ZISC Information Security Colloquium HS 2007, 2007. Hitachi, Ltd. 8, 9

[TG04] TUYLS P., GOSELING J.: Capacity and examples of template protecting biometric authentication systems. In *Biometric authentication workshop (BioAW 2004)* (Prague, 2004), LNCS, (Ed.), no. 3087, pp. 158–170. 10, 16, 22

[TJC*06] TEOH A., JIN B., CONNIE T., NGO D., LING C.: Remarks on biohash and its mathematical foundation. *Information Processing Letters 100*, 4 (2006), 145 – 150. 96, 99

[TP91] TURK M., PENTLAND A.: Eigenfaces for recognition. In *Journal of Cognitive Neurosicence* (1991), vol. Vol. 3, pp. pp. 71–86. 36

[TTMM00] TOPI M., TIMO O., MATTI P., MARICOR S.: Robust texture classification by subsets of local binary patterns. In *Proceedings of the International Conference on Pattern Recognition - Volume 3* (Washington, DC, USA, 2000), IEEE Computer Society. 77

[Tuy04] TUYLS P.: Privacy protection of biometric templates: cryptography on noisy data. In *Revue HF (Rev. HF) ISSN 0035-3248* (2004), no3, pp. 55–64. 28, 42

[TVI*04] TUYLS P., VERBITSKIY E., IGNATENKO T., SCHOBBEN D., AKKERMANS T. H.: Privacy protected biometric templates: ear identification. In *Proceeding of SPIE* (2004), vol. 5404, pp. 176–182. 10

[TwGdCN06] TEOH A. B., WYN GOH A., D C.L. NGO D.: Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. Pattern Anal. Mach. Intell. 28*, 12 (2006), 1892–1901. 9

[VDRY09] VETRO A., DRAPER S., RANE S., YEDIDIA J.: *Securing Biometric Data*. Elsevier, 2009. 26, 66

[vdVKS*06] VAN DER VEEN M., KEVENAAR T., SCHRIJEN G.-J., AKKERMANS T. H., ZUO F.: Face biometrics with renewable templates. In *Security, Steganography, and Watermarking of Multimedia Contents VIII* (San Jose, California, USA, January 2006). 10, 44

[VTDL03] VERBITSKIY E., TUYLS P., DENTENEER D., LINNARTZ J. P.: Reliable biometric authentication with privacy protection. *24th Benelux Symp. on Info. Theory* (2003). 10

[Wol98] WOLF S.: Unconditional security in cryptography. *Lectures on Data Security* (1998), 217–250. 23

[WST95] WILLEMS F. M. J., SHTARKOV Y. M., TJALKENS T. J.: The context tree weighting method: Basic properties. *IEEE Transactions on Information Theory 41* (1995), 653–664. 77

[ZRC08] ZUO J., RATHA N., CONNELL J.: Cancelable iris biometric. In *19th International Conference on Pattern Recognition, 2008. ICPR 2008.* (2008), pp. 1–4. 10

[ZSBF08] ZHOU X., SEIBERT H., BUSCH C., FUNK W.: A 3d face recognition algorithm using histogram-based features. In *Eurographics Workshop on 3D Object Retrieval* (Crete, Greece, 2008), pp. 65–71. 37

Publications and Talks

Publications

Book Chapter:

- Zhou, Xuebing; Kuijper, Arjan; Busch, Christoph: Template Protection for 3D Face Recognition In: Oravec, Milos (Ed.): Face Recognition. Sciyo; 2010, pp. 315-328

Paper (first author):

1. Zhou, Xuebing; Kuijper, Arjan; Busch, Christoph: Cracking Iris Fuzzy Commitment In: IEEE the International Conference on Biometrics (ICB 12), 2012
2. Zhou, Xuebing; Kuijper, Arjan; Veldhuis, Raymond; Busch, Christoph: Quantifying Privacy and Security of Biometric Fuzzy Commitment In: IEEE the International Joint Conference on Biometrics (IJCB 11), 2011
3. Zhou, Xuebing; Opel, Alexander; Korte, Ulrike; Merkle Johannes; Busch, Christoph: Enhanced Template Protection with Passwords for Fingerprint Recognition In: IEEE the 3rd International Workshop on Security and Communication Networks, 2011
4. Zhou, Xuebing; Araujo Sanchez, Silvia; Kuijper, Arjan: 3D Face Recognition with Local Binary Patterns In: Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Proceedings: IIH-MSP 2010, 2010, pp. 329-332
5. Zhou, Xuebing; Kalker, Ton: On the Security of Biohashing In: Media Forensics and Security, SPIE Press, 2010, pp. 75410Q-1 - 75410Q-8. (Proceedings of SPIE 7541)
6. Zhou, Xuebing; Wolthusen, Stephen; Busch, Christoph; Kuijper, Arjan: Feature Correlation Attack on Biometric Privacy Protection Schemes In: Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Proceedings IIH-MSP 2009. 2009, pp. 1061-1065
7. Zhou, Xuebing; Wolthusen, Stephen; Busch, Christoph; Kuijper, Arjan: A Security Analysis of Biometric Template Protection Schemes In: Image Analysis and Recognition: 6th International Conference, ICIAR 2009
8. Zhou, Xuebing; Seibert, Helmut; Busch, Christoph; Funk, Wolfgang: A 3D Face Recognition Algorithm Using Histogram-based Features In: European Association for Computer Graphics (Eurographics): EG 3DOR 2008: Eurographics 2008 Workshop on 3D Object Retrieval
9. Zhou, Xuebing; Busch, Christoph: A Novel Privacy Enhancing Algorithm for Biometric System In: Gesellschaft für Informatik (GI): BIOSIG 2008. Proceedings: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures,2008, pp. 39-46

10. Zhou, Xuebing; Kevenaar, Tom; Kelkboom, Emile; Busch, Christoph; van der Veen, Michiel; Nouak, Alexander: Privacy Enhancing Technology for a 3D-Face Recognition System In: Gesellschaft für Informatik (GI): BIOSIG 2007: Biometrics and Electronic Signatures: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures
11. Zhou, Xuebing: Template Protection and its Implementation in 3D Face Recognition Systems In: (SPIE) Biometric Technology for Human Identification IV. Bellingham: SPIE Press, 2007, 8 p. (Proceedings of SPIE 6539)

Paper (coauthor):

1. Busch, Christoph; Korte, Ulrike; Abt, Sebastian; Böhm, Christian; Färber, Ines; Fries, Sergej; Merkle, Johannes; Nickel, Claudia; Nouak, Alexander; Opel, Alexander; Oswald, Annahita; Seidl, Thomas; Wackersreuther, Bianca; Wackersreuther, Peter; Zhou, Xuebing: Biometric Template Protection: Ein Bericht über das Projekt BioKeyS In: Datenschutz & Datensicherheit. 35 (2011), 3, S. 183-191. - DOI 10.1007/s11623-011-0047-5
2. Kevenaar, Tom; Korte, Ulrike; Merkle, Johannes; Niesing, Matthias; Ihmor, Heinrich; Busch, Christoph; Zhou, Xuebing: A Reference Framework for the Privacy Assessment of Keyless Biometric Template Protection Systems In: BIOSIG 2010, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 2010, pp. 45-56
3. Busch, Christoph; Abt, Sebastian; Nickel, Claudia; Korte, Ulrike; Zhou, Xuebing: Biometrische Template-Protection-Verfahren und Interoperabilitätsstrategien In: Gesellschaft für Informatik (GI), Fachbereich Sicherheit – Schutz und Zuverlässigkeit: Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit, 2010, S. 1-12
4. Chindaro, Samuel; Deravi, Farzin; Zhou, Ziheng; Ng, Ming; Castro Neves, Margarida; Zhou, Xuebing; Kelkboom, Emile: A Multibiometric Face Recognition Fusion Framework with Template Protection In: The International Society for Optical Engineering (SPIE): Biometric Technology for Human Identification VII. Bellingham: SPIE Press, 2010
5. Nickel, Claudia; Zhou, Xuebing; Busch, Christoph: Template Protection for Biometric Gait Data In: BIOSIG 2010: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 2010, pp. 73-81
6. Kelkboom, Emile; Zhou, Xuebing; Breebaart, Jeroen; Veldhuis, Raymond; Busch, Christoph: Multi- Algorithm Fusion with Template Protection In: IEEE Third International Conference on Biometrics: Theory, Applications and Systems: BTAS 2009
7. Kelkboom, Emile; Breebaart, Jeroen; Veldhuis, Raymond; Zhou, Xuebing; Busch, Christoph: Multi-Sample Fusion with Template Protection In: BIOSIG 2009: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures. 2009, pp. 55-67
8. Wu, Di; Zhou, Xuebing; Niu, Xiamu: A Novel Image Hash Algorithm Resistant to Print-scan In: Signal Processing. 89 (2009), 12, pp. 2415-2424
9. Nickel, Claudia; Busch, Christoph; Zhou, Xuebing: Template Protection via Piecewise Hashing In: Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP 2009
10. Franssen, Thomas; Zhou, Xuebing; Busch, Christoph: Fuzzy Vault for 3D Face Recognition Systems In: 2008 Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Proceedings: IIH-MSP 2008

11. Busch, Christoph; Nouak, Alexander; Zhou, Xuebing; van der Veen, Michiel; Deravi, Farzin; Suchier, Jean- Marc: Towards Unattended and Privacy Protected Border Control In: Institute of Electrical and Electronics Engineers (IEEE): Biometrics Symposium 2007

Paper of Other Topics:

1. Hamon, Kevin; Schmucker, Martin; Zhou, Xuebing: Histogram-Based Perceptual Hashing for Minimally Changing Video Sequences In: Ng, Kia (Ed.), Badii, Atta (Ed.), Bellini, Pierfrancesco (Ed.): Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution. Proceedings: Axmedis 2006. Los Alamitos, Calif.: IEEE Computer Society, 2006, pp. 236-241.
2. Zhou, Xuebing; Schmucker, Martin; Brown, Christopher L.: Video Perceptual Hashing Using Interframe Similarity In: Dittmann, Jana (Hrsg.): Sicherheit 2006: Haupttagung Sicherheit – Schutz und Zuverlässigkeit. Bonn: Gesellschaft für Informatik, 2006, pp. 107-110. (GI-Edition – Lecture Notes in Informatics (LNI) P-77).
3. Zhou, Xuebing; Schmucker, Martin; Brown, Christopher L.: Perceptual Hashing of Video Content Based on Differential Block Similarity In: Computational Intelligence and Security: Springer, 2005, pp. 80-85. (Lecture Notes in Artificial Intelligence (LNAI) 3802).

Magazine:

1. Nouak, Alexander; Zhou, Xuebing: Erkennbar, aber ungleich: Sicherungsmöglichkeiten für Biometrie-Templates In: KES. (2010), 6, S. 71-73.
2. Kevenaar, Tom; van der Veen, Michiel; Zhou, Xuebing; Busch, Christoph: Privacy for Biometric Identification Information In: Datenschutz & Datensicherheit. 32 (2008), 6, pp. 393-395.

Patents

1. Stephen Wolthusen, Xuebing Zhou, Alexander Nouak, “ Forensic Analysis of Digital Video Streams”, German application, 2010
2. Xuebing Zhou; Martin Schmucker, “Sichern von Personen-Identitätsdokumenten gegen Fälschung”, Pub. No.: WO/2009/074342, International Application No.: PCT/EP2008/010607, Publication Date: June 18, 2009, International Filing Date: December 12, 2008
3. Xuebing Zhou, “Verfahren und Vorrichtung zum Erkennen eines Gesichts sowie ein Gesichtserkennungsmodul”, Pub. No.: WO/2008/034646, International Application No.: PCT/EP2007/008507, Publication Date: March 27, 2008, International Filing Date: September 21, 2007

Talks

1. “Security Evaluation of Template Protection”, invited talk at Workshop on Privacy and Security for Biometrics, Las Palmas de Gran Canaria, Canary Islands, May 10-11 2010
2. “Security Evaluation of Biometric Privacy Enhancing Techniques”, International Biometric Performance Testing Conference, NIST, Gaithersburg, USA, March 1-5, 2010
3. “Biometric Template Protection”, Teletrust, Darmstadt, September 10. 2008
4. “Zukünftige Trends in der Biometrie”, MATNET, Berlin-Schönefeld, July 14. 2008

5. “Towards Secure Biometrics – Applications of Template Protection for 3D Face Recognition”, Safety and Security Systems in Europe - IT for Security, Security for IT, Potsdam, October 09. 2007

Curriculum Vitae

Personal Data

Name	Xuebing Zhou
Birth date	November 20, 1977
Birth place	Shenyang, Liaoning, China
Nationality	China

Education

2011	Graduated as Dr. -Ing. with distinction at Technische Universität Darmstadt Doctoral thesis “Privacy and Security Assessment of Biometric Template Protection”
1999 – 2005	Graduation in Electrical Engineering (Dipl. -Ing.) at Technische Universität Darmstadt Diploma Thesis: “Digital Video Fingerprinting”
1996 – 1998	Study Mechanical Engineering at Tongji-University in Shanghai, China
1993 – 1996	Shenyanger 1. grammar school in Shenyang, China

Work Experience

2005 – 2011	Research staff member at competence center “Identification and Biometrics” of Fraunhofer Institute for Computer Graphics Research IGD

Honors and Prizes

2011	CAST/GI dissertation award in IT-Sicherheit 2011
2010	Winner of the European Biometrics Forum (EBF) Research Award 2010
2008	Nominated as an expert within the steering committee of the special group BIOSIG (Working group on Biometrics and electronic signatures) within the Gesellschaft für Informatik (GI)
2006 – 2009	Received the scholarship from Fraunhofer-Gesellschaft within the framework “Doktorandinnenprogramm”

Research Interests

- Biometrics
- Privacy enhancing techniques
- Security analysis
- Perceptual hashing

Projects (Selected)

- Project manager at Fraunhofer IGD for the projects "BioKeyS-Testing" and "BioKeyS – Pilot-DB – Teil 2" funded by the Federal Office for Information Security (BSI)
- Participant responsible for the development of 3D face recognition and template protection in “3D FACE” funded by the European Commission within the Sixth Framework Program for Research
- Participant responsible for video perceptual hashing in “eCrypt” and “AXMEDIS” funded by the Sixth Framework Program of the European Commission.

Academic Activities

- Program committee, international conferences of the Special Interest Group on Biometrics & Electronic Signatures of the Gesellschaft dür Informatik. BIOSIG 2009, BIOSIG 2010, BIOSIG 2011, Darmstadt, Germany
- Co-Chair of Invited Sessions, Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Darmstadt, Germany (IIHMSP 2010)
- Co-Chair of Special Session on Biometrics, Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Kyoto, Japan (IIHMSP 2009)