Towards Template Security for Iris-Based Biometric Systems

by

Marwa Fouad

Thesis

submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Electrical & Computer Engineering

School of Electrical Engineering and Computer Science
University of Ottawa

Abstract

Personal identity refers to a set of attributes (e.g., name, social insurance number, etc.) that are associated with a person. Identity management is the process of creating, maintaining and destroying identities of individuals in a population. Biometric technologies are technologies developed to use statistical analysis of an individual's biological or behavioral traits to determine his identity. Biometrics based authentication systems offer a reliable solution for identity management, because of their uniqueness, relative stability over time and security (among other reasons). Public acceptance of biometric systems will depend on their ability to ensure robustness, accuracy and security. Although robustness and accuracy of such systems are rapidly improving, there still remain some issues of security and balancing it with privacy. While the uniqueness of biometric traits offers a convenient and reliable means of identification, it also poses the risk of unauthorized cross-referencing among databases using the same biometric trait. There is also a high risk in case of a biometric database being compromised, since it's not possible to revoke the biometric trait and re-issue a new one as is the case with passwords and smart keys. This unique attribute of biometric based authentication system poses a challenge that might slow down public acceptance and the use of biometrics for authentication purposes in large scale applications.

In this research we investigate the vulnerabilities of biometric systems focusing on template security in iris-based biometric recognition systems. The iris has been well studied for authentication purposes and has been proven accurate in large scale applications in several airports and border crossings around the world. The most widely accepted iris recognition systems are based on Daugman's model that creates a binary iris template. In this research we develop different systems using watermarking, bio-cryptography as well as feature transformation to achieve revocability and security of binary templates in iris based biometric authentication systems, while maintaining the performance that enables widespread application of these systems. All algorithms developed in this research are applicable on already existing biometric authentication systems and do not require redesign of these existing, well established iris-based authentication systems that use binary templates.

Acknowledgements

I would like to seize this opportunity to pay tribute to all those who have contributed, one way or another, to the completion of this work, which marks another important milestone in my life.

First of all, I would like to express my heartfelt thanks to Prof. Emil Petriu taking an interest in my work and having the initiative to assume a guidance role, and helping me to submit this thesis.

I would also like to express my profound gratitude and great indebtedness to Prof. Abdulmotaleb El Saddik, for his benevolent supervision of my doctorate thesis. I thank him for encouraging and believing in me. His continuous support and constructive criticism, his invaluable advice, guidance, as well as his understanding were of great value to me. But most of all, I thank him for his patience with me through the highs and lows of this research time.

I deeply appreciate the help and contributions received from many people during this project: I am very grateful to Prof. Jiying Zhao. Your kindness and helpfulness will forever remain imprinted in my mind. I would also like to gratefully acknowledge the contributions of Fawaz A Alsulaiman. I really appreciate your help in a field that was new to me.

I dedicate this thesis to my husband, my supporting pillar, whose continual back-up and loving support was of great value in accomplishing this work. I also dedicate this thesis to my children; watching you grow is the greatest pleasure in my life and raising you has taught me so much about life and about myself.

Last but not least, I wish to repay the debt of gratitude I owe my beloved parents, my mentors and teachers, my idols and my heroes; for years of encouragement and for their strong belief in me. I owe them great appreciation for what I have learned and what I have achieved. I wish you were here with me, mom, but you're always on my mind and your love, support and wisdom are forever engraved in my heart and mind. God bless your soul and may you rest in peace.

Contents

List of Figures

List of Tables

List of Acronyms

Following are described the definition of acronyms that might have been used in the thesis:

FAR: False Accept Rate
FRR: False Reject Rate
FTE: Failure to Enroll
FTA: Failure to Accept
GAR: Genuine Accept Rate
EER: Equal Error Rate
ROC: Receiver Operating Curve
CRC: Cyclic Redundancy Check
ICA: Independent Component Analysis
AES: Advanced Encryption Standard
DCT: Discrete Cosine Transform
M2DCT: Modified Two Dimensional Discrete Cosine Transform
DWT: Discrete Wavelet Transform
DFT: Discrete Fourier Transform
FFT: Fast Fourier Transform
VQ: Vector Quantization
MCBA: Modified Correlation Based Algorithm
QIM: Quantization Index Modulation
HVS: Human Visual System
LSB: Least Significant Bit

Chapter 1 Introduction

1.1 Biometric Security

As we go about our daily lives, we often need to verify our identities or identify someone else. Biometrics is derived from the Greek words “bios” and “metrics”; which means “life” and “measurement” respectively. Biometric technologies are, hence, technologies developed to use statistical analysis of an individual’s biological traits to determine his identity. The objective of all biometric recognition systems is to automate the authentication process, which would bring greater security, efficiency, and convenience to our lives. Biometric traits suitable for automatic recognition systems are anatomical like fingerprints, iris prints, facial features, etc., which are inherent physical characteristics of an individual, or behavioral like gait, signature, speech patterns, etc., which are usually characteristics acquired naturally during an individual’s life time.

Anatomical or behavioral traits that qualify for biometric systems are characterized by: universality: does everybody has it, uniqueness: can we distinguish between users based on that trait, permanence: is this trait stable over a long time, measurability: can this trait be quantitatively measured for identification, performance: how accurate and fast can identification be performed, acceptability: is it acceptable by the public to be used for everyday access, circumvention: how easy is it to “fool” the system [47]. Biometrics authentication systems are convenient because they measure something we are, which cannot be lost like smart card or forgotten like passwords. But, on the other hand, unlike passwords that require exact matching for authentication, biometrics cannot be exactly matched. Hence, biometric authentication systems rely on pattern recognition and decision making algorithms to compensate for the inherent intra-user variability that can be the result of environmental, behavioral, or patho-physiological changes that can occur naturally or accidently. These pattern recognition and decision making algorithms also add to the imperfection of biometric recognition.

A biometric system usually consists of four main modules as shown in Figure 1; the first module is the biometric capturing module responsible for scanning or sensing the biometric trait. The capturing device varies from biometric trait to another, but also for

the same trait, different devices perform differently and hence subsequent modules should be adjusted accordingly to achieve best performance possible. The second module is the feature extraction module responsible for determining if the quality of the captured biometric trait is good enough for further processing or if a "retake" is necessary. If the quality is good enough for further processing, "features" are then extracted, which can distinguish between different users. Third in the biometric system is the matching and decision making module responsible for comparing captured biometric features with stored ones, compensating for the intra-user variations and calculating a similarity score that is then used for making the identity decision. The fourth module is the database module responsible for holding all the "original" set of features (called templates) of all users.

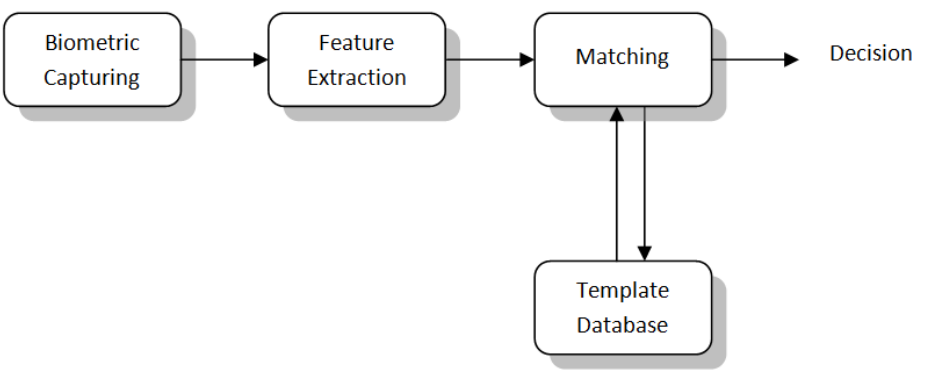

Figure 1 A generic biometric authentication system

Despite the inherent qualities, biometrics have their limitations. Most notably, biometric data are irreplaceable, they exhibit considerable variability, and they are subject to imperfect data acquisition. To better improve the performance of biometric systems, its vulnerabilities must be identified and addressed in order to avert security problems and to better promote their public acceptance for implementation on a large scale. Besides the practical limitations of biometric systems that include: Noise, Intra-class variations, Inter-class similarities, Interoperability issues, Intrinsic Errors (False Accept Rate - FAR, False Reject Rate - FRR, Failure to Enroll - FTE, Failure to Accept - FTA), and attacks, biometric systems face challenges not found in traditional security systems like the lack

of secrecy (fingerprints are left on objects, faces are captured on cameras, etc.) and the non-replaceability (unlike passwords, keys, or tokens, biometric data cannot be "reissued" once compromised) [3][5]. Another issue that arises with the growing number of applications using biometrics is the limited number of biometric traits, which raises concern about cross-application usage; how can a person ensure his biometric data used to access his account at the bank won't be used by the bank to access his medical records?

While some of these issues cannot be avoided due to the nature of biometrics, others have to be studied and possibly reduce their risk in order to make the widespread use of biometric authentication even possible. Possible attacks on biometric systems are shown in Figure 2 [15]. They can be grouped into four main categories [14]: Interface, Communication Channels, Modules and Database attacks.

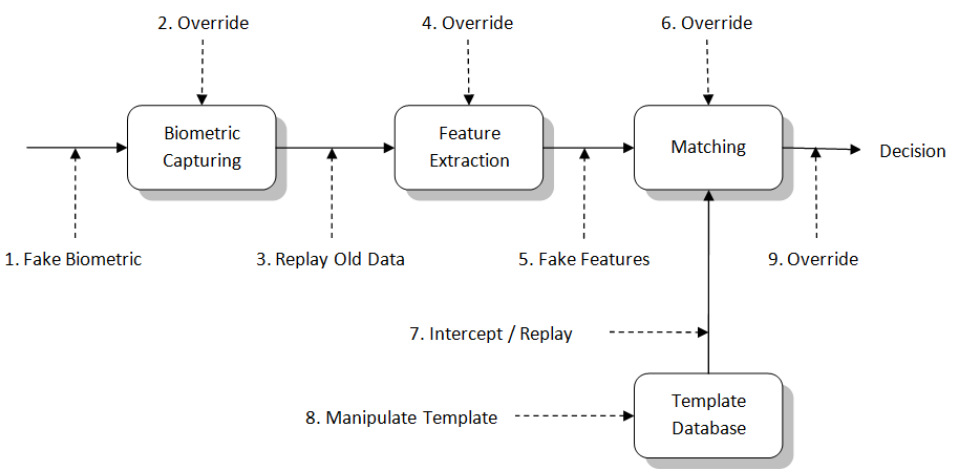

Figure 2 Attack points in a biometric system [15]

Interface attacks are mainly replaying a fake or intercepted biometric to gain access to the system. Spoofing attacks can be avoided by developing hardware and/or software solutions to detect aliveness.

Communication channels attacks take advantage of physical and crypto-graphical vulnerabilities in the data transfer between modules in order to intercept or alter the data.

Intercepted data from a successful authentication, even if encoded, could be replayed [8] at a different time to gain access. Countermeasures include timestamps [9], [10] and challenge/response mechanisms [11].

Modules attacks exploit software loopholes to access the system, either by modifying the output regardless of the input (Trojan Horse Attack) or by exploiting exceptions not handled by the algorithm. It is also always possible to attack a biometric system by overriding the output of the decision module.

Attacks on the template database are a major concern, because beside granting access to unauthorized users, it can also allow the use of intercepted biometrics into other biometric systems using the same trait, also referred to as function creep [1]. There is also the fact that because biometric templates are inherently unique, once compromised, these templates cannot be revoked or replaced, which compromises the whole biometric authentication system.

There are two major ways of attacking the template database: 1) Fake, in which attackers first reconstruct the biometric sample according to an intercepted feature template [7], and then import it to cheat the biometric system and get a legal login or an intention export; 2) Replacement, in which attackers directly use an imposter identity data to replace a genuine one in a database and get a legal identity. Because of the privacy of biometrics, in practical public applications biometric feature templates are generally used or stored in the biometric network system, and original biometric templates are only stored in a central database.

Compromising template security poses four main risks [6]: (i) biometrics in general are considered to contain personal information, (ii) biometric templates are irrevocable in nature, (iii) because of their uniqueness, biometric templates can be cross-referenced across different databases, and (iv) biometric templates can be reverse-engineered to create fake biometric traits.

Besides all the aforementioned reasons, in a biometric authentication system, there is no need for the complete images of the face, fingerprint, iris, etc. All the system really needs are only the features necessary and sufficient for authentication.

An ideal biometric template protection scheme should possess the following four properties [14]: 1) Diversity: The secure template must not allow cross-matching across databases, thereby ensuring the user's privacy. 2) Revocability: It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data. 3) Security: It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template. 4) Performance: The biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

Template protection has been gaining more attention in recent years and attempts in different directions have proven promising. The security analysis of existing schemes is mostly based on the complexity of brute-force attacks which assumes that the distribution of biometric features is uniform. In practice, an adversary may be able to exploit the non-uniform nature of biometric features to launch an attack that may require significantly fewer attempts to compromise the system security.

One way of securing biometric templates is to use smart cards that have acquisition, feature extraction and comparison embedded in them. This ensures that the template is always with the user and the system only receives a signal indicating positive or negative authentication results. While such a system could be more comfortable for users and might be appropriate for some access granting applications, such systems are not yet available for all biometric modes and more importantly do not work in systems that need identification. Hence, other ways for securing biometric templates need to be developed.

In general, template protection algorithms follow one of three main categories as shown in Figure 3:

In feature transformation, a transform is used on the template and only the transformed template is stored. If the template database is compromised, simply the coefficients of the transform are changed and hence a "new" template database is created. This category can be further divided according to the nature of the transform into invertible and non-invertible feature transformation. The challenge is to find a transform that will maintain uniqueness and separability of the templates of different users.

Biometric cryptosystems refer to algorithms that combine biometrics with cryptography. This method relies on the retrieval of a user specific key. If the key is directly generated from the user template we refer to it as key-generating biometric cryptosystem and if the user specific key is in some way combined with the template, we refer to it as a key-binding biometric cryptosystem. The challenge here is that standard cryptography is not a smooth function and small differences in the input result in huge differences in the output, which cannot be used for biometrics. Hence specialized algorithms have to be developed that can accommodate intra-user variability.

The last category of algorithms used in the literature for template security is watermarking. Watermarking refers to algorithms that hide a watermark into a cover work, in a way that makes the watermark imperceptible to humans. If the cover work is the biometric template, watermarking techniques can detect any tampering in the template. If the template is the watermark, watermarking techniques can make computationally difficult to extract the template from the watermark without esthetically compromising the cover work. Watermarking can also be used to hide one template into another, which accomplishes template security as well as multi-biometric authentication.

Each of these categories has its strengths and challenges that need to be studied carefully to choose the most suitable category for the application at hand.

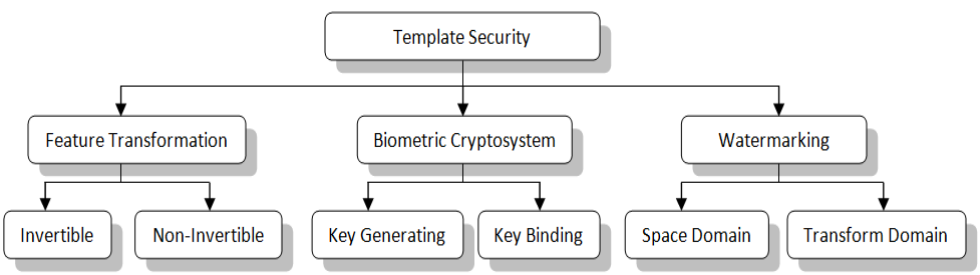

Figure 3 Categorization of template protection schemes (adapted from [14])

Template protection algorithms also depend on the biometric trait and in our research we chose to focus on iris based biometric systems. Iris based-biometric systems have many advantages over other biometric traits: (i) the iris is protected inside the human body and is, hence, less prone to environmental factors like cuts, sweat, dirt, etc, as in the case of fingerprints, (ii) the iris cannot be surgically manipulated without significant risk to the vision, (iii) the iris' reaction to light offers one of many methods of livelihood test against artifice, (iv) iris-based biometric systems [41][43][44], have proven to be highly accurate. Table 1 shows typical False Accept Rates (FAR) and False Reject Rates (FRR) of biometric authentication systems based on different traits.

Biometric Trait	***Test***	***False Accept Rate***	***False Reject Rate***
Iris	ICE 2006 [17]	0.1%	1.1%
Fingerprint	FVC 2006 [16]	2.2%	2.2%
Face	FRVT 2006 [17]	0.1%	1.6%
Voice	NIST 2006 [18]	3%	3%

Table 1 Typical performance of biometric recognition systems for different biometric traits.

In this research we will thus focus on the protection of iris templates. Although most of the general algorithms can be applied to any biometric trait, our research here focuses on implementations specifically designed to the special characteristics and nature of iris templates that will be later discussed in detail.

1.2 Motivation

The primary motivation for this research is the development of several algorithms that secure the template database in iris based biometric recognition systems, so as to ensure the revocability, privacy and security of the templates while maintaining the performance of already existing iris-based authentication systems. Securing the template database prevents of unauthorized cross-referencing among different databases using the same biometric trait as wells as insures the ability of issuing different templates in case the database is compromised. We focus our research on systems that use the binary

"IrisCode" developed by Daugman [41], which has been proven to be efficient in several large scale deployments across the world [43]. Template security has risen as the most serious attack on biometric based authentication systems because it not only compromises the affected database, but also all other databases using the same biometric trait [15].

Airports in the Netherlands, United Arab Emirates, United Kingdom as well as some other programs for border crossing like the NEXUS program US-Canada border and the CANPASS program in Canada, are already using iris recognition for their systems. Integrating security systems into these applications will significantly enhance their security and will put a lot of the public concerns about privacy and cross-referencing to ease. Concerns that biometric technologies are used for other applications than the ones users are aware of are increasing day after day, especially with increasing news about hacking and stolen identities. Our efforts to secure those templates and to offer means of revoking identities that are compromised will enhance the public acceptance of the use of biometric technologies for authentication purposes.

Most efforts to secure biometric templates has been focused on fingerprints [33], and although some research was dedicated to iris based biometric authentication systems, most of the research required a new iris recognition algorithm that would be suitable for existing template protection schemes. While this approach might be successful, it doesn't take advantage of the years of research put into binary "IrisCodes" that were developed by Daugman [41] and have been deployed on large scales in many international airports [43]. These new secure iris recognition algorithms would also require systems already in deployment to be completely changed in order to secure the templates. Replacing the whole system might be costly and more importantly inconvenient, which might deter from including template security into already deployed systems. The work in this thesis, thus, focuses on the template security of iris recognition systems that use binary IrisCodes for authentication. In this thesis we explore all three categories of template security for iris based biometric authentication systems, in each category we develop an algorithm for iris template security and test all algorithms using the same iris database. This gives us insight into the pros and cons of each category, as well as, helps us understand the challenges facing each category with reference to the iris based biometric recognition systems. This enables us to develop an algorithm that will combine the pros,

avoid the cons and most importantly achieve the four main objectives of revocability, privacy, security without compromising the performance of the iris based biometric authentication system.

1.3 Goals, Requirements and Challenges

In the following chapters, we will give an overview of each one of the proposed algorithms and review some of the methods and algorithms suggested in the literature. As we have mentioned before, while there has been some research in template security, there is very little research on iris templates. And even then, most of the literature on iris template security, is exploring new algorithms for iris recognition that is more suitable for existing template security algorithms.

Our goal in this thesis is to develop and implement several algorithms for securing iris templates. All the algorithms presented here can be appended to already existing iris based biometric recognition systems that use binary iris templates.

The requirements for accomplishing these goals are:

1) Revocability: It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

2) Privacy: The secure template must not allow cross-matching across databases, thereby ensuring the user's privacy.

3) Security: It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

4) Performance: The biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

The challenges in developing such algorithms for securing iris templates lies in trying to maintain seperability between different users or inter-user variability, as well as, account

for fuzziness of the templates of the same user, or intra-user variability. Maintaining those two variablities while providing revocability, preventing cross-matching and not affecting the performance of the biometric authentication system is no easy task. Another major challenge is developing algorithms that can be appended to existing biometric recognition systems using binary iris codes.

1.4 Thesis Overview

The thesis is organized in 7 chapters:

Chapter 1 gives an introduction and presents the motivation and goals of this research, as well as a list of the major contributions.

Chapter 2 provides a brief overview of how binary iris templates are generated and how iris recognition works. Then, feature transformation as a means of securing binary iris templates is explored by implementing several algorithms that were suggested in the literature and comparing their performance using a common iris database. This gives us a good understanding on feature transformation and guides future implementations.

Chapter 3 discuses in details biometric cryptosystems with its two subcategories: key-generating and key binding bio-cryptosystems. We also present in this chapter two key-binding algorithms for securing binary iris templates and for each method we will highlight 3 main points: (i) how the method deals with inter-user variability, (ii) what data is stored in the database, and (iii) what kind of security guarantee is offered.

Chapter 4 explores watermarking as a means of securing binary iris templates. A brief background is given about watermarking and then an algorithm is presented and evaluated using the same iris database used in all other algorithms throughout the thesis. Thus enabling an objective comparison between all different algorithms suggested in this research.

Chapter 5 describes in details a hybrid algorithm that combines all three different categories for securing binary iris templates in biometric authentication systems. The

suggested algorithm is, then, evaluated and results are compared to the other algorithms presented in earlier chapters.

Chapter 6 evaluates the novel field of securing templates used in haptic based authentication systems, by applying our proposed biometric cryptosystem. This is a new field that we tried to explore to assess the possibility of applying the same principals and algorithms used for iris templates in the new field of using biometric-haptic information to authenticate people.

Chapter 7 draws the conclusions reached and offers suggestions for future work.

1.5 Contributions

In this research, the security of biometric templates in iris-based biometric authentication systems will be analyzed and appropriate solutions will be proposed and developed to ensure; (i) diversity of the templates, which enables the same biometric trait to be used in different databases without any cross-reference, (ii) revocability of the templates, which enables reissuing of templates if the database or record is compromised, (iii) security of the iris templates, which makes it impossible for an imposter to reverse engineer the template to obtain the original iris image, and (iv) integrating the template protection schemes into existing well established biometric authentication systems without compromising the performance. Specifically, the major contributions of this dissertation include:

- ✓ Design and development of watermarking techniques to increase the security of iris-based biometric templates.
- ✓ Design and development of a practical biometric cryptosystem utilizing iris features that combines the benefits of biometric systems with the security of cryptographic systems.
- ✓ Adapting existing biometric cryptosystems that focus on using iris based biometric templates for key management to better suit our goal of protecting the iris-based biometric templates.
- ✓ Design and development of an algorithm that combines feature transformation, bio-cryptography and watermarking to secure binary iris templates.

- ✓ Exploring the possibility of extending the suggested systems to secure biometric-haptic information used to authenticate people in virtual environments.

1.6 Scholarly Output

The following are publications that resulted from the research in this thesis:

Papers in refereed Conferences:

- M. Fouad, A. Elsaddik, and E. Petriu, "***Combining DWT and LSB Watermarking to Secure Revocable Iris Templates",*** International Conference on Information Sciences, Signal Processing and their Applications, ISSPA 2010.

- M. Fouad, A. Elsaddik, J. Zhao, and E. Petriu; "***A Fuzzy Vault Implementation for Securing Revocable Iris Templates***", IEEE International Systems Conference, SysCon 2011.

- M. Fouad, A. Elsaddik; "***Using cyclic redundancy check to eliminate key storage for revocable iris templates***", Canadian Conference on Electrical and Computer Engineering, CCECE 2011.

- M. Fouad, A. Elsaddik, J. Zhao, and E. Petriu; "***Combining Cryptography and Watermarking to Secure Revocable Iris Templates***", International Instrumentation and Measurement Technology Conference, I2MTC 2011.

- M. Fouad, A. Elsaddik, and E. Petriu; "***Revocable Handwritten Signatures with Haptic Information***", IEEE International Symposium on Haptic Audio-Visual Environments and Games, HAVE 2011.

Chapter 2 Feature Transformation

Feature transformation was first suggested by Ratha et al [12] to protect templates from fraudulent usage. Feature transformation involves using a distorted version of the biometric signal or the feature vector [4],[11],[12]. If a specific representation of the template is compromised, the distortion transform can be replaced with another one from a transform database. Every application can use a different transform so that the privacy concerns of subjects related to database sharing between institutions can be addressed. Matching should be done in the transformed domain, so that original templates remain protected. Only transformed feature vectors are stored and used in the authentication process.

Design of such transformations is challenging, because it has to satisfy a couple of requirements. First, they have to maintain "uniqueness" of the biometric templates, i.e. the ability to distinguish between different users. Second, transformation of templates from the same user, but with different parameters should not give a positive match [13].

It is important to note that for successful template protection the transformation should be integrated in the template creation, so that the "real" template is never created and hence cannot be compromised.

2.1 Iris Template Creation

The first step in addressing iris template security is understanding how the iris template is created in the first place. In this section we will give a review of the iris template creation algorithm suggested by Daugman [41].

The iris is a protected internal organ of the eye, located behind the cornea and the aqueous humour, but in front of the lens. It is seen in cross-section in the anatomical drawing in Figure 4. It is the only internal organ of the body that is normally visible externally. Images of the iris adequate for personal identification with very high confidence can be acquired from distances of up to about 1 meter [41].

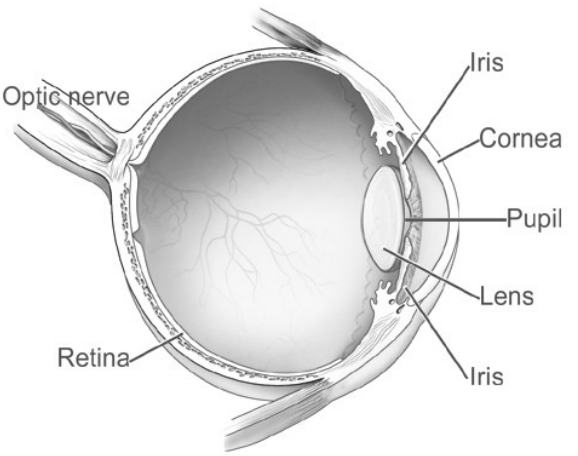

Figure 4. Anatomy of the eye [40]

Among the visible features of an iris are the trabecular meshwork of connective tissue (pectinate ligament), the collagenous tissue of the stroma, ciliary processes, contraction furrows, crypts, rings, a corona and pupillary frill, colouration, and sometimes freckles. The striated anterior layer covering the trabecular meshwork creates the predominant texture seen with visible light as depicted in the collage in Figure 5.

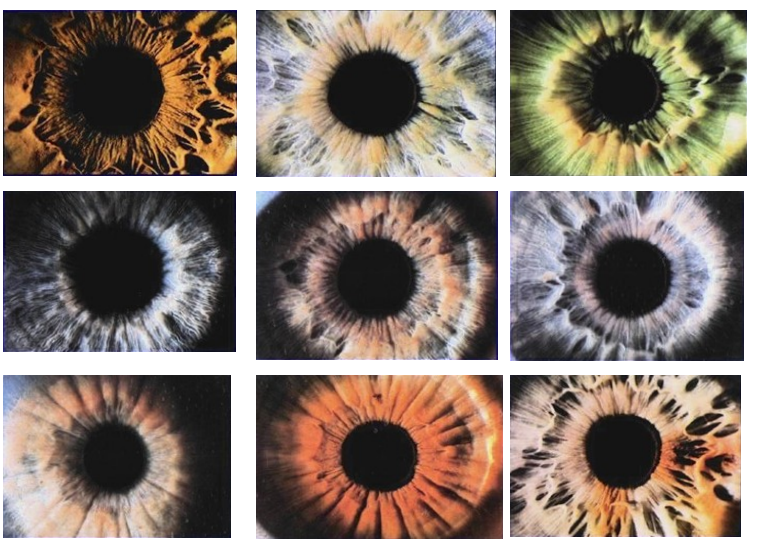

Figure 5. Examples of visibly different iris patterns

All of these sources of radial and angular variation taken together constitute a distinctive "iris print" that can be imaged from some distance. Further properties of the iris that enhance its suitability for use in high confidence identification systems include: (i) its inherent isolation and protection from the external environment; (ii) the impossibility of surgically modifying it without unacceptable risk to vision; and (iii) its physiological response to light, which provides one of several natural tests against artifice [42]. A property the iris shares with fingerprints is the random morphogenesis of its minutiae. Because there is no genetic penetrance in the expression of this organ beyond its anatomical form, physiology, colour and general appearance, the iris texture itself is stochastic or possibly chaotic. Since its detailed morphogenesis depends on initial conditions in the embryonic mesoderm from which it develops, the phenotypic expression even of two irises with the same genetic genotype (as in identical twins, or the pair possessed by one individual) have uncorrelated minutiae. This makes every iris as unique as every fingerprint, whether or not they share the same genotypes. But the iris enjoys further practical advantages over fingerprints and other biometrics for purposes of automatic identification, including: (i) the ease of registering its image at some distance from a subject without physical contact, unintrusively and perhaps inconspicuously; (ii) its intrinsic polar geometry, which imparts a natural coordinate system and an origin of coordinates; and (iii) the high level of randomness in its pattern, creating inter-subject variability spanning 266 degrees-of-freedom [43].

The human iris begins to form during the third month of gestation. The structures creating its distinctive pattern are complete by the eighth month of gestation, but pigmentation continues into the first years after birth, during which a blanket of chromatophore cells usually changes the colour of the iris, but the available clinical evidence indicates that the trabecular pattern itself is stable throughout the lifespan [42].

The layers of the iris have both ectodermal and mesodermal embryological origin, consisting of (from back to front): a darkly pigmented epithelium; pupillary dilator and sphincter muscles; heavily vascularized stroma (connective tissue of interlacing ligaments containing melanocytes); and an anterior layer of chromataphores and melanocytes with a genetically determined density of melanin pigment granules. The combined effect is a visible pattern displaying various distinctive features such as arching ligaments, crypts, furrows, ridges, and a zigzag collarette. Iris colour is determined

mainly by the density of the stroma and its melanin content, with blue irises resulting from an absence of pigment: long wavelength light penetrates and is absorbed by the pigment epithelium, while shorter wavelengths are reflected and scattered by the stroma. The heritability and ethnographic diversity of iris colour have long been studied, but until the present research, little attention had been paid to the achromatic pattern complexity and textural variability of the iris among individuals [43].

Being an internal organ of the eye, the iris is immune (unlike fingerprints) to environmental influences, except for its pupillary response to light. The elastic deformations that occur with pupillary dilation and constriction are readily reversed mathematically by the algorithms for localizing the inner and outer boundaries of the iris. Pupillary motion, even in the absence of changes in illumination (termed "hippus"), and the associated elastic deformations it creates in the iris texture, provide one test against photographs, glass eyes, or other simulacra for a living iris. Other tests involve changing infrared LED light sources which should cause corresponding changes in their specular reflections from the cornea; detecting the properties of contact lens which might contain a printed fake iris pattern riding upon the spherical surface of the cornea, rather than in an internal plane within the eye; testing for the properties of living tissue under varying wavelengths of both visible and infrared illumination; and so forth.

Iris recognition involves 4 main steps as shown in Figure 6: segmentation of the iris from the image of the eye, normalization of the circular iris into a fixed dimension rectangular strip, third is the feature extraction module and last is the matching module. In the following subsection a more detailed explanation of each module is given together with the results of the implementation. This implementation is based on Libor Masek's implementation [90]

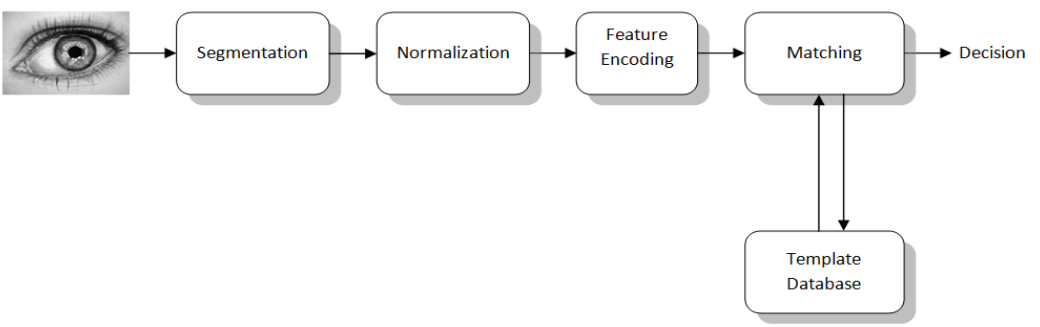

Figure 6. General diagram for iris recognition steps

2.1.1 Iris Segmentation

The first step in iris recognition is localizing the iris by finding its inner boundaries with the pupil and its outer boundaries with the sclera. This can be achieved by applying circular Hough transform to find the pupil and iris boundaries. This required the use of Canny edge detection to obtain the edge map. The database will be introduced in section 2.3.5. Linear Hough transform is applied on the edge map to detect eyelids as shown below and a simple thresholding detects the much darker eyelashes. Below is an example showing the different steps of iris segmentation.

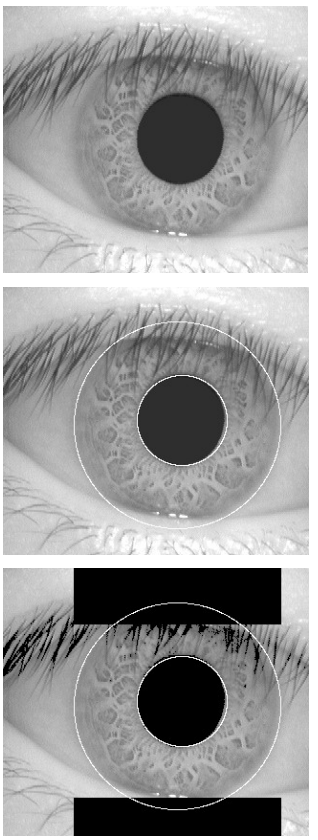

Figure 7. An example of an iris for the CASIA database before and after segmentation and eyelid and eyelash detection

2.1.2 Iris Normalization

After successful separation of the iris from the eye image, normalization takes place. Normalization refers to the process of obtaining a constant dimension iris image in preparation for feature extraction. Differences in pupil dilation due to difference in illumination, distance from the camera, head tilt or eye rotation all account for different size of extracted iris. Daugman's rubber sheet model [41] maps points within the iris region into a set of polar coordinates r → [0,1] and Θ → [0,2Π] as shown in Figure 8. To account for the fact that the center of the pupil and the iris are not concentric the following mapping equations are used:

$$r' = \sqrt{\alpha}\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_I^2} \qquad 2.1$$

where

$$\alpha = o_x^2 + o_y^2 \quad \text{and} \quad \beta = \cos\left(\pi - \arctan\left(\frac{o_y}{o_x}\right) - \theta\right)$$

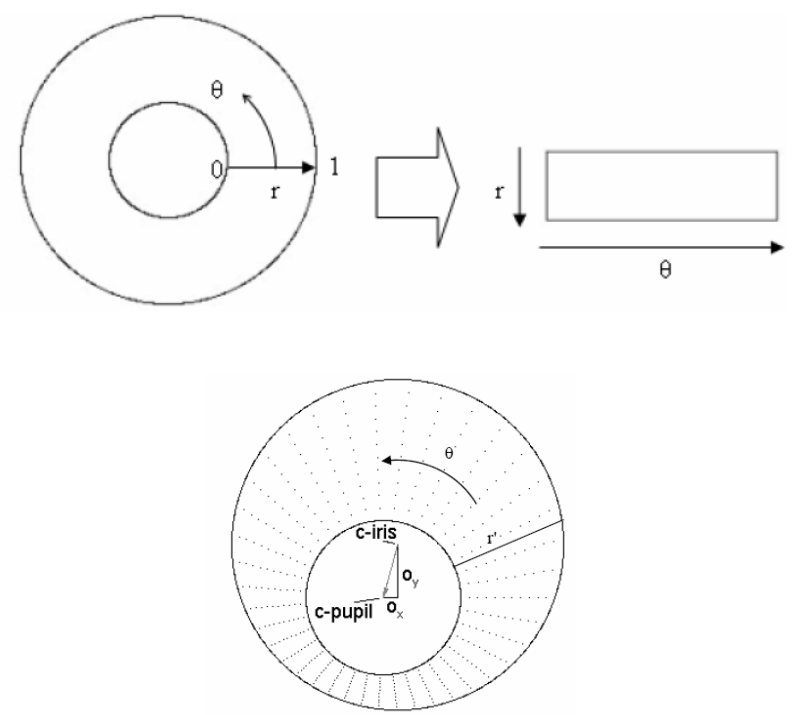

Figure 8. Iris normalization using Daugman's rubber sheet model [90]

Figure 9 shows the results of normalization on the segmented iris in Figure 7 together with the normalized mask of iris pixels occluded by eyelids or eyelashes. To obtain a 2048 pixel template the radial resolution is chosen to be 8 and angular resolution is chosen to be 128 in our implementation.

Figure 9. An example of the same iris after normalization together with the mask

2.1.3 Feature Encoding

After normalizing the iris it is convolved with 2D Gabor filters to extract unique textural characteristics of the iris. Here rows of the normalized iris are convolved with 1D Gabor wavelets. The resulting phase coefficients are then quantized as shown in Figure 10, where each phase coefficient is represented by 2 binary bits representing the quadrant the phase coefficient lies in.

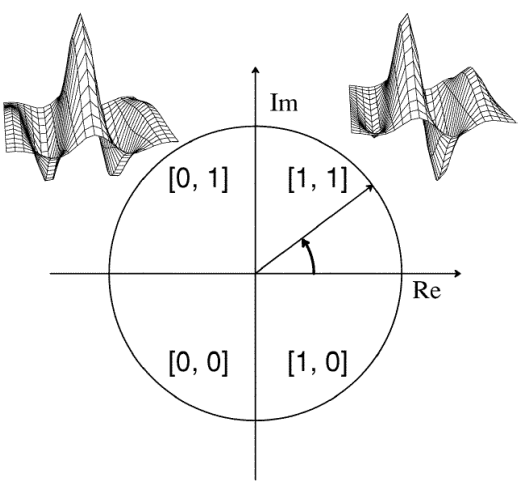

Figure 10. Quantization scheme for the phase coefficients to form the iris template [41]

This gives us the IrisCode that is stored in the database and subsequently used for matching. An example of an IrisCode and Mask are shown in Figure 11. The IrisCode together with the Mask constitute the iris template for a given individual. It has to be noted that IrisCodes of the two different eyes of the same individual do not match and hence care must be taken as to match the same eye of the individual every time authentication is required. It is very similar to fingerprints, where each fingerprint is independent from the other fingers of the same individual.

Figure 11. An example of the "IrisCode" of the same iris together with the binary mask

2.1.4 Iris Code Matching

To compare different "IrisCodes" the Hamming distance between them need to be calculated, which represents the bitwise difference between the two templates as a percentage of the total size of the template. The formula has also to account for masked bits from both masks and the formula used is as follows:

$$\mathrm{HD} = \frac{\sum(\text{Template 1})\text{XOR (Template 2) AND (Mask1) AND (Mask 2)}}{\mathrm{N} - \sum(\text{Mask 1})\text{OR (Mask 2)}} \qquad 2.2$$

Where N refers to the total number of bits in the iris template, Template 1 is the binary reference template; Mask 1 is the masked bits in the reference template; Template 2 and Mask 2 are the template and masked bits of the sample template to be compared with the

reference template. Figure 12 shows the hamming distance distribution for all the iris templates created in our database. The solid line refers to the hamming distances of iris templates belonging to the same user (genuine), while the dotted line refers to the hamming distance between iris templates from different users (imposter). If the hamming distance is below a predetermined threshold a positive match occurs. If it is above the threshold a negative match is decided. The vertical axis n refers to the number corresponding to each hamming distance value measured using all the samples in our database.

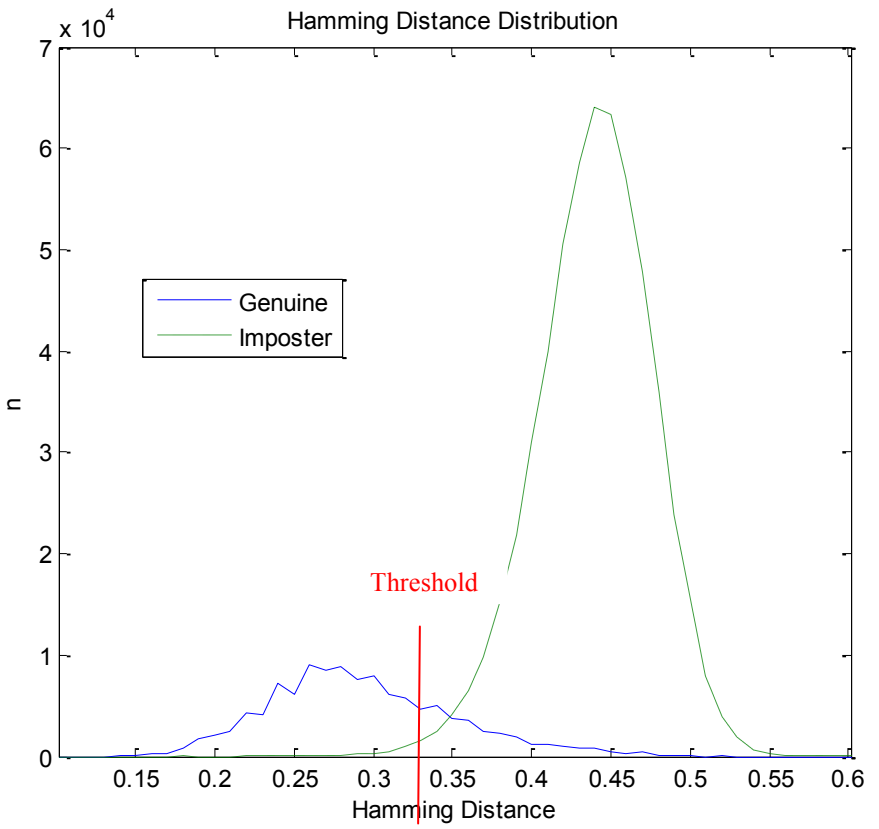

Figure 12. The Hamming distance distribution for genuine and imposter users

As we can see for the above Figure, there is an overlap between the genuine and imposter distributions, which means that for a certain threshold there will be some false positives

(False Acceptance Rate – FAR) corresponding to the part of the imposter curve below the threshold and some false negatives (False Rejection Rate –FRR) corresponding to part of the genuine curve above the threshold.

2.1.5 Performance Evaluation

To evaluate the performance of biometric recognition system the FAR and FRR of the system are calculated at different thresholds to determine the Receiver Operating Curve or ROC of the system. Each point on the curve correspond to the FAR and Genuine Accept Rate (GAR=1-FAR) at a certain threshold. Figure 13 below shows the ROC for our implementation. The Equal Error Rate (ERR) point refers to the threshold at which the FAR equals the FRR.

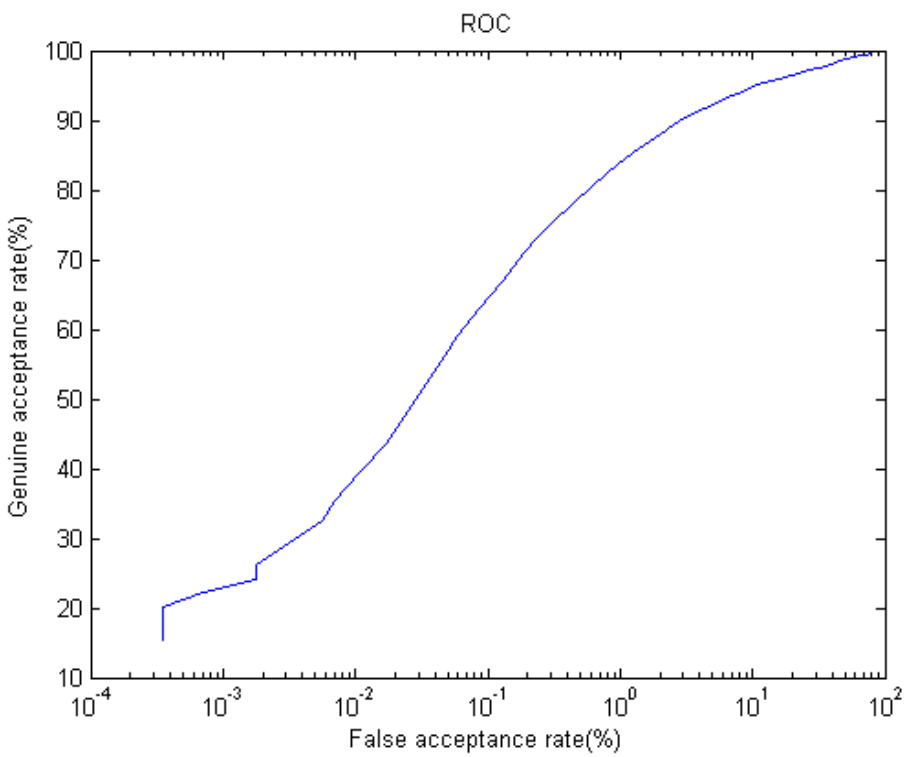

Figure 13. Receiver Operating Curve for the implemented Iris Recognition System

2.2 Invertible Feature Transformation

Feature transformation is achieved when a user specific key is used to determine the coefficients for the transform. The transformation occurs while creating the template and only the transformed template is stored and used for authentication. Invertible feature transformations rely on the secrecy of the user specific key in securing the iris template since the transform is invertible.

In the literature, only a couple of papers offered invertible feature transformation as a means of securing iris templates. In [64] the authors achieve template security and revocability by generating a pseudo random password and integrating it into the template creation. Their S-Iris code is generated by convolving segmented and normalized iris with 1D log Gabor filter in the angular direction and then using weak inner product of Gabor magnitude coefficients and the random password. The result is then binarized by thresholding to give the final S-Iris code. Their results show lower Equal Error Rate (EER) as well as reduced template size after S-iris encoding and again after the weak inner product algorithm compared to templates generated using only 1D Gabor filtering. This achieves the revocability desired for securing iris templates, but this scheme cannot be appended to already existing iris based authentication systems that rely on Daugman's binary Iris Code [42].

Another approach was presented in [75][76] by Kanade et al. and introduced an iris shuffling algorithm that uses a binary n-bit key to shuffle the iris code after dividing it in n segments. Their results show that the algorithm not only achieves revocability, but also increases seperability between the hamming distance distributions of genuine and imposter users.

2.3 Non-Invertible Feature Transformation

Ratha et al. [4],[12] first introduced the concept of cancelable biometrics, and later [81] they applied their idea on fingerprints. They proposed one-way transformations in the cartesian, polar and transformation domain.

In [46] the authors suggest two different ways of creating cancelable iris templates by applying non-invertible one-way transformation. The first method involves shifting and combining rows of the unwrapped iris image or binary iris template to create a new cancelable template. The second method uses a key to add a random noise pattern or a synthetic iris pattern again to the original unwrapped iris or the binary template to generate the cancelable template. While the first method offers cancelability, and does not need registration, its performance is compromised because the valid iris area that is not masked due to occlusion and that can be used for matching, is generally decreased after combing the rows. The second method of salting avoids this problem because the valid iris area remains the same, but it does need registration to compensate for any rotations in the iris prior to the salting.

Non-invertible feature transformation, while a very attractive idea, is still very difficult to successfully be implemented in practical systems [56], especially for iris templates that have been usually represented as a binary code where correlation exists between the bits. In this research we did not experiment with non-invertible transforms and iris templates need to be studied in future research to explore possibilities of transformations that will not break the underlying defining structure needed for the recognition, in order to achieve the desired performance.

2.4 Feature Transformation Evaluation

2.4.1 Iris Shuffling

In the literature, three different algorithms were suggested that use invertible feature transformation to introduce revocability to binary iris templates. To compare these three algorithms we implemented and evaluated them using the same database and recognition algorithm as a benchmark for comparing the three different algorithms. This would enable us to better understand the nature of the iris template and how the bits in an iris template are correlated. It also enables us to compare the different transforms in terms of how they affect the performance of the iris based biometric recognition system. Our intent was to use one of those algorithms to introduce revocability in future algorithms designed to secure iris-based biometric templates.

The first algorithm used in this research is an invertible feature transformation iris shuffling algorithm proposed in [75] as shown in Figure 14 . In this scheme, the iris code is divided into 128 blocks. A 128-bit user-specific key is the used to shuffle the iris code. All blocks corresponding to 1's are placed first, followed by the rest of the blocks corresponding to 0's. The size of the blocks has to be chosen carefully as to increase the user specific key length while maintaining the uniqueness of the features in the iris template. A longer key will result in smaller size blocks, which will destroy the uniqueness of the features in the iris template. After experimenting with many sizes a block size of 16 bits gave the best performance while maintaining a reasonable key size of 128 bits.

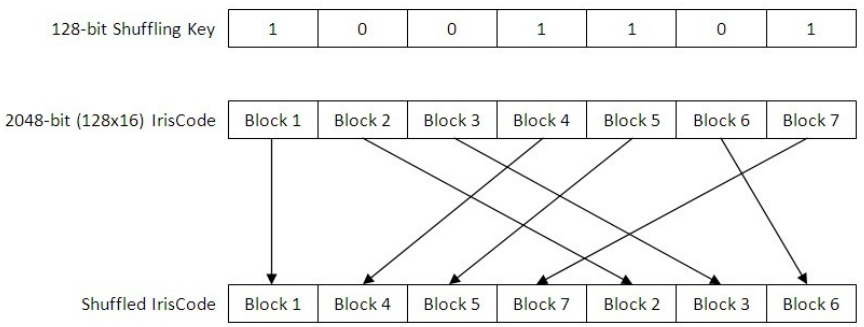

Figure 14. Iris shuffling algorithm (as proposed in [75])

2.4.2 Iris Folding

The second algorithm used is also an invertible feature transformation algorithm, proposed in [84], in which a random position is chosen according to a user specific key. This position serves as the starting point of the template that is rolled end-to end to form the new template, as shown in Figure 15. A user specific key is used as the seed for the random generator that chooses one of 256 columns and one of 8 rows. Once the position is determined the iris template is rolled end to end horizontally and vertically as shown in Figure 15. The vertically hashed rectangle is hence appended to the right of the template; the horizontally hashed rectangle is appended at the bottom of the template. In the figure the blue rectangle represents the original iris template, while the red rectangle depicts the "new" transformed one.

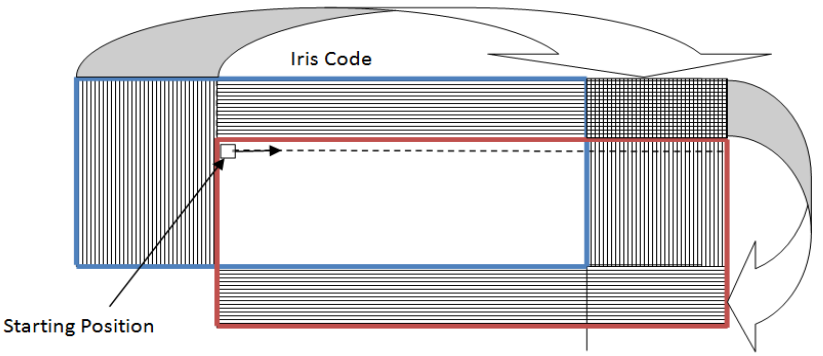

Figure 15. Iris folding algorithm (as proposed in [84])

2.4.3 Row Shifting and Permutation

The third algorithm we intend to use is the one suggested in [85] and is a non-invertible feature transformation algorithm; in this algorithm rows are shifted according to a user specific key and then rows are permuted to yield a "new" template. In the original algorithm[85], combination or rows by binary XOR operation were also added. In their discussion, the authors acknowledged that the combination of rows using XOR decreases the actual information bits in the template because masks are combined as well.

To avoid the loss of information bits due to overlapping masks that mask even more information bits in the template, the binary XOR combination of the rows was omitted in our implementation. The algorithm becomes hence an invertible feature transformation algorithm as illustrated in Figure 16. The results of our implementation will be shown in the following segment.

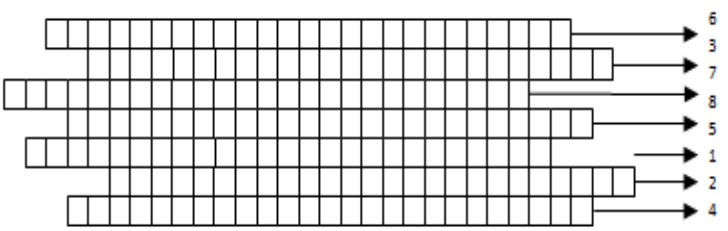

Figure 16. Iris permuting and shifting algorithm (adapted from [85])

2.4.4 Database

The chosen algorithms are evaluated using the CASIA V1 database [45] that consists of 756 iris images of 108 individuals and 7 images for each individual taken in 2 different sessions with at least one month difference. Images are all 8-bit gray images with a resolution of 320 x 280 and they are stored in bitmap format. In our experiments we use the first image out of seven for each individual as the template and the other 6 images are used for evaluation.

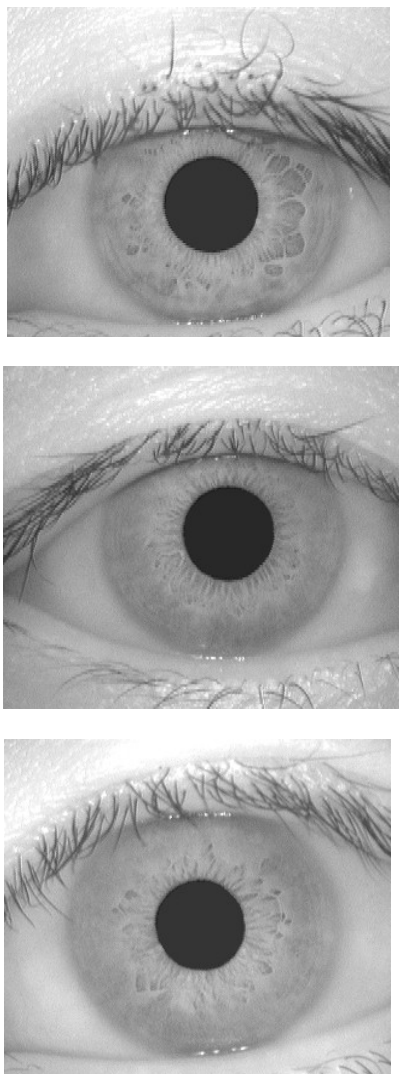

Figure 17. Samples of iris images from CASIA V1 database [45]

2.4.5 Parameter Values

In this section we discuss our choice of parameters for the three transformations. Binary iris templates are generated according to Daugman's scheme [41], which yields an 8x256 bit template. The template size is adjusted by altering the number of samples taken in the rubber sheet model. We maintained the 8x256 bit template size that Daugman uses in his iris recognition model to achieve the goal of keeping all our algorithms compatible with the model that is already deployed in many large scale applications.

For the iris shuffling algorithm the template is converted into a 2048-bit vector, that is in turn divided into 128 blocks of 16 bit each. Blocks were chosen big enough to ensure integrity of the features but small enough to ensure "good" shuffling. From experiments a 16-bit block proved to be a reasonable compromise.

For the folding algorithm, a user specific key is used a seed for the random generator, that randomly selects the column and row for the first element in the transformed template. The template is the rolled end-to-end to form the transformed template. To account for rotations of iris images during acquisition, the template is shifted by 8 elements in each direction to try to find the smallest hamming distance. An element is the 2 bits representing the quantization of the phase coefficients in the iris template.

In the third algorithm, there are 2 keys used; the first key determines the shifts in each row. And the second key is used to randomly permutate the order of the rows. For the first key, 8 shifts of a maximum of 16 bits in each direction are used to maintain the correlation between the different rows. The second key is used as a seed for the random generator used to permutate the rows' position.

To account for rotations of iris images during acquisition, again the template is shifted by 8 elements in each direction to try to find the smallest hamming distance.

2.4.6 Performance

The performance of the three one-way transformations was evaluated by calculating the genuine and imposter distributions in each case, as well as the receiver operating characteristics ROC curves for all three algorithms in comparison with the original

distributions and ROC curve. All three algorithms were tested using the same database for each user the same first template was used as a reference, while the other 6 were used for testing. Figure 18 shows the original Hamming distance distributions, where we can clearly see the overlap between the genuine and imposter distributions. The genuine distribution was vertically magnified for illustration purposes, but still we can see that both curves intersect at about a threshold of 0.35. The portion of the genuine curve above the threshold constitutes the FRR, while the portion of the imposter distribution below the threshold constitutes the FAR.

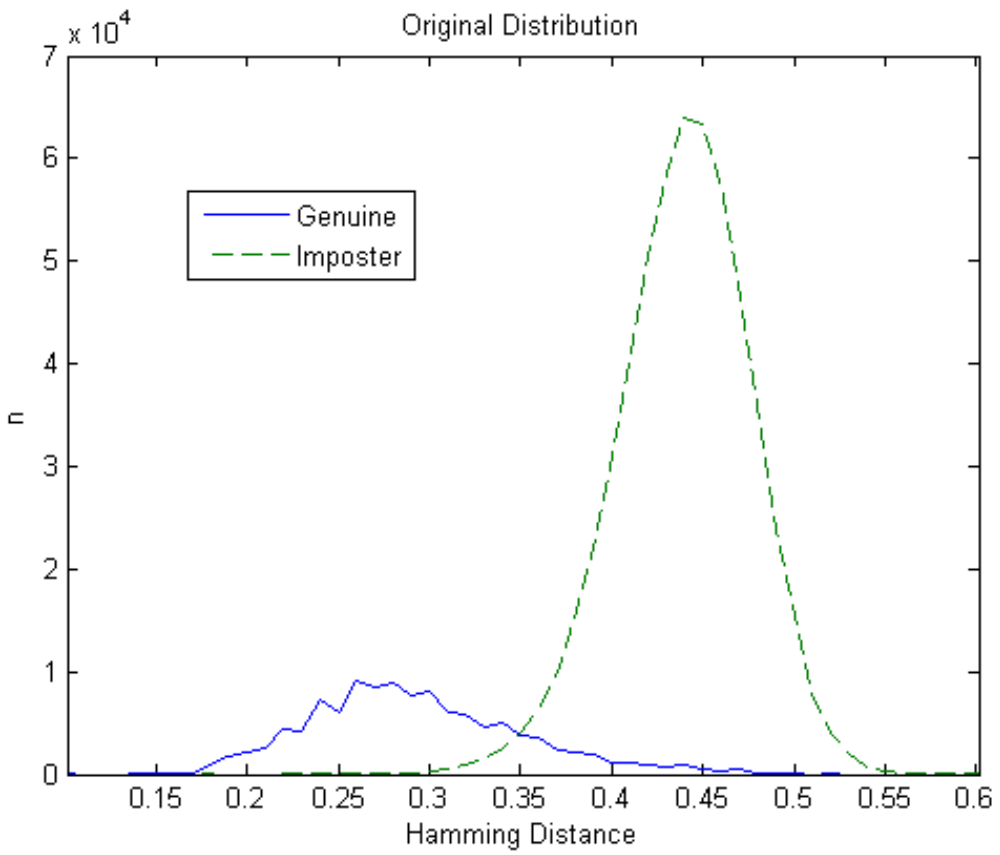

Figure 18. Original genuine and imposter distributions of the Hamming distances

After applying the shuffling algorithm described in section 2.4.1 and shown in Figure 14 the genuine and imposter Hamming distribution are as shown in Figure 19. One of the main objectives of feature transformation, as mentioned before, is to maintain the uniqueness if the templates after the transformation. From the figure we can clearly see

that the distributions are not only maintained but actually moved apart and now the curves intersect at a threshold of about 0.4. This improves the FAR and FRR because the portion of the genuine distribution above the threshold is now smaller and the portion of the imposter distribution below the threshold is smaller, too. This, hence, achieves revocability for the iris templates and actually improves the performance of the iris based biometric recognition system.

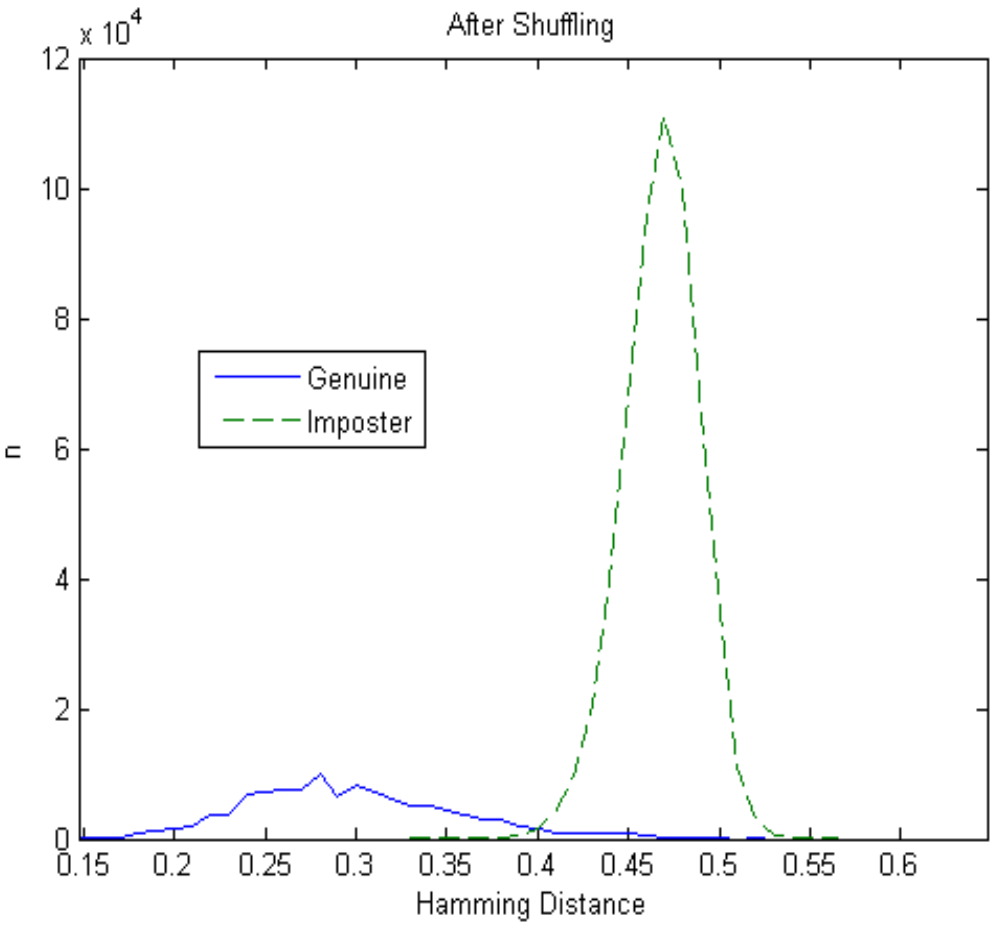

Figure 19. Genuine and imposter distributions of the Hamming distances after the shuffling algorithm.

The folding algorithm was described earlier in section 2.4.2 and a diagram in Figure 15 illustrated the algorithm. The performance of the folding algorithm as shown in Figure 20, shows also an improvement in the separation between genuine and imposter Hamming distance distributions with the curves intersecting at a threshold of about 0.39.

This is still an improvement compared to the original distribution, while introducing revocability to the iris template.

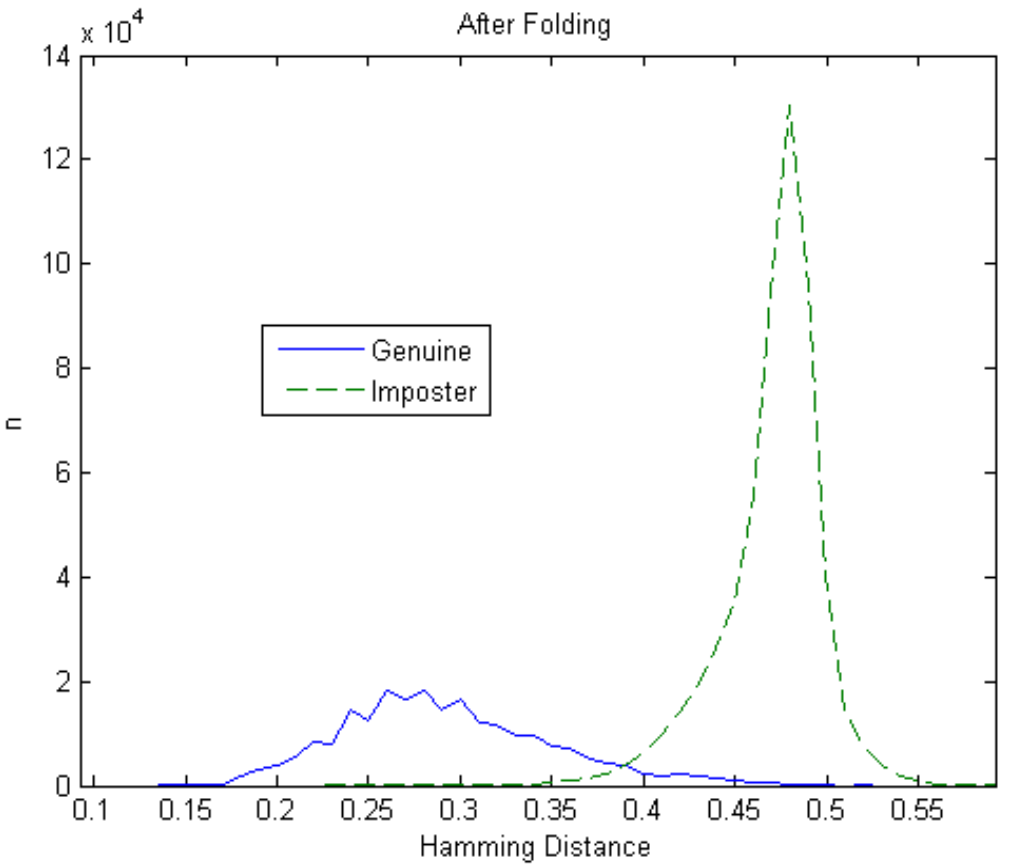

Figure 20. Genuine and imposter distributions of the Hamming distances after the folding algorithm.

The third algorithm of raw shifting and permutation was described in detail in section 2.4.3 and illustrated in Figure 16. The performance of this algorithm is shown in Figure 21 and we can see that the curves intersect at a threshold of about 0.41. Again, the performance of iris based biometric recognition system is actually improved while securing the iris templates by introducing revocability.

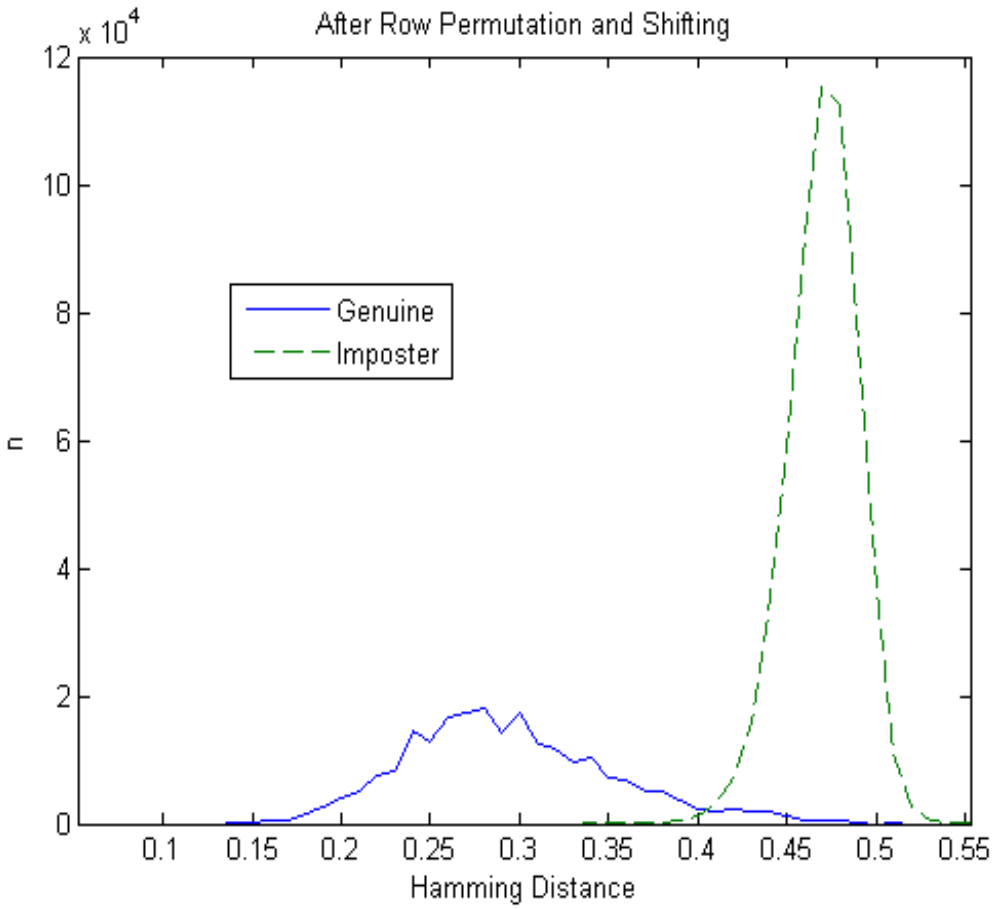

Figure 21. Genuine and imposter distributions of the Hamming distances after the the row shifting and permutating algorithm.

Figure 22 shows the ROC for all three algorithms together with the original ROC for comparison. We can clearly see that all three algorithms surpass the requirement of maintaining the performance by improving both the FAR and the FRR. The folding algorithm gives a noticeable improvement, while both the shuffling and row shifting and permutating algorithm significantly improve the genuine accept rate (GAR) even for very small FAR. This is very useful especially for high security applications where FAR has to be kept to a minimum; from the graph we can clearly see an improvement of about 4 times the GAR. Both algorithms perform very similar, while the row shifting and permutation algorithm performs slightly better.

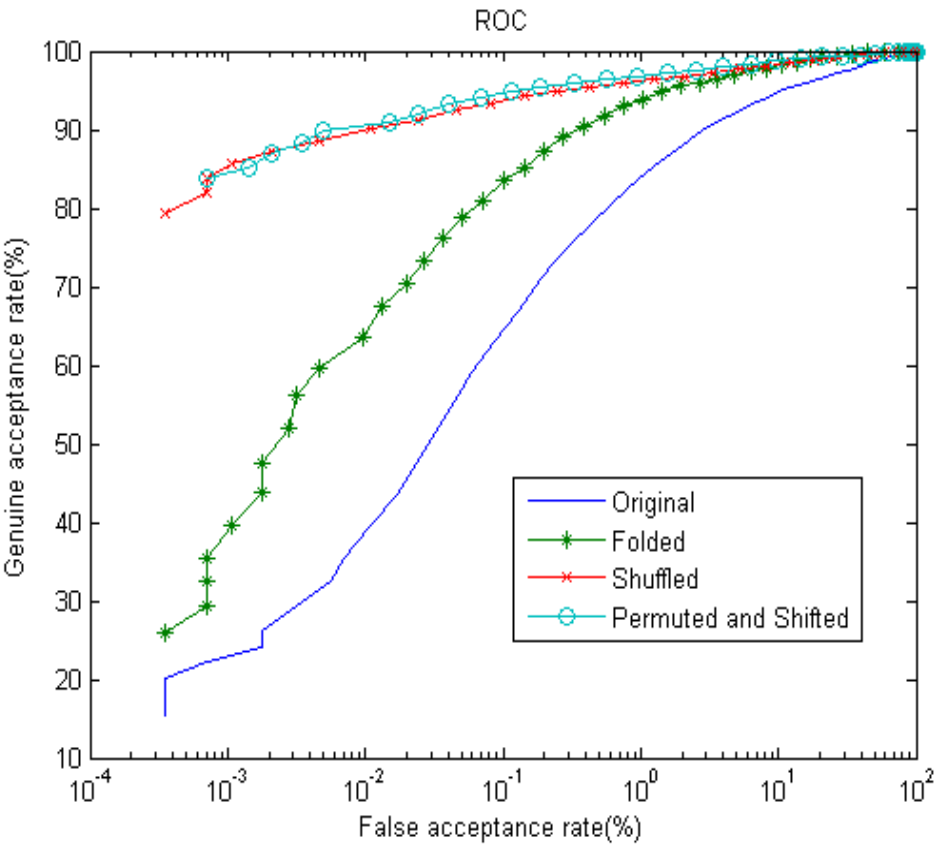

Figure 22. Receiver Operating Characteristics of the implemented invertible transformation.

2.4.7 Security Analysis

Feature transformation provides a means of revocability for otherwise irrevocable iris templates. But the fact that these transforms are invertible makes the security of the biometric system dependant on the secrecy of the keys. For an attacker to have access to the system, he has to provide an iris code and in addition to the key used in the transforms.

The shuffling algorithm uses a 128-bit key, while the folding algorithm uses an 11-bit key (3 bits for choosing the row and 8 bits for choosing the column in the 8x256 bit iris template). The shifting and permutation algorithm uses 4 bits for a maximum of 16 bits of shifting, plus one bit for direction, thus 5 bits for each row. Hence it uses 5*8 =40 bits for shifting the columns and 8! (= 16 bit) for permutating the rows. This adds up for a total of ~56 bits for both the shifting and permutation.

While these keys do not provide enough security by themselves, they do introduce revocability and hence increases the security of the existing biometric system. However, proper measures for securing the key are essential for ensuring the security of the iris based biometric system.

Comparing the three discussed algorithms for feature transformation, we notice that shuffling and permuting while shifting give very similar results while folding performs less. It still improves the system's performance, but not to the same extent. Hence, for the remainder of this research the shuffling algorithm will be adopted to provide revocability, while it can as well be replaced with permutation and shifting in any of the algorithms that will be discussed in the coming chapters.

2.4.8 Conclusion

With the increased use of biometric systems, the possibility of attacks on the template database also increases. As we can see from Figure 18 and 19, the proposed one-way transformations not only preserve the uniqueness of iris templates, but they actually increase the separability between genuine and imposter hamming distance distributions, These transformations serve to decrease the inter-class correlations present in iris-based biometric authentication systems.

The iris shuffling and row shifting and permutation perform very similar and well above the performance of the folding algorithm. This could be explained by the fact the most of the inter-class correlations are preserved, as opposed to the first two algorithms.

These invertible transformations offer little security when compared to non-invertible transforms, but their biggest contribution is offering revocability to the iris templates

without affecting and in fact improving the performance of the original iris based biometric authentication system.

Chapter 3 Biometric Cryptosystems

Biometric cryptography is the science of combining traditional cryptographic methods with biometrics either for securing the cryptographic keys or also for securing biometric templates. In either case the data stored should not reveal information that can be used to reconstruct either key or biometric template, but is necessary for key retrieval and/or biometric-based authentication. Matching is performed indirectly by verifying the validity of the extracted key, which eliminates the need for the matching module in the biometric system.

The successful implementation of integrating both fields is promising, while biometric technology possesses the potential of identifying individuals with great accuracy, thus providing a foundation for trust, cryptography, on the other hand, has a solid proven foundation for security and thus offers a means of transferring the trust from where it exists to where it is needed [48].

Biometric cryptosystems have three main challenges; first they have to accommodate intra-user variability (Intra-class Stability), second they have to successfully distinguish between different users (Inter-class Sensitivity), and third neither template or cryptographic key could independently be extracted from stored information [61].

These are not easy tasks because standard encryption is not a smooth function and a small difference in the values of the feature set extracted from the raw biometric data would lead to a very large difference in the resulting encrypted features. Also, standard encryption techniques, if applied for biometric template protection, require decryption before matching, which exposes the template for attacks. Besides, error correction coding assumes that biometric templates are independent and identically distributed (feature vectors are uncorrelated or independent random variables), which of course is not the case. Also, the entropy in a given biometric feature set will vary depending on both the feature chosen and also on the representation used for the template.

Biometric cryptosystems can be classified as key binding or key generating systems depending on how the cryptographic key is obtained. When the key used is independent of the biometric features, we refer to it as a key-binding biometric cryptosystem. If the

key used is derived from the biometric template, it leads to a key generating biometric cryptosystem.

3.1 Key-Generating

Key-generating bio-cryptosystems transfer a key into the stored identity code as illustrated in Figure 20. The key is combined with the biometric query to generate the stored code. During verification, the biometric sample is used in the same way as in the enrollment to create a sample code, which can be seen as a noisy version of the enrolment code. A corrupted codeword can then be obtained with the help of the biometric query and if the deviation between the enrolled and verified codewords is within the error correction ability of the applied coding method, exactly the same key can be retrieved. The publicly accessible identity codes should not reveal information about the original template or the key.

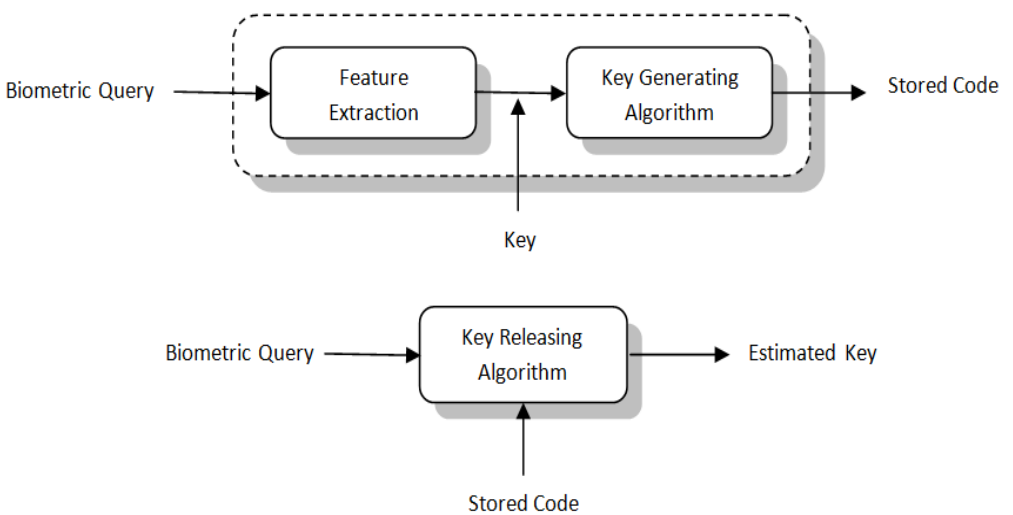

Figure 23 A generic key-generating biometric cryptosystem

Monrose et al. [73] where among the first to address biometric key generation by using key stroke dynamics and later voice features [74] to create a hardened password. Their

technique relies on identifying which features, in this case, which keystroke latencies, are "distinguishing" for a specific user, and which are not. To do so, they set a global threshold for each feature, and extract a bit for each user by assigning a 0 or 1 if his measurements are consistently below or above that threshold. If the user does not provide measurements that fall consistently on one side of the threshold, then the system ignores that feature for that user.

Davida et al. [51],[52] proposed an algorithm for template protection based on the iris biometric. They assumed that the iris template (as suggested by Daugman [44]) from different sampling of the same iris can have up to 10% difference and that iris template of different irises differ in as many as 45%. During enrollment, multiple scans of the iris of a person are collected and k-bit iris templates are generated for each scan. The multiple iris templates are then combined (through a majority decoder) to arrive at a canonical iris template of the same length. A bounded distance decoding error-correcting code [60] is then constructed by adding C check bits to the K-bit iris template (C is determined such that 10% of bits can be corrected) resulting in an N–bit codeword, denoted by T||C. The codeword is hashed and digitally signed, and together with the check bits C, stored as the database template for the user. At the time of authentication, again, multiple samples of iris of a person are collected and T′ is estimated. The check bits C from the database template are used to perform error correction on the codeword and the corrected iris template T″ is produced. Then T″||C is hashed and signed and compared to the signed-hashed-code in the database. Although iris templates from the same iris are assumed to differ in only 10% when in fact it could be up to 30% [44], the idea of acquiring multiple samples is hoped to minimize the errors. The assumption, though, that iris templates are completely aligned is one thing that had to be addressed in future implementations of the algorithm for a more a better performing iris based secure biometric authentication system.

In [70] the authors adopted a different approach to minimize intra-user variability. They used only the inner ¾ of the lower half of the iris for their feature extraction, arguing that this is the part most stable and consistent for iris recognition and the least affected by eyelashes and eyelid occlusions. They then applied Reed-Solomon to the extracted feature vector that is stored together with the key encrypted hash values of the feature vector.

To generate a key from an iris image or feature vector is a very complicated task, since the process must accommodate intra-user variability and at the same time maintain inter-user variablities. This is why, most template protection schemes do not fall under this category and especially if one of the goals is to be able to apply the suggested algorithm to already existing binary iris templates.

3.2 Key-Binding

Key-binding bio-cryptosystems transfer a key into the stored identity code as illustrated in Figure 21. A user specific key is generated by a pseudo random number generator, which is then subsequently extended to a codeword after an error correction encoder. The result is the hashed resulting in the pseudo identity. The key-binding algorithm integrates both the codeword and biometric template into the stored identity code. In the verification, the key-releasing algorithm uses the acquired biometric sample, which can be seen as a noisy version of the enrolment template, a corrupted codeword can be obtained. If the deviation between the enrolled and verified codewords is within the error correction ability of the applied coding method, exactly the same key can be retrieved. The publicly accessible identity codes should not reveal information about the original template or the key.

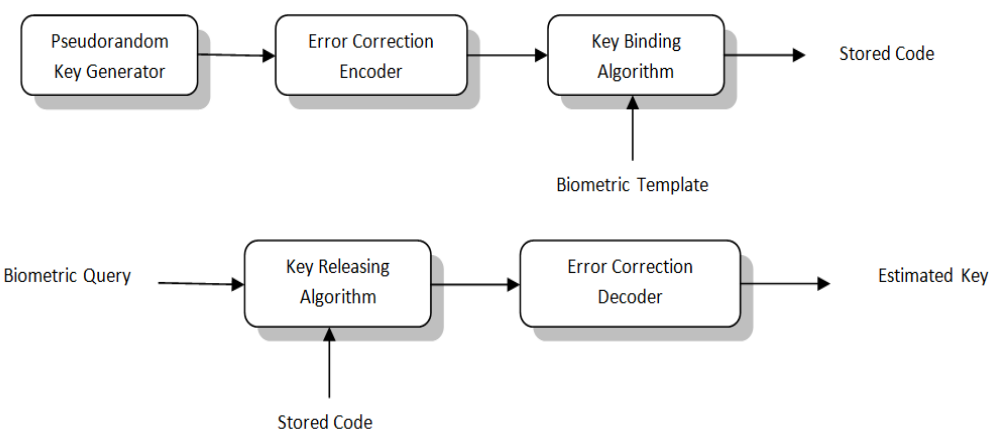

Figure 24 A generic key-binding biometric cryptosystem

One of the widely used key-binding biometric cryptosystem is the "fuzzy commitment" scheme [62] suggested by Juels and Wattenberg, in which the user selects a secret message C from a set of codewords of some error-correcting code at the enrollment time. To commit to a value x, the user selects a codeword c uniformly at random from C and computes an offset of the form δ=c-x. The commitment then consists of the pair (δ; y), where y=h(c) for some suitable one-way function h. To decommit using key x', the user computes δ+x' and, if possible, decodes to the nearest codeword c'. The decommitment is successful if h(c')=y. Again in this scheme, complete alignment of ordered feature sets is assumed, which is not the case in practical applications and need to be addressed for a successful implementation.

Another key-binding biometric cryptosystem are shielding functions that were suggested by Tylus et al.,[53],[54],[55] for template protection. They assumed that a noise-free template X of a biometric identifier is available at the enrollment time and use this to enroll a secret K to generate a helper data P. Shielding functions are described as "δ-contracting" and "Є-revealing" functions. δ-contracting refers to the function's ability to give the same output (helper data) for all inputs within a δ distance of the original input X (template). And Є-revealing refers to its ability to conceal the information, so that the helper data P reveals up to Є-bits of the secret K (key) or original input X (template).

In their implementation for the protection of fingerprint templates Tylus et al. assume that each dimension of the template is quantized at q resolution levels. In each dimension, the process of obtaining P is equivalent to finding residuals that must be added to X to fit to odd or even grid quantum depending upon whether the corresponding K bit is zero or one. At decryption time, the "noisy" biometric template X' is used to decrypt and obtain a decrypted message K', which is approximately the same as K. It is hoped that the relatively few errors in K' can be corrected using error-correction techniques. Again, the proposed technique assumes that the biometric representations are completely aligned and that noise in each dimension is relatively small compared to the quantization Q.

Dodis et al. [57] formalized the idea of using error correction codes to deal with inter-user variablities. They introduced the terms secure sketch and fuzzy extractors for template protection. Fuzzy extractors are schemes that allow the extraction of stable string k (key) from in a noise-tolerant way. In order to be able to re-extract the key,

during enrollment some helper data P need to be generated that does not compromise the security of the key.

A basic tool needed in the development of fuzzy extractor is the secure sketch, which are derived from information theory and they view biometric templates as messages that go through noisy communication channels and the goal is to retrieve the “original” message from the “corrupted” received message. These methods hope that without knowledge of the “original” message or template in our case and given the helper data P, we’ll be able to “retrieve” a key k.

The main concept is that given a string W and the sketching function we are able to create a “sketch” P that does not leak too much information about W. With the help of the sketch or helper data and a string W’ that is close to W according to some measure of similarity to some predefined tolerance threshold, we should be able to recover the original string W or key S.

One possible construction, suggested by the authors, was to use code c randomly chosen from an (N,K,D) codeword space. The sketch P is chosen as the c-x and is stored together with the hash value H(c). At the time of authentication, an estimate c’ is calculated as P+x’ and after applying error correction decoding H(c’) is compared with the stored value of H(c) and authentication occurs only if both values exactly match [59].

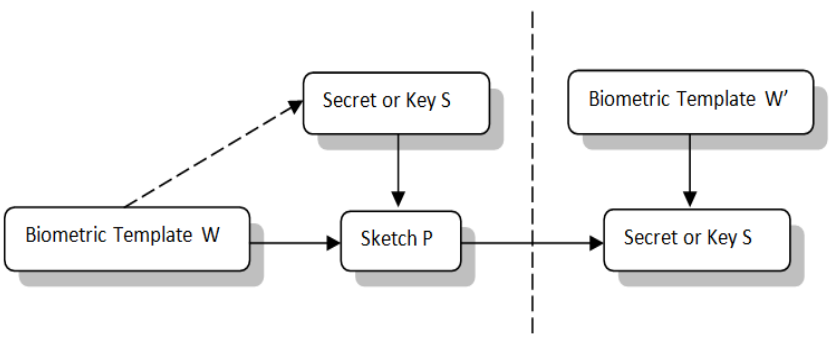

Figure 25 Fuzzy sketches

Fuzzy sketches were studied in [50] to apply them to protect iris templates and to try to find their theoretical limits. A coding/decoding scheme was suggested that achieved near classical performance rates. Their main idea is the use of an iterative min-sum algorithm on a 2D product code that in turn is constructed of 2 binary Reed-Muller codes of order 1 to achieve efficient error correcting for iris templates.

Juels and Sudan's fuzzy vault scheme [63] is one of the most popular algorithms implemented for fingerprint template protection. During Enrollment a key is used to determine the coefficients of an n-degree polynomial as shown in Figure 23. The user specific polynomial is used to map the feature set (x-axis) to the "secure" feature set (y-axis = p(x)) by evaluating them using the polynomial.

Because the sequence of the feature points are not taken into account, fuzzy vaults require an unordered feature set, i.e. a feature set where the position or sequence of elements are not required for authentication.

To prevent intruders from estimating the polynomial, and hence the user key, from the stored "secure" feature set represented as black points in Figure 23, points that don't lie on the polynomial are then added as chaff points to hide the real feature points and are presented as red points in Figure 23.

Genuine mapped feature points together with the chaff points are stored and now form the fuzzy vault. To "unlock" the vault a sample template is acquired and then using the user key is mapped using the polynomial.

Comparing the mapped points with the fuzzy vault, the nearest points in the fuzzy vault are chosen to try to estimate at least (n+1) genuine points so reconstruction of the polynomial through Lagrange interpolation would be possible. If successful, coefficients of the polynomial should match the stored key.

The main challenge when using the fuzzy vault with iris templates is that it requires the creation of iris templates, whose coefficients comprise an unordered set, which is not the case with most iris-based authentication systems that use Daugman's [41] model. Another challenge is the fact that Daugman's iris code is binary, which makes it impossible to implement a fuzzy vault using these binary templates.

An implementation of the fuzzy vault to protect iris templates was suggested in [68],[69]. To obtain an unordered feature set that can be used in the fuzzy vault scheme; the iris texture was represented as nodes and end points similar to those used in fingerprints. These points' polar coordinates are used together with Cyclic Redundancy Check (CRC) to account for rotations and fuzziness in iris templates. CRC refers to a number of bits appended to a message to recognize errors in the received message. A 128 bit key and 16 bit CRC for a total of 144 bits. A polynomial of degree 8 is used for the fuzzy vault. Chaff points in the order of 10 times the genuine points are added to create the fuzzy vault. And in [69] hardening of the Fuzzy vault was achieved by using a password that is used as a key to determine translations of minutiae points. This hardened fuzzy vault offered revocability of the iris templates.

Another implementation of the fuzzy vault for iris template protection was suggested in [66],[71]. The authors implemented an Independent Component Analysis (ICA) based fuzzy vault system that uses a pattern-clustering technique together with a local shift-matching method to account for interclass variations. These enabled the generation of an iris template whose elements constitute an unordered set that is suitable for fuzzy vault construction

In [77] another realization of iris-based fuzzy vault is introduced. This time a modification to the classic fuzzy vault is introduced, in which two matrices are created to form the fuzzy vault. The position, in the first matrix rows (called Grid B), corresponds to the position on the x–axis in Figure 23. The evaluation of the polynomial p(x) corresponds to the position in the matrix columns. Instead of a polynomial that is user dependant, another matrix (called Grid C) is used that determines the positions of the elements in each row, and the chaff points are the rest of the elements in the matrix. The Grid C matrix is formed by computing the CRC codes of the message and appending it to the feature vector, which are further encoded with Reed-Solomon encoding algorithm. Grid C is then formed by randomly (among columns while preserving the row position) putting the RS codes into the Grid. Iris features are then put into Grid B in the same positions as the RS codes. Grid C and B form the fuzzy vault. The feature vector in this proposed modified fuzzy vault scheme was obtained by computing the average of 16x4 blocks of the 2-D Gabor filtered iris picture. The results of this scheme proved promising but again required a development of a new iris matching algorithm.

In [79],[80] the authors again implemented an iris template based fuzzy vault system. A secret is used as coefficients for the polynomial p of degree d. Random n points (>>d) are chosen and evaluated at p and the set is then encoded using a Reed-Solomon code and hashed to produce the stored helper data H. The iris template is divided into n parts and a set Δ is formed by subtracting the iris template parts from the code words. Then Δ and H are stored to form the fuzzy vault. The suggested scheme was tested on a very small database and the results showed a much higher FAR and FRR than the original "non-secure" iris based biometric recognition system.

Hao et al. [48] proposed a different key-binding iris template protection scheme, in which a random key is entered into a coding module to generate a 2048 bit string adapted to the Daugman's iris code length [53]. The encoder also includes random (Hadamard) and burst (Reed Solomon) error correction codes to compensate for the fuzziness of biometric templates. The choice of the error correction coding parameters was based on studying the errors in iris code and the genuine and imposter distributions. They found two types of errors, burst errors caused by eyelid occlusion and eyelashes; and random background errors cause by environmental elements, like lighting, camera noise, etc. During authentication, the acquired iris template is encoded the same way. If by using error correction codes the acquired key is equal to the original key. A simple comparison between their hash functions serves as the authentication and decision making module. The use of a password that encodes the stored code or to permutate the rows and/or columns of the Hadamard matrix was also suggested to further enhance the security. The proposed system acts considerably well with key lengths of up to 140 bit long however the efficiency of the system starts to deteriorate once the chosen key length becomes longer.

Another iris template protection scheme was introduced in [75], where they base their system again on Hadamard and Reed-Solomon Codes to correct background errors and burst errors respectively. To increase the error correction capability of Hadamard Codes, iris templates are uniformly padded with zeros (to increase error bits relative to the total number of bits). A user password is then used as a binary key to shuffle blocks of the iris code to ensure security (revocability). They were able to achieve an 83 bit entropy which is much higher than the 44 bit entropy achieved in [48].

In [76] the authors used a couple of keys; one k1 to be block-wise encoded with Hadamard encoding algorithm and then xored with the iris code to give the locked iris code, and k2 used to shuffle the iris code according to [75]. The block-wise hashed k1, shuffled iris code, locked iris code and k2 are then hashed using a password to form the stored template.

In [78] again Reed-Solomon encoding is combined with convolution encoding to account for inter-user variability. They chose concatenated code to increase key length as well as error correcting capabilities. Bit masking was used to transform burst errors into random ones, so they can use convolutional error correction code that is suited to deal with random errors. Compared to block coding used in [48], the authors claim that the concatenation of codes was able to achieve better error correction.

3.3 Proposed Key-Binding System

Bio-cryptosystems rely on error correction codes to compensate for inter-user variablities, and on the minimum leakage of the stored helper data for the security of the template. Despite the voluminous literature available on bio-cryptosystem, most of the schemes proposed offer theoretical solutions that face a lot of challenges when implemented in order to achieve practically acceptable performances. Also, most of the main ideas are general to all biometric modalities and we believe that more specialized schemes need to be created. This will enable the exploitation of the specific features of the iris as well as ensure that performances of classic iris recognition methods can be matched if not improved. Enhancing the performance of iris based biometric recognition system while ensuring security and revocability is needed for successful large scale deployment of such systems.

To this regard Hao et.al [48] carefully studied iris codes and errors in them that cause intra-class variability, and identified two types of errors; burst errors caused by eyelashes and eyelid occlusion and random errors caused by environmental changes like position, light, etc. They used concatenated Hadamard (for random errors) and Reed-Solomon (for burst errors) error correction encoding/decoding to account for those errors. Hadamard codes of length 2^k are capable of correcting up to $2^{(k-2)}$-1 errors. According to their

scheme, a random user specific key is encoded into a pseudo-iris code. The key is discarded and never stored. The pseudo-iris code is then XORed with the reference iris template to obtain the locked iris code. At verification time, a sample iris code is then XORed with the locked iris code to recover the pseudo-code, which in turn is decoded using Hadamard then Reed-Solomon decoding to retrieve the user-specific key. Only the locked iris code is stored.

Hadamard codes are generated using Hadamard matrices, which are square orthogonal matrices, whose elements are either +1 or -1. Orthogonality means that the any two rows or columns represent two perpendicular vectors, whose inner product is always 0. This also means that any two rows or columns match in half of their elements and mismatch in the other half. In the Sylvester method the matrix size is a power of 2 [49]. The Hadamard Code is obtained by appending –H to H, where H is the Hadamard matrix. The codewords are obtained by replacing -1 with 0 in the rows of the resulting matrix. A Hadamard matrix of size $n = 2^k$ has 2n codewords. The code has minimum distance 2^{k-1} and hence corrects up to $2^{k-2} - 1$ errors. To encode a value x, we find the xth row of the Hadamard code matrix.

For decoding the received vector y is multiplied with the transpose of the Hadamard code matrix after replacing all 0's with -1. Decoding is successful when there is one distinct absolute maximum value in the result. The position of the absolute maximum results in the decoded value.

Hadamard codes can correct up to $2^{k-2} - 1$ ~25% of the errors, but iris codes from the same user can differ in up to 50% of the iris code as described is section 2.1.4. Since the inherent error correction capabilities cannot be altered, we suggest zero padding, in which zeros are uniformly distributed in the iris code. This does not affect the total amount of errors, but decreases the amount of errors per block and hence improves the overall error correction capabilities of the Hadamard code. We also integrate an iris shuffling algorithm [76] to introduce revocability as well as increase seperability between genuine and imposter distributions. The proposed algorithm is shown in Figure 27.

First, a user-specific key is encoded using concatenated Reed-Solomon and Hadamard encoding. This gives a pseudo-code that is then XORed with the shuffled, zero-padded sample iris code to produce the locked iris code. At the time of authentication, a shuffled,

zero-padded sample iris code is XORed with the locked iris code, and again, concatenated Hadamard and Reed-Solomon decoding is performed to obtain the user specific key. In this scheme shuffling is used to introduce revocability, Reed Solomon and Hadamard encoding are used to account for intra-user variability.

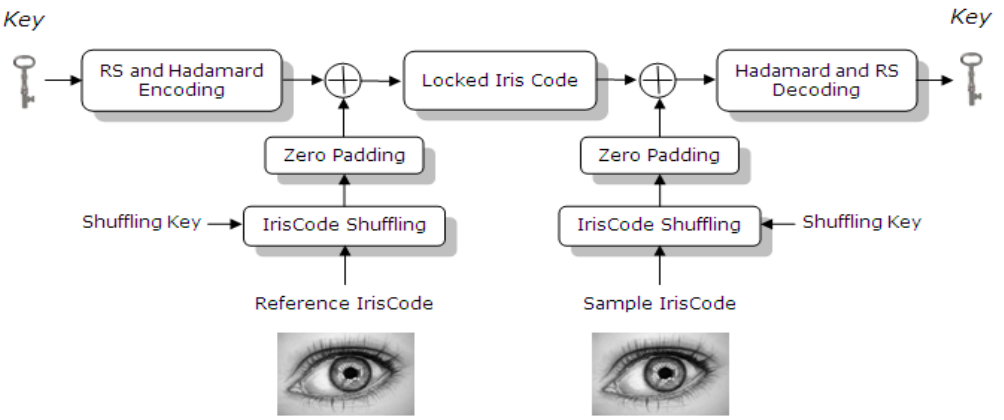

Figure 26 Block diagram of the proposed key-binding algorithm

3.3.1 Revocability

One of the main objectives of an iris template protection scheme is to provide revocability to the iris template, so that the original template is never stored and in case of the database being compromised a new set of iris template can be issued.

Caution must be taken though as to maintain the "uniqueness" of the template. In our scheme we use the iris shuffling algorithm shown in Figure 14 that not only maintains uniqueness, but actually improves the separability between the genuine and imposter hamming distance distributions as shown in Figure 19.

3.3.2 Performance

In our design and implementation we first needed to study the effects of the different parameters in our error correction scheme. In our experiments we used a 2048 bit iris

code. The following table summarizes the results of our experiments, where m refers to the message length in bits that is then encoded using a $2^{(m-1)}$ Hadamard matrix. The Reed-Solomon code outputs n blocks for an input of (n-2t) blocks, where t is the number of error blocks that can be corrected by the Reed-Solomon encoding. Each block contains m bits. The key length is calculated as m (n-2t).

Finally, c and r are used in the zero-padding algorithm, where every c bits in the iris code are followed by r zeros. This is achieved by segmenting the iris template into c-bit blocks and inserting r zeros after each block. This will decrease the errors in each block and hence enhance the error correction ability of the Hadamard code.

						FAR	FRR
No ECC (Before Shuffling)						0.0008	0.0035
No ECC (After Shuffling)						0.000007	0.0016
Error Correction Coding							
m	n	t	c	r	key		
7	32	7	4	0	126	0	0.0074
7	32	9	4	0	98	0	0.0069
7	32	11	4	0	70	0	0.0063
7	32	13	4	0	42	0	0.0053
7	32	15	4	0	14	0	0.0040
7	56	7	4	3	294	0	0.0033
7	56	9	4	3	266	0	0.0021
7	56	11	4	3	238	0	0.0013
7	56	13	4	3	210	0	0.0007
7	56	15	4	3	182	0	0.00055

Table 2 Results of the iris recognition system before and after error correction coding

From Table 2 we can see that there is a tradeoff between key length and recognition performance of the proposed system. While False Acceptance Rate (FAR) remains zero for all tested parameters there is a light decrease in False Rejection Rate (FRR) as we increase the error correction capabilities of the code by increasing t.

3.3.3 Cyclic Redundancy Check Module

Bio-cryptosystems like the one described above where always designed as a means to solve key management issues and hence all the systems in the literature are designed on the basic idea of recovering a key using biometric information. When the main objective is to protect the biometric template recovering the key does not become a priority anymore.

More importantly, storing the key for comparison becomes an unnecessary requirement for a biometric based authentication system. This led us to modifying biometric crypto system suggested by Hao et al [48] to use CRC to eliminate the need for key storage and key comparison [39].

CRC is usually used to detect errors occurring in transferred digital messages through noisy communication channels. The CRC check bits are obtained by a similar approach as polynomial long division and the remainder is the result. Thus every CRC code is specified by a polynomial that determines the width of the check bits and is chosen to detect specific errors.

To incorporate this idea into the existing key-binding algorithm shown in Figure 24, first the CRC check bits are calculated for the user specific key and then appended to the key to form an extended key.

The key is then encoded using concatenated Reed-Solomon and Hadamard encoding. This gives a pseudo-code that is then XORed with the shuffled sample iris code to produce the locked iris code as shown in Figure 25.

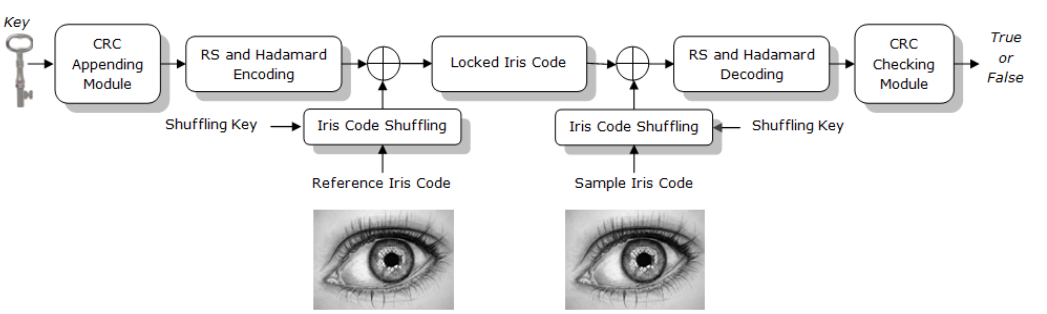

Figure 27 Block diagram of the proposed key-binding algorithm with CRC module

At the time of authentication, a shuffled sample iris code is XORed with the locked iris code, and again, concatenated Hadamard and Reed-Solomon decoding is performed to obtain the extended user-specific key as shown in Figure 25.

CRC decoding then determines if the recovered user-specific key has errors or no. If no errors are detected the sample iris code is verified as authentic. Zero-padding was omitted just to better understand the effect the CRC module had on the performance of the system.

For our implementation we chose to experiment with the following parameters: m=7, n=32, t=10 for a total extended key length of 84, because it is large enough, yet the performance of the biometric system is very well above performance requirements of most practical systems with 0% FAR and a 0.07% FRR.

We have also chosen CRC polynomials of different degrees already used in the industry standards. The polynomial is represented as its hexadecimal representation of the coefficients of the polynomial. The performance rates show almost no change in the FRR but a slight improvement in FAR and overall no decrease in performance after substituting key matching with our CRC module.

It is also to be noted that with increasing the size of the check bits the actual user key is shortened by the same amount to yield a total key of m*(n-2*t) = 84 bits. This means that the CRC of length c bits, the user specific key will be k=84-c.

	Polynomial	FAR	FRR
CRC8 (CCITT) [86]	0x07	0.0037	0.0067
CRC16 (CCITT) [86]	0x1021	0.00001	0.0067
CRC24 (FlexRay) [87]	0x5D6DCB	0	0.0066
CRC32 (IEEE 802.3) [88]	0x04C11DB7	0	0.0066

Table 3 Results of the iris recognition system before and after error correction coding with different parameters.

3.3.4 Security Analysis

In our proposed scheme we used 2 layers of security for the iris templates. First, a 128-bit shuffling key is used to ensure revocability. Second, an 84-bit key is used in the error correction module to conceal the iris code.

For an attacker to guess the cryptographic key by providing a 2048-bit iris code, we consider the worst case scenario, where the attacker has knowledge of the correlations that exist in the iris code. An 2048 iris code has 249 degrees of freedom [43] and hence only 249 bits are uncertain. The Hadamard code is capable of correcting 15 bits out of 64 bits (~25%). This means that the attacker needs to find a 249-bit string within P=58 bits hamming distance of the key. By the sphere-packing bound similar to the approach to Hao et al.[48]

$$\text{Entropy} \approx \log_2 \frac{2^N}{\frac{N!}{P!\,(N-P)!}} \approx 58 \text{ bits} \qquad 3.1$$

This is more than the 44 bits calculated for Hao et al.'s suggested bio-cryptosystem [48]. This means that the overall key is 58+128+84= 186 bits.

3.3.5 Discussion

With the increased use of biometric systems, the possibility of attacks on the template database also increases. As we can see from the results in the Table 2, in the error correction module there is a tradeoff between key length and performance of the system. We chose to use the 84-bit key-length, because it is large enough, yet the performance of the biometric system is very well above performance requirements of most practical systems with 0% FAR and a 0.07% FRR.

We also suggested the use of an iris shuffling algorithm to introduce revocability and the proposed algorithm actually increased separability between genuine and imposter distributions.

The introduction of the cyclic redundancy check module eliminates the need to store the user specific key used in the error correction module and hence simplifies the database and therefore decreases vulnerabilities of the database, even if the shuffling key is compromised and even if a sample iris code is spoofed. Thus the system increases security while maintaining performance rates as well as ensures revocability and the suggested CRC module can easily be integrated in already established systems without any need for redesigning the whole system.

In our implementation we only experimented with already existing CRC polynomials of different degrees. This enabled a better understanding of the effect of the polynomial length on the performance of the iris-based biometric authentication system. All of these polynomials were developed to detect specific errors common in communication systems. To achieve better results with the proposed system CRC polynomials need to be developed that are designed to correct the specific errors present in iris codes. This will ensure a better performance and has to be studied further in future research.

3.4 Proposed Fuzzy Vault System

The fuzzy vault, as we have mentioned before, is one of the most researched algorithms when it comes to template protection. An illustrative diagram that explains the fuzzy vault is shown in Figure 28. While the fuzzy vault scheme has been very successful when implemented with fingerprints and face features, there are two main issues when implementing a fuzzy vault for iris templates.

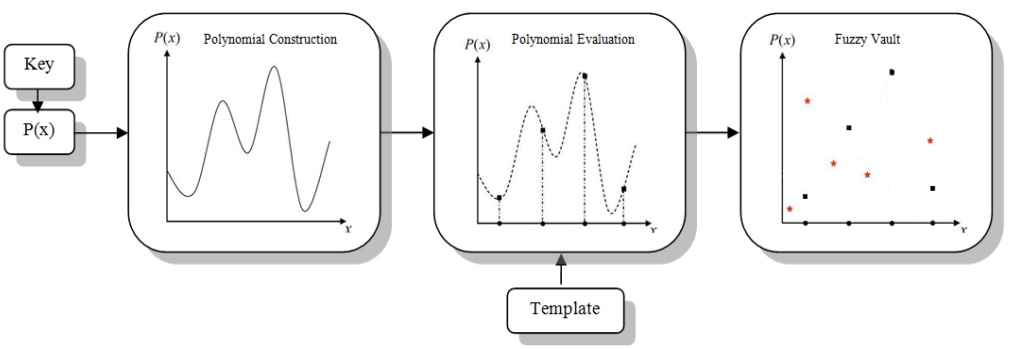

Figure 28 Fuzzy vault scheme

First, the fuzzy vault scheme requires an unordered set [63] and second, the iris templates are usually stored and matched using a binary form. This is why most of the research in literature resorts to finding new algorithms for extracting the features from the iris texture that would be "unique" enough for authentication. At the same time, Daugman's [41] binary template model has been well studied and implemented on a very large scale with success.

In our research we again build our system, based on Daugman's [41] iris recognition model and offer security for binary iris templates already in use in those systems.

In the final decoding stage of iris recognition, the phase of the Gabor coefficients are quantized according to which quadrant the phase falls in, as shown in Figure 29. Instead of the two bits representing each quadrant, we propose using their decimal equivalent and adding one for convenience. This allows us to use the modified fuzzy vault, in which 5 columns representing the 4 quadrants and a fifth representing masked bits, can be implemented. Masked bits are represented by a 0. This gives us a 1024-element feature vector that we can use in our fuzzy vault implementation [38] as shown in Figure 30.

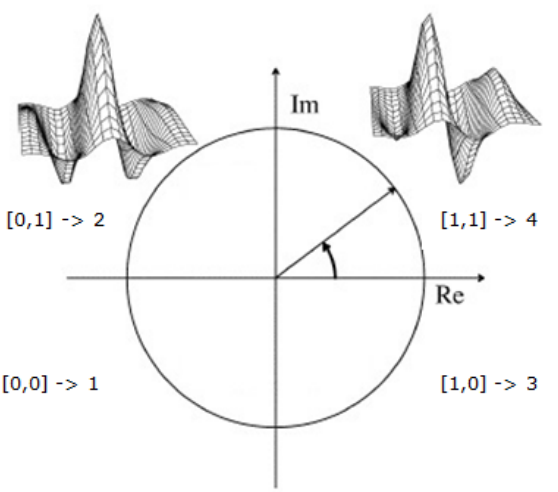

Figure 29 Proposed decoding scheme (adapted from [41])

A modified fuzzy vault [83] substitutes the polynomial in the fuzzy vault scheme by positions in a look-up table or grid. Instead of the unordered set, ordered set can use their indices as abscissa, which enables us to use our iris feature vector for constructing the modified fuzzy vault.

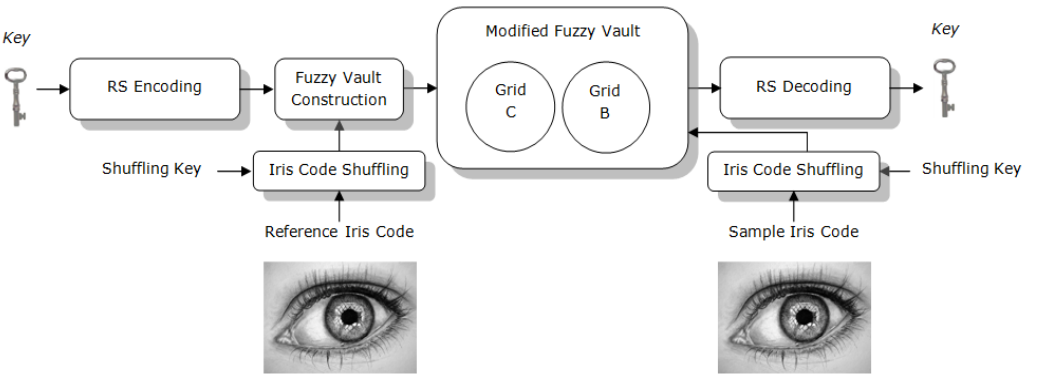

Figure 30 Block diagram of the proposed fuzzy vault implementation

First, the user specific key is encoded using Reed-Solomon encoding algorithm. Then a 1024x5 Grid C is created by putting RS code elements in the grid while maintaining the row and randomly choosing the column. The rest of the Grid is randomly assigned numbers in the appropriate range to conceal the real RS code. An illustrative example is shown in Figure 31.

In the next step the mask is applied to the feature vector, such that all masked bits become 0. Then another 1024X5 Grid B is created and the masked iris feature vector is put in the same position as the equivalent RS code element. The rest of the Grid is formed such that each row is a shifted version of the number sequence (1 2 3 4 0), as shown in Figure 31. This way the masked iris feature vector and the corresponding RS codes have the exact same positions in both grids. This is the key for the decoding process. The values of RS codes are hidden with the randomly assigned values in the rest of the grid. These are the equivalent to the chaff points in the classic fuzzy vault scheme. In Grid B since the values range from 0 to 4, the iris feature value is concealed by placing all the values in this range in the same order for each row. The 2 Grids B and C form the fuzzy vault.

During decryption, the masked iris feature vector is evaluated and using Grid B as alook-up-table the corresponding positions for each value are determined. These exact same positions are then used in Grid C to find the corresponding RS values. These are in turn decoded using Reed Solomon decoding to obtain the key. Positive match occurs if the decoded key is matched to the stored user specific key.

To account for rotations of iris images during acquisition, the feature vector is shifted by 3 elements in each direction and for each shifted iris code an attempt to retrieve the key is performed. Matching occurs if the decoded key in any of the shifted versions matches the stored user specific key.

An illustrative example of both the encoding and decoding process is shown in Figure 31.

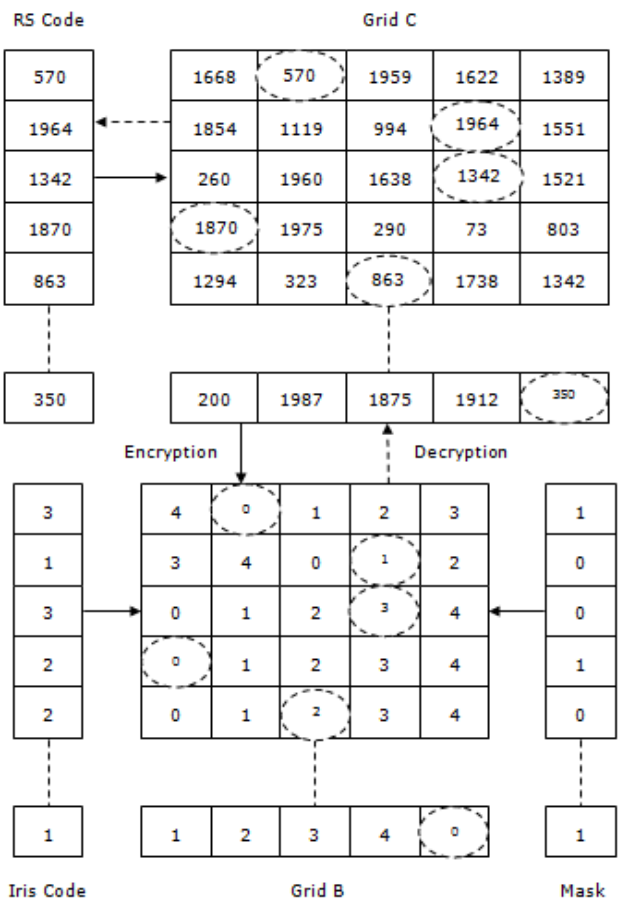

Figure 31 An illustrative example of the proposed modified fuzzy vault

3.4.1 Parameter Values

In this section we discuss our choice of parameters for the proposed fuzzy vault. For the iris template creation part we chose to keep the parameters that Daugman's [41] used so we can maintain the 2048 bit iris template. After our proposed coding algorithm we obtain a 1024-element feature vector as well as a 1024-bit mask. Masked elements are set to 0 and this is why we chose a 5 column grid for our fuzzy vault; 4 quadrants and an extra column for masked features. For the Reed-Solomon (n,k,t) error correction coding we used n to be 1024 so that we can obtain a code of the same length as our iris feature vector. The tolerance t of the code, which refers to the error correcting ability of the code, was chosen as 350, i.e. the code was able to correct 350 out of the 1024 elements of the code. This number was chosen from figure 4 so as to correct up to 35% of the code. This results in a key, k, that is equal to (n-2t), i.e. 324.

3.4.2 Revocability

Again in this scheme we used the iris shuffling algorithm as shown in Figure 14. In this scheme, the iris code is divided into 128 blocks. A 128-bit user-specific key is then used to shuffle the iris code. All blocks corresponding to 1's are placed first, followed by the rest of the blocks corresponding to 0's. This shuffling algorithm not only maintains uniqueness, but actually improves the separability between the genuine and imposter hamming distance distributions as shown in Figure 18.

3.4.3 Privacy

In our proposed scheme, privacy is achieved by filling both grids with elements that are of no significance to the authentication process. Elements in Grid C are randomly chosen to be in the same range as the calculated RS codes, so that it becomes impossible to guess the genuine RS codes from the randomly generated ones. In Grid B all rows are the shifted version of the same vector, again, making it impossible to guess the genuine from the rest of the grid.

3.4.4 Performance

The performance of the proposed system was evaluated by determining the False Accept Rate (FAR) and False Reject Rate (FRR). FAR refers to the number of correct key retrievals from non-genuine users in the system. FRR refers to the number of rejections for genuine users in the system.

m	n	t	key	FAR	FRR
11	1024	350	324	0	0.0092
7	64	24	256	0	0.0093
7	64	20	384	0	0.0092
7	64	16	512	0	0.0092
7	64	8	768	0	0.0091

Table 4 Performance of the proposed fuzzy vault.

3.4.5 Security Analysis

In our proposed scheme we used 2 layers of security for the iris templates. First, the 128-bit shuffling key used to ensure revocability. Second, a key used to obtain the Reed Solomon (RS) codes used in the modified fuzzy vault construction.

For an attacker to guess the cryptographic key he has to provide a 1024 iris code and guess it`s position in one of the 5 possibilities in Grid B. Hence the information bits are N=128. The Reed-Solomon code is capable of correcting 324 out of 1024 elements (~32%). This means that the system is capable of correcting P=40 error bits. Following a similar approach to Equation 3.1:

$$Entropy \approx log_2 \frac{2^N}{\frac{N!}{P!\,(N-P)!}} \approx 17\ bits \qquad 3.2$$

The overall key is hence 128+17=145 bits more than the acceptable 128 bit keys used for Advanced Encryption Standard (AES).

3.4.6 Discussion

As we can see from the results in the Table 4, there is a tradeoff between key length and performance of the system. We also suggested the use of an iris shuffling algorithm to introduce revocability and the proposed algorithm actually increased separability between genuine and imposter distributions. The proposed system uses 2 user specific keys, one for the shuffling algorithm (128 bit) and another for the Reed-Solomon encoding algorithm, which ensures entropy for revocability and security of the system.

The proposed fuzzy vault system achieves the goals set for template security by providing revocability, privacy and security while maintaining a performance acceptable for public deployment.

Because the proposed fuzzy vault system is designed to use binary iris templates, it achieves another important goal by enabling the proposed system to be appended to already existing iris based authentication systems using binary iris templates without the need to redesign the whole system.

Chapter 4 Watermarking

Watermarking is the art of embedding or hiding critical data into unsuspected multimedia content, so that it's imperceptible for humans and hence doesn't affect the quality of the multimedia content [2].

In general, a watermarking system consists of an *embedder* and a *detector*, as illustrated in Figure 29. In the embedding process the original cover work and a watermark enter the system together with an optional key to give the watermarked work. The output of the watermark embedder is typically transmitted or recorded. Later, that work is presented as an input to the watermark detector. Most detectors try to determine whether a watermark is present or not, and if a watermark is detected, output the message encoded by it.

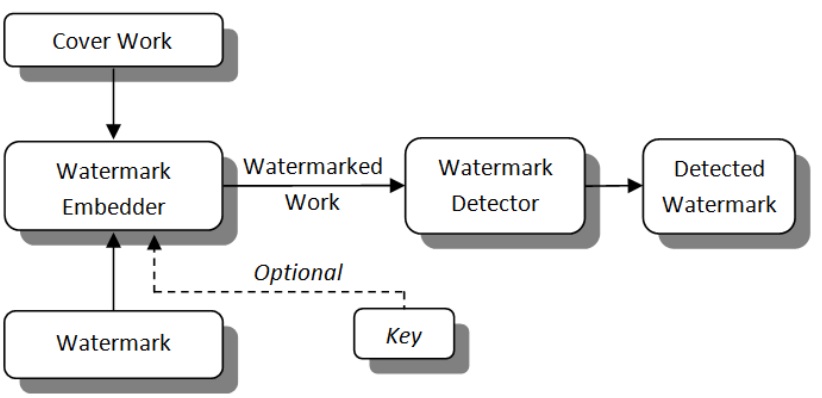

Figure 32 A generic watermarking system [19]

Watermarking is distinguished by two important characteristics [19]: one, watermarks do not detract from the aesthetics of the media; second, watermarks are inseparable from the works in which they are embedded. They do not get removed when the work is displayed or converted to another format, remaining with the content in digital and printed form and are still detectable when for example an image is printed and then scanned back into a computer [19].

Watermarking systems can be designed to use keys in an analogous manner to encryption. The key is used to cast, detect and remove a watermark [21]. The idea is to make it impossible to detect the presence of a watermark in a work without knowledge of the key, even if the watermarking algorithm is known. Further, by restricting the access to the key, it is extremely difficult, if not impossible, for attackers to remove the watermark without causing significant degradation in the fidelity of the cover work.

There are many watermarking techniques according to application area and purpose and they have different insertion and extraction methods. They can be categorized according to many criteria as follows [20]:

- *According to Inserted Media:* The inserted watermark could be in form of *text* with special font, inter-character spacing and line spacing. It could also be an *image* or *video* with special information or it can be an *audio* watermark.

- *According to Perceptibility:* The watermark could be *visible* (in case of text, image and video watermarking) or audible (in case of audio watermarking), but it can also be *invisible* or inaudible. *Visible* watermarks are designed to be easily perceived by the viewer, and clearly identify the owner. However, the watermark must not detract from the media content itself and most research currently focuses on *invisible* watermarks, which are imperceptible under normal conditions.

- *According to Robustness:* A watermark may be *fragile*, *semi-fragile* or *robust*. Fragile watermarks are designed to be distorted or "broken" under the slightest changes to the work. Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold. (A threshold of zero would form a fragile watermark.) Robust watermarks withstand moderate to severe signal processing attacks (compression, rescaling, etc…).

- *According to Inserting Watermark Type:* Inserting watermark types can be *noise* (Pseudorandom noise sequence, Gaussian random sequence, Chaotic sequence, etc…) or *image* (Binary image, stamp, logo or label).

- *According to Processing Method:* Watermark processing methods could be done in the spatial or frequency domain. *Spatial watermarks* are constructed in the media spatial domain, and embedded directly into the sampled data. This could be done by hiding data in a fixed number of LSBs of a sample or manipulating the value of some chosen patches of points. *Spectral* (or transform-based) *watermarks* are incorporated into the transform coefficients (DCT, Wavelet). It could be a random function generated by a known (key) seed, by a lookup table, or by spread spectrum or hopping spread spectrum.

- *According to Necessary Data for Extraction:* Watermark extraction methods can be *blind* or *informed* watermarking according to the necessity of an original media. *Blind* watermarking techniques can perform verification of the mark without use of the original data. Other techniques rely on the original to detect the watermark. Many applications require blind schemes; these techniques are often less robust than informed algorithms.

4.1 Watermarking Security

The security of a watermark refers to its ability to resist hostile attacks. A hostile attack is any process intended to hinder the watermarking's purpose. The attacks can be divided into 3 categories [20]:

I. *Unauthorized removal* (active attack, modifies the cover work) - refers to attacks that prevent a work's watermark from being detected. There are three forms of unauthorized removal:

   ~ *Elimination attacks* – means that an attacked work cannot be considered to contain a watermark at all

   ~ *Masking attacks* – means that an attacked work is still watermarked, but the mark is undetectable by existing detectors

~ *Collusion attacks* – the attacker obtains several copies of a given work, each with a different watermark, and combines them to produce a copy without a watermark.

II. *Unauthorized embedding* (active attack, modifies the cover work) – refers to acts that embed illegitimate watermarks into works that should not contain them. This process can lead to the detector to falsely authenticate an invalid work.

III. *Unauthorized detection* (passive attack, does not modify the cover work) – there are 3 levels of severity:

~ The attacker detects and deciphers the embedded message

~ The attacker detects the watermarks, can distinguish one mark from another, but cannot decipher the message

~ The attacker detects the watermarks, but is neither able to decipher the message nor to distinguish between embedded messages.

There are basically three prototypes of possible attacker [19]:

~ *The private pirate* – is the prototype of the most naïve user of multimedia services. He basically wants a copy of a content for his own use or that of his close friends. He is usually not qualified and does not use powerful technologies.

~ *The professional pirate* – intent to make a commercial profit from the counterfeit. He may invest in powerful technologies and has qualified competencies to break the watermarks.

~ *The private hacker* – computer scientist who is looking for a technical challenge. He is extremely well qualified and may use very powerful techniques. He is not interested in any financial benefit, and only looks for the widest recognition.

4.2 Watermarking for template protection

Although watermarking algorithms were first developed to protect multimedia from illegal use, or sharing, it has recently emerged as one of the ways to protect biometric templates. Besides offering secure transmission and storage of biometric templates, it also provides a means for proving ownership by using a specific cover for every organization and/or application. If the biometric template is "hidden" within another biometric representation, it also offers a way for multimodal biometric authentication as well as template protection.

In recent years there has been some attempts to protect biometric templates by watermarking them, so as to detect any tampering with the original template [29]. And several attempts even used one type of template to watermark another template [30][31][32][33][34][35], which provides multimodal authentication, as well as, template protection. Most of these efforts focused on fingerprint and face templates.

4.2.1 Space Domain

Embedding watermarks in the space domain involves the manipulation of the least significant bits of the multimedia content [19]. The pseudo-random number traversing method or a spread spectrum method can be used together with a key to disperse its spatial locations. The permuted watermark can then be convolved with the content after applying a weighting factor that ensures robustness of the watermark as well as imperceptibility.

Space domain watermarking, although simple to implement and usually involving minimal computational complexity, its robustness against many attacks like compression, blurring, cropping, etc... is minimal, too. Spatial watermarking also does not exploit the properties of the cover image, which can significantly help the robustness of the watermark. That's why, in practical applications it's very rare to find spatial watermarking applied solely in a watermarking scheme for template protection.

One of those efforts to hide binary iris template using spatial watermarking of a face image is described in [22], in which the iris template is hidden as a bit stream in the least

significant bit of pixels in a face image according to the amplitude modulation based technique [23]. A key is used to determine the location the start of watermark embedding in the host image, as well as determining a reference bit in the iris template. All rows in the template are then connected end-to end to form a roll. Starting from the reference bit all bits are then embedded into the host image. Although this approach provides diversity, revocability and some security, performance of the proposed method was not tested against any watermarking attacks, which the method most probably won't survive.

4.2.2 Transform Domain

Watermarking in the transform domain exploits properties of the cover image and the human visual system to improve robustness of embedded watermarks. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions, because degradation in smoother regions of an image is more noticeable to the human visual system, and is a prime target for lossy compression schemes. The classic domain for image processing is that of the Discrete-Cosine-Transform, or DCT. Using the DCT an image can easily be split up in pseudo frequency bands, so that the watermark can conveniently be embedded in the most important middle band frequencies.

Furthermore, the sensitivity of the human visual system to the DCT basis images has been extensively studied, which resulted in the recommended JPEG quantization table [24]. These results can be used for predicting and minimizing the visual impact of the distortion caused by the watermark. Finally, the DCT block-based DCT is widely used for image and video compression. By embedding a watermark in the same domain as the compression scheme we can anticipate which DCT coefficients are more likely to be discarded during compression[24].

Another possible transform for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition.

One of the many advantages of the wavelet transform is that it is believed to more accurately model aspects of the HVS (Human Visual System) as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive, such as the high-resolution detail bands (LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [24].

The performance of a watermarking algorithm, in general, is computed based on measures such as peak signal-to-noise ratio, mean square error, normalized cross correlation, and histogram similarity. However, for a biometric watermarking algorithm, the most important performance metric is the recognition accuracy.

An example of how transform domain watermarking can exploit image properties to embed a more robust watermark is shown in [27]. The authors chose to use the FFT (Fast Fourier Transform) for use on segmented normalized iris (watermark) and normalized face image (cover work). The authors noted that iris recognition relies on the high frequency fine texture present in the iris patterns, and face recognition, on the other hand, relies on "low frequency" eigen-features. The authors hence chose to embed mid- and high frequency components of iris texture patterns into the face image, and because these bands had little effect on face recognition, more robust watermarking was possible. The proposed algorithm showed little degradation in recognition performance after blurring, cropping, rotation and addition of Gaussian noise.

Another example of transform domain watermarking is suggested in [28], where a binary iris template is used to watermark a face image using a modified correlation algorithm as well as a modified 2D Discrete Cosine Transform. The experimental results show that both watermarking algorithms are robust against filtering, noise addition and jpeg compression without significant degradation in the recognition accuracy.

In [29], the authors compared 4 watermarking techniques to embed an iris template into a face cover image. The four techniques are LSB substitution, Modified Correlation Based Algorithm (MCBA), Modified 2D DCT (M2DCT), and DWT. Robustness of all four algorithm was tested against Jpeg compression, Gaussian noise addition, median filtering, blurring, gamma correction, file format conversion, and printing and rescanning of the watermarked image. As in all other biometric watermarking robustness is measured by

the recognition accuracy. In their experiments transform domain watermarking as expected performed better in withstanding different types of attacks, with DWT performing best in most cases, followed by the M2DCT and then MCBA. LSB substitution again, as expected, performed worst especially after Jpeg compression where the watermark was completely lost.

In [25] another watermarking algorithm is implemented. The authors chose to study the effect of watermarking using QIM algorithm on iris recognition. Quantization Index Modulation (QIM) refers to the use of a set of m quantizers, where m is the possible values of the watermark [26]. They studied the 2 cases of iris watermarking; the first when the iris template is the watermark and the other when the iris image is the cover work. They applied 11 different watermarking attacks that include scaling, low pass filtering, median filtering, cropping, Gaussian noise addition, and Jpeg compression. They concluded that when the iris image is the cover work there is no significant drop in recognition accuracy. However, when the iris template is the watermark, the iris recognition‘s accuracy is proportional to the robustness of the watermarking algorithm against the different types of attacks, but the degradation is still low compared to the benefits of securing and protecting the templates.

4.3 Proposed Watermarking Scheme

Discrete Wavelet Transform (DWT) is another popular domain for image watermarking, because DWT preserves frequency information in stable form and allows good localization both in spatial and frequency domain [89]. In this scheme we propose the combination of the traditional DWT and LSB substitution algorithm to achieve robustness against both geometric and frequency watermarking attacks [36].

4.3.1 Revocability

Again in this scheme we used the iris shuffling algorithm as shown in Figure 14. In this scheme, the iris code is divided into 128 blocks. A 128-bit user-specific key is then used

to shuffle the iris code. All blocks corresponding to 1's are placed first, followed by the rest of the blocks corresponding to 0's. This shuffling algorithm not only maintains uniqueness, but actually improves the separability between the genuine and imposter hamming distance distributions as shown in Figure 18.

4.3.2 Privacy

Figure 35 shows the watermark embedding process and the steps for embedding the biometric watermark, which are as follows:

Step 1: Three-level Discrete Wavelet Transform (DWT) is applied to the original cover image I. Because the approximation band carries the most sensitive coefficients (to the human visual System) and the diagonal approximation band carries the least significant ones (most vulnerable to image processing attacks) [2], the coefficients of the vertical and horizontal band are chosen for watermark embedding. To provide more resilience to geometric and frequency attacks, the second and third levels of DWT are used for embedding.

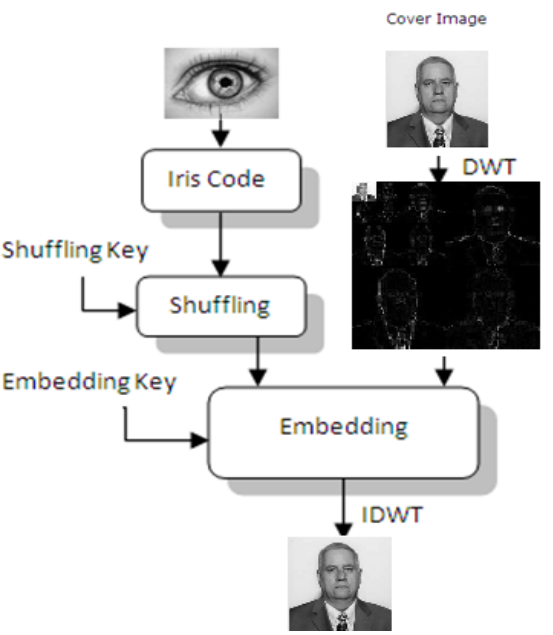

Figure 33 A general diagram for the proposed biometric watermark embedding algorithm

Step 2: In the detailed sub-bands p coefficients are chosen according to a user specific key. Since the watermark will be embedded in 4 sub-bands, p is ¼ of the watermark length. The watermark is embedded 5 times to increase robustness. After choosing the positions of the coefficients to be watermarked, they are adjusted according to the following equation:

$$LSB_5(Cw_{i,j})=W_n \quad 4.2$$

where Cwi,j is the watermarked coefficients, Wn the watermark bit at position n and LSB5 indicates the 5th least significant bit.

Step 3: After embedding, Inverse Discrete Wavelet Transform (IDWT) is applied to the watermarked coefficients to generate the secured watermarked cover image.

For authentication the watermark (iris template) needs to be recovered and since the watermarking algorithm is blind; i.e. we do not need the original coverwork to extract the embedded image, the steps for extracting the watermark are according to the following steps as shown in Figure 36:

Step 1: As in embedding, three-level DWT decomposition of the cover image I is performed to obtain the 2nd and 3rd level detail bands.

Step 2: The user specific key is used to determine the watermark embedding locations in the same manner as in the embedding process. From each coefficient a watermark is extracted from the 5th least significant bit of the coefficient.

Step 3: For each 5 bits of extracted watermark, majority decoding is used to determine the equivalent extracted watermark bit.

Step 4: The extracted bits are then arranged to form the iris template.

The extracted iris template is then matched with the sample iris template for authentication using the Hamming distance between both templates. If the distance is above a predefined threshold for the system, a mismatch is decided. And if the Hamming distance is below the predefine threshold a match is decided.

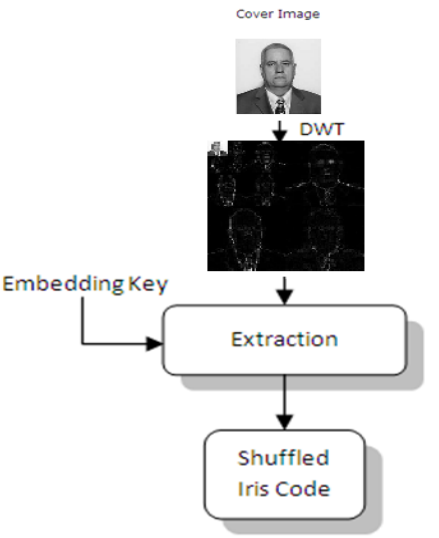

Figure 34 A Block diagram of the proposed biometric watermark extraction algorithm

4.3.3 Performance

Watermarking systems are usually evaluated as peak signal-to-noise ratio, mean square error, normalized cross correlation, and histogram similarity, but for biometric watermarking systems only recognition rates are of importance. The performance of the proposed biometric watermarking system is evaluated using an iris recognition system and the iris codes are matched according to the hamming distance between them as described in chapter 1.

The iris code embedded in the cover image may be vulnerable to low-level signal processing techniques such as compression, low-pass filtering or geometric distortions and may affect the robustness and integrity of the iris template. To evaluate the performance of the proposed biometric watermarking algorithm under these conditions, we perform selected frequency and geometry based attacks such as JPEG compression with 75% quality, Gaussian filtering with variance of 3 pixels, median filtering with 3x3 kernel, blurring using 3x3 kernel, rotation by 10 º and then reversing the rotation (-10 º) , and scaling with ratio of 110%.

		FAR	FRR
No Watermarking		0.0011	0.0128
Watermarking Attack			
	No Attack	0.0011	0.0128
	Jpeg Compression (Q=75%)	0.0007	0.0045
	Gaussian Filtering (var=3)	0.0021	0.0881
	Median Filtering (3x3)	0.0043	0.0370
	Blurring (3x3)	0.0019	0.0922
	Rotating (10º)	0.0025	0.0690
	Scaling (1.1)	0.0011	0.0922

Table 5 Results of the iris recognition system before and after watermarking, as well as after different geometric and frequency attacks.

4.3.4 Security Analysis

In our proposed scheme we used 2 layers of security for the iris templates to ensure the revocability and security of the templates. First, a 128-bit shuffling key is used to ensure revocability. And second, a watermark embedding key, a ($4*10^7$) key, is used as a seed for the random generator used to randomly select positions of the coefficients to be modified. The watermark is also embedded 5 times to increase robustness.

4.3.5 Discussion

Watermarking has recently been increasingly used for template protection. In this chapter we proposed a watermarking based iris template protection scheme that satisfies the four important goals of any template protection scheme.

First, we achieved revocability by implementing an iris shuffling scheme and the proposed algorithm actually increased separability between genuine and imposter distributions.

Second, privacy was established by hiding the iris template into some cover work, where the iris template is imperceptible and is robust to some frequency and geometric attacks. As we can see from the results in the Table 5, the watermarking scheme suggested does not affect the performance of the iris recognition system. Attacks on the watermarked image slightly affect the false acceptance rate and increase the false reject rate, but still within very acceptable limits that does not degrade the performance of the system.

Third, to ensure security, the proposed system uses 2 user specific keys, one for the shuffling algorithm (120 bit) and another for the watermark embedding algorithm ($4x10^7$) which ensures entropy for revocability and security of the system, even if the watermarking algorithm is known.

Chapter 5 Hybrid Iris Template Security Scheme

In this chapter, we propose a system that combines a key binding bio-cryptosystem using revocable iris codes with a watermarking algorithm. The proposed system has 3 layers of security, which decreases the chance of the database being compromised even if one of the keys is revealed. This algorithm is designed, like all other algorithms described in the rest of this thesis, to be appended to already existing binary iris-code based biometric recognition systems [43], that are well established and have proven reliable in large scale applications. The proposed algorithm combines the bio-cryptosystem and watermarking algorithm as well as the one-way transformation algorithm chosen to introduce revocability[37].

The combination of these methods aims to benefit from the strengths of each method, as well as complexity in trying to breach the security of the iris templates. The main criteria used in evaluating our system are the same criteria mentioned in Chapter 1; diversity, revocability and privacy while maintaining the performance of the iris-based authentication system.

5.1 Revocability

To ensure diversity and revocability of the iris templates, we chose to integrate the iris shuffling algorithm [75] shown in Figure 14. While this algorithm performs very similar to the permutation and shifting algorithm [85] shown in Figure 16, it is easier to implement and was hence chosen because it not only maintains uniqueness, but actually improves the separability between the genuine and imposter Hamming distance distributions as shown in Figure 18. The hamming distance refers to the bitwise difference between any two templates as a percentage of the total size of the template. For authentication purposes a threshold is chosen as to minimize false acceptance of imposters (False Acceptance Rate) as well as false rejection of genuine users (FRR).

5.2 Privacy

To ensure privacy of the iris templates we combined the biometric cryptosystem described in Chapter 3 with the watermarking algorithm [36] described in Chapter 4.

A user-specific key is hence is encoded using Reed Solomon and Hadamard encoding and is then XORed with a zero-padded shuffled iris code. The locked iris-code is then embedded in the cover image using another user-specific key using the same LSB-DWT algorithm described in Chapter 4. Figure 34 shows the general scheme of the proposed iris template protection algorithm.

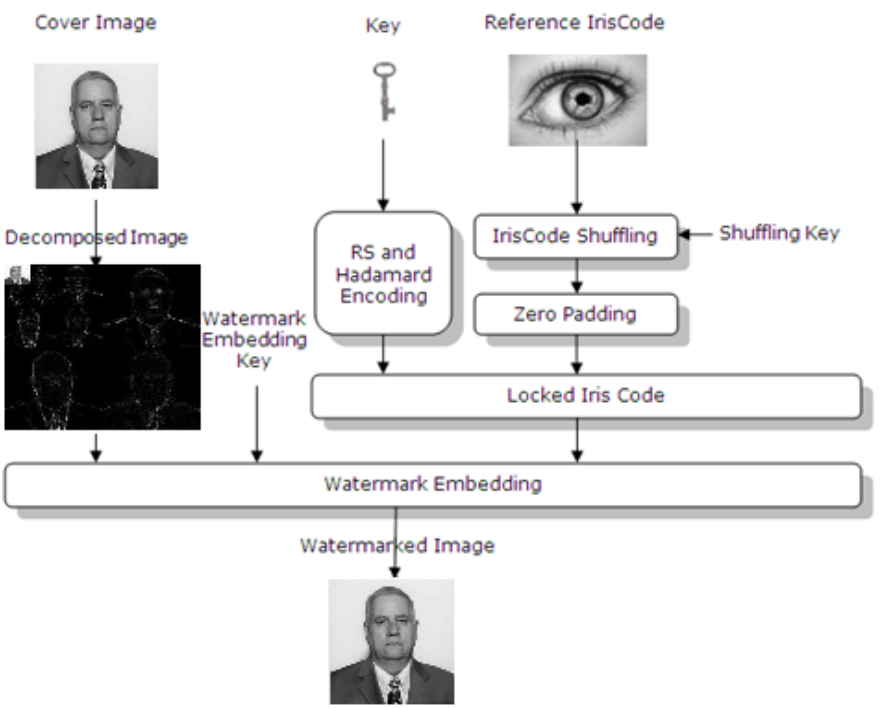

Figure 35 A block diagram of the proposed hybrid iris template protection encoding algorithm

For authentication, the locked iris code is recovered from the watermarked image using the user-specific key following the steps described in Section IV. The locked iris code is then XORed with zero-padded shuffled sample iris code, the result is then decoded using the Hadamard and Reed Solomon decoding algorithms to retrieve a key. Authentication

is established when the retrieved key is matched with the stored user-specific key. Figure 35 shows a general scheme of the proposed authentication scheme.

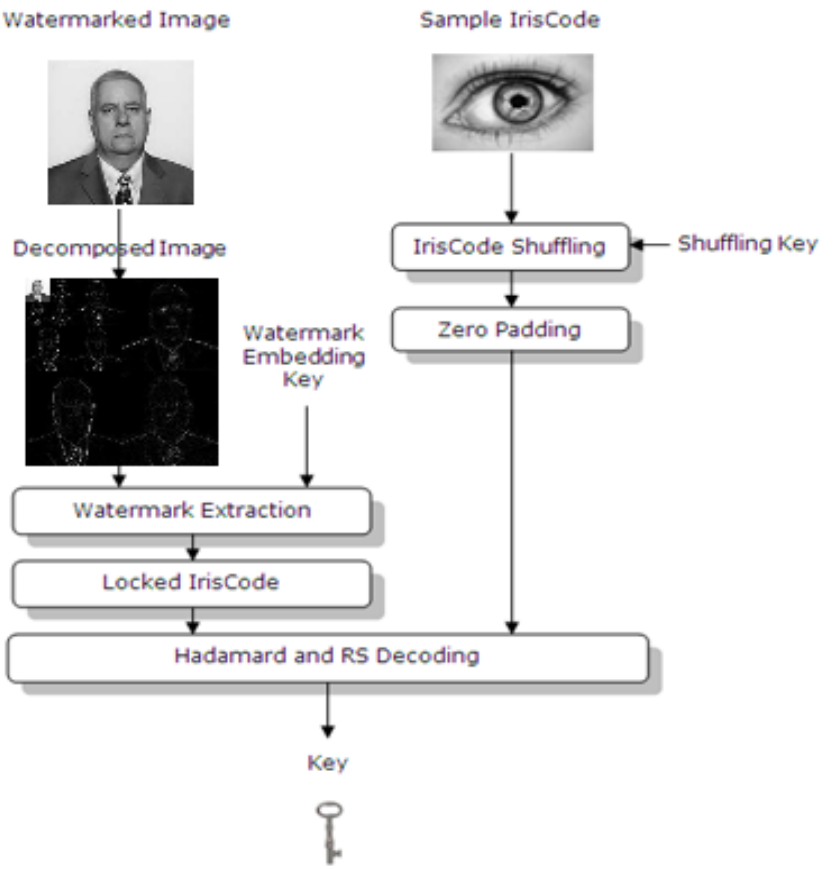

Figure 36 A block diagram of the proposed hybrid iris template protection decoding algorithm

5.3 Performance

The efficacy of the proposed algorithm is evaluated using the FAR and FRR of the overall system and comparing it to the original system. Selected frequency and geometry based attacks are, hence, performed on the stored watermarked images such as JPEG

compression with 75%, 50%, 25% quality, Gaussian filtering with variance of 3 pixels, median filtering with 2×1 kernel, blurring using 2×1 kernel, rotation of the image by 10º, and scaling with ratio of 110%. We chose the following parameters for the bio-cryptosystem module, where m=7, n=56, t=13, c=4 and r=3, which are associated with a 210-bit key. These parameters offer excellent performance and a key long enough to ensure security of the templates. Table III shows the results of the proposed system before and after the watermarking attacks.

	FAR	FRR
No Watermarking	0	0.0007
Watermarking Attack		
No Attack	0	0.0007
JPEG Compression (Quality=75%)	0	0.0020
JPEG Compression (Quality=50%)	0	0.0073
JPEG Compression (Quality=25%)	0	0.0091
Gaussian Filtering (variance=3)	0	0.0093
Median Filtering (2×1)	0	0.0092
Blurring (2×1)	0	0.0091
Rotating (10º)	0	0.0093
Scaling (1.1)	0	0.0093

Table 6 Results of the iris recognition system before and after combining one-way transformation, bio-cryptography and watermarking.

5.4 Security Analysis

In our proposed scheme we used 3 layers of security for the iris templates. First, a 128-bit shuffling key is used to ensure revocability. Second, a 210-bit key is used in the error correction module to conceal the iris code. And finally, a (4×10^7) key, used to randomly select positions of the coefficients to be modified in the watermark embedding algorithm.

For an attacker to guess the cryptographic key by providing a 3584-bit iris code, the actual information is N=256 bits. Because of the zero-padding, the Hadamard code in now capable of correcting 15 bits out of 36 or 37 information bits (~40%). This means that the system is capable of correcting P=107 error bits. Following a similar approach to Equation 3.2:

$$Entropy \approx log_2 \frac{2^N}{\frac{N!}{P!\,(N-P)!}} \approx 10\ bits \qquad 5.2$$

5.5 Discussion

With the increased use of biometric systems, the possibility of attacks on the template database also increases. From Table 4, we can see that there is a tradeoff between key length and performance. We chose to use the 210-bit key-length, because it is large enough, yet the performance of the biometric system is very well above performance requirements of most practical systems with 0% FAR and a 0.07% FRR. When comparing Table 6 (Hybrid System) with Table 5 (Watermarking) we can clearly see that the suggested combination of biometric cryptography and watermarking improves the performance of the iris-based recognition system and also adds another layer of security which makes it harder for an intruder to attack the template database.

Attacks on the watermarked image slightly affect the false acceptance rate and increase the false reject rate, but still within very acceptable limits that does not degrade the performance of the system. We also suggested the use of an iris shuffling algorithm that not only introduces revocability but actually increased separability between genuine

and imposter distributions. The proposed system uses 3 user specific keys, one for the shuffling algorithm (128 bit), a 210-bit key for the error correction module and another for the watermark embedding algorithm (4×10^7); these keys ensure revocability and security of the system, even if the watermarking algorithm is known.

The combination of the three iris template protection methods adds layers of security, which will make it hard for an attacker to breach the system. The proposed system meets the requirements for iris template security and can be implemented using already existing and established iris recognition systems using the Daugman iris-code model. This will make the transition to secure iris templates easier for developers and will promote public acceptance of iris based biometric systems.

Chapter 6 Haptic-biometric Template Protection

With recent advances in both the hardware and software for three dimensional applications, virtual environments are growing in popularity. Haptic devices offer a more immersed interaction between users and the virtual environments; and with the growing use of the internet to connect more users, arises the need to authenticate their identity in a secure manner. Identifying users by their interaction with haptic devices is an emerging research field that is proving promising, but like all biometric based authentications relies on the uniqueness of the stored template, which poses a risk if the template is compromised, because unlike passwords and pins, biometric templates are irrevocable. In this chapter we explore different ways to introduce revocability to biometric templates with haptic information which are used for user authentication.

Virtual environments have long exploited the visual and hearing senses of the users and recently haptic devices that offer tactile/force feedback have greatly enhanced the user experience in those virtual environments. Haptic devices also offer a means to authenticate users by their behavioral interaction with such devices [91] [92] in a similar way to keystroke dynamics [93] and two dimensional handwritten signatures [94]. These behavioral biometrics not only provide initial authentication like passwords, but they also provide continuous authentication throughout the duration of the interaction if desired.

In this chapter we present a key-binding biometric cryptosystem using online handwritten signatures with haptic information. The proposed system introduces 2 layers of security. First, a user specific key is used to "shuffle" the user signature template. This shuffling ensures revocability, so that a compromised template can be revoked and a different user specific key can be assigned or chosen to "shuffle" the same user template into a "new" template. The second layer of security is a different user specific key that is combined with the user template to produce a "locked" code, that doesn't reveal the original template nor the user specific key. These two layers of security decrease the chances of the database being compromised even if one of the keys or one of the algorithms is known.

6.1 Related Work

Biometric authentication using human interaction with haptic devices is an emerging field still in its infancy. It was first developed in a maze application that observed users interaction using a haptic device. Hidden Markov Model was used to capture the users individual characteristics [95]. Later, Artificial Neural Networks were used to identify users in a graphical password application [96]. In [91] the relative entropy of the different haptic features were analyzed in a virtual check application and it was concluded that haptic interfaces were more suited for verification applications. Further research found that haptic information can be used for identification as well as verification purposes [92].

Since this field is fairly new most of the research was focused on trying to find the best methodology for measuring and comparing haptic features for authentication purposes. The idea of providing secure templates is new to this field, but it is essential to try to integrate security of the templates within the design of such systems in order to promote future use and acceptability of such systems without compromising the user's privacy and security. This chapter is, hence, our attempt to introduce a secure biometric authentication system based on handwritten signatures using a haptic device.

6.2 Proposed System

The experimental setup provides a virtual environment where users can write their signature on a virtual plate as shown in Figure 1. The users grab and move the end-effector of the haptic device as a pen and its 3-dimensional position is mapped to a cursor in the virtual environment. When the cursor collides against a white rectangular virtual plate, the users can feel the repulsive force based on the penalty method and red dots are drawn on the collision position. A Phantom OMNI haptic device, which can measure 3-dimensional position and orientation of the end-effector, is used as the haptic device [92].

The 3-dimensional position (p), force (f), velocity (v), angular rotation (a) and timestamp (t) of the virtual pen-tip were measured. A simple state element can be

represented as s $\{p_x , p_y , p_z , f_x , f_y , f_z , v_x , v_y , v_z , a_x , a_y , a_z , t\}$ where subscript x, y, and z represent spatial dimensions.

We calculate the average and the standard deviation for the position, force, velocity and acceleration. This gives us 25 features at each time stamp.

Figure 37 Experiment setup

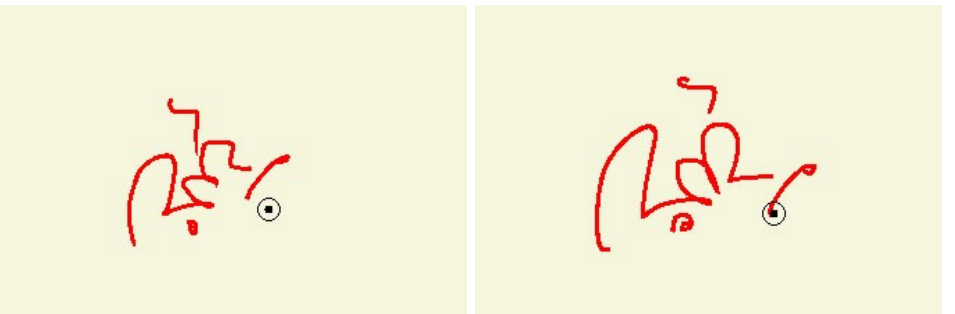

Figure 38 Sample snapshots of signatures from the same user [92]

The dataset used to test our system is proprietary and includes 16 volunteers between the ages of 25 to 35, two of which are females and 14 males. Each user gave 12 signatures after enough time was given for each user to familiarize themselves with the setup.

6.2.1 Revocability

Each user templates consists of a matrix of 25 columns representing the different measured features and a variable row length that depends on the time the user takes to sign the virtual pad. To introduce revocability we suggest a shuffling of the columns and hence the features using a user specific key. If the template is compromised a different key is assigned or chosen to cause a different permutation of the features.

During enrollment, the signature features are preprocessed. During this stage the variable length signature is resampled to a fixed length signature. Then the features are all normalized to the interval [-1,1] in order for a more uniform quantization and transform into a binary string. This step is essential since the range for each feature varies significantly depending on the feature measured. The signature is then divided into 10 equal segments and shuffled according to a user specific key. The key is used as a seed for the random generator used in the shuffling algorithm. After shuffling the signature is the quantized into 127 levels and converted into a binary string.

The signature is divided into n segments whose order is in turn permuted. The segments' length was chosen to be large enough to maintain user uniqueness, yet small enough to allow for good shuffling. In our experiments we used a user specific key to permutate the order of the features in the signature template. Figure 4 below shows the Hamming distance distributions of the preprocessed haptic signatures before and after the shuffling algorithm. It is clear that the algorithm, not only maintains user uniqueness, it actually improves the performance of the authentication system by increasing the seperability between genuine and imposter hamming distance distributions.

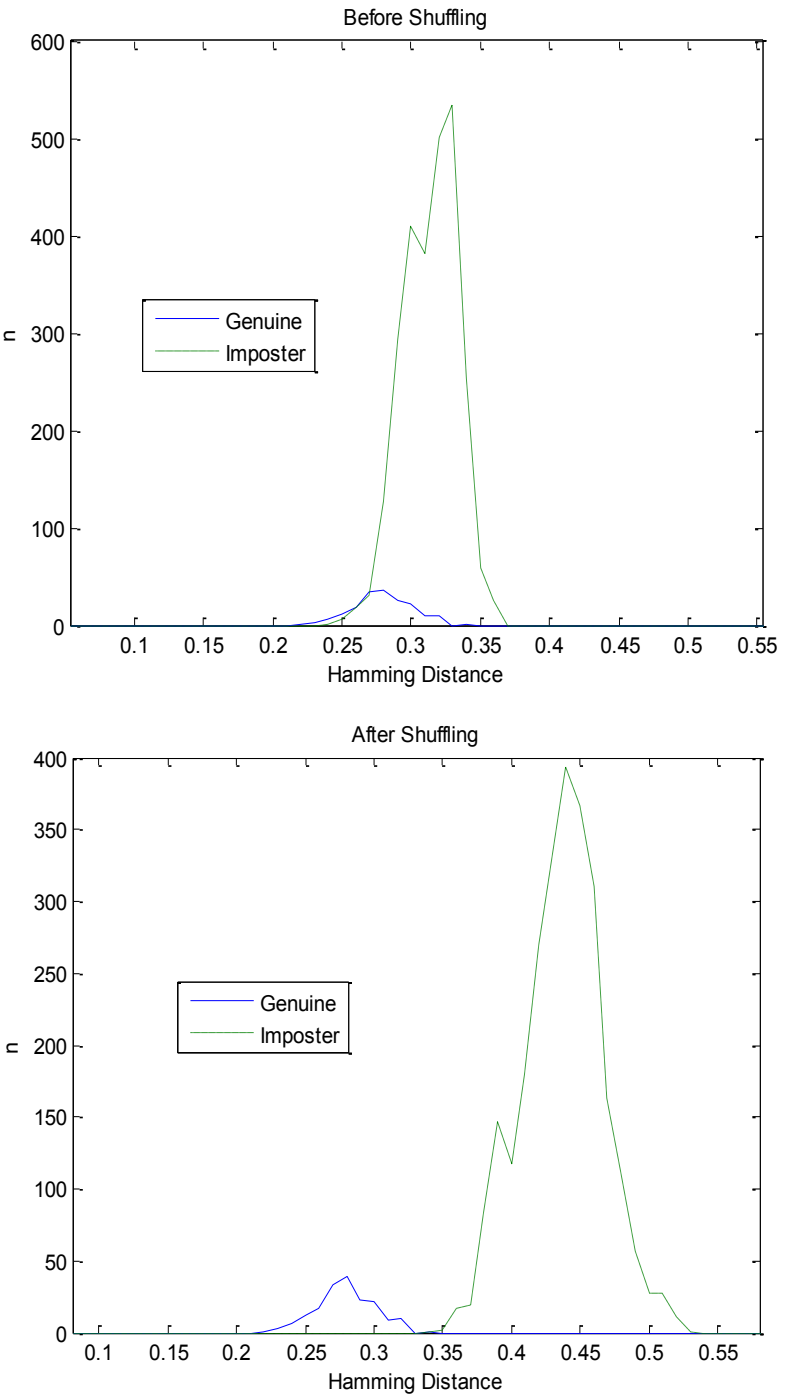

Figure 39 Hamming distance distributions of genuine and imposter distributions before and after shuffling

To further test the shuffling algorithm we evaluated the performance of biometric recognition system based on haptic handwritten signatures using two methods that have been used in the literature: artificial neural networks (ANN) and k-nearest neighbor algorithm (KNN).

For the the ANN algorithm, the shuffled template matrix is fed to a multilayer Perceptron (MLP) Neural network [97] with 25 input neurons corresponding to each of the measured features; the neural network has a hidden layer of 14 neurons and 2 output neurons. We used a supervised learning approach with back propagation algorithm with a momentum of 0.2 and learning rate of 0.3. For each user we use 6 signatures for training and 6 for testing.

Neural networks are inherently secure since only the weights or strengths are stored for each user. The templates used for training are never stored nor needed in the authentication process. Artificial neural networks were chosen because of their ability of classification where strong correlations between the different attributes exist, like force and velocity or position and acceleration.

We also experimented with the k nearest neighbor (KNN) algorithm [98], to evaluate the performance of the shuffling algorithm on a different authentication method. K-NN is a type of instance-based learning, where an object is classified by a majority vote of its k neighbors. Hence, the object is assigned to the class most common amongst its k nearest neighbors. In our experiment we chose k = 3.

To evaluate our proposed system we hence compare the ROC of the system before and after the proposed shuffling. Figure 40 shows the ROC for the artificial neural network recognition system and as we can see the shuffling algorithm not only maintains the performance of the system, it actually improves the performance by improving the intra-user variability. Figure 41 shows the ROC for the k-NN algorithm, and although not as much as in the case of neural networks, a slight improvement is still obvious in the recognition rates after the shuffling algorithm.

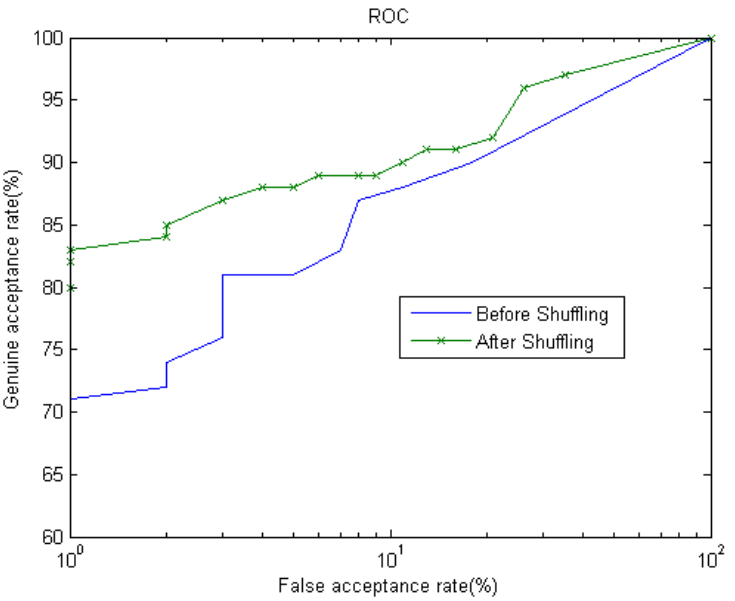

Figure 40 Performance of the proposed ANN system before and after shuffling

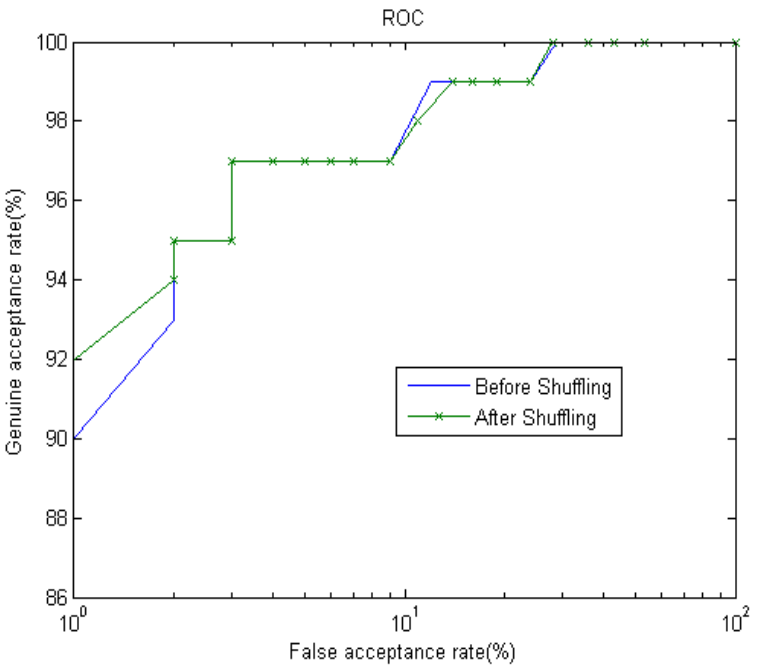

Figure 41 Performance of the proposed k-NN system before and after shuffling

To gain better insight we also compared the performance of the both systems in terms FAR and FRR for each user based on user dependant threshold that was set using trails 7, 8 and 9. Table 7 shows the results for ANN, while Table 8 shows the results for the KNN.

User	Before Shuffling			After Shuffling		
	Threshold	FAR%	FRR%	Threshold	FAR%	FRR%
1	0.23	1	17	0.13	2	0
2	0.13	0	0	0.13	0	0
3	0.37	0	50	0.17	3	33
4	0	100	0	0.01	33	17
5	0.03	1	50	0.12	12	17
6	0.01	8	0	0.12	4	0
7	0.02	3	0	0.59	0	33
8	0.01	21	17	0.15	3	50
9	0.01	10	0	0.05	12	0
10	0.01	8	0	0.06	2	0
11	0.02	22	0	0.01	24	0
12	0.01	10	0	0.07	6	0
13	0.02	4	0	0.04	2	0
14	0.18	0	33	0.18	1	0
15	0.06	7	0	0.22	2	0
16	0.11	2	0	0.24	0	33

Table 7 Performance of the proposed ANN based on user dependant threshold (trail 7,8,9 are used for setting the threshold)

User	Before Shuffling			After Shuffling		
	Threshold	FAR%	FRR%	Threshold	FAR%	FRR%
1	0.35	0	67	0.35	0	67
2	0.19	0	0	0.19	0	0
3	0.16	0	0	0.16	0	0
4	0.09	26	0	0.09	26	0
5	0.33	0	33	0.33	0	33
6	0.12	1	0	0.19	0	0
7	0.12	1	0	0.15	1	0
8	0.26	3	0	0.26	2	0
9	0.25	1	0	0.25	1	0
10	0.1	1	0	0.26	0	0
11	0.03	28	0	0.03	28	0
12	0.18	2	0	0.18	2	0
13	0.12	1	0	0.11	2	0
14	0.18	1	17	0.17	1	17
15	0.06	8	0	0.06	8	0
16	0.16	2	0	0.16	2	0

Table 8 Performance of the proposed k-NN based on user dependant threshold (trail 7,8,9 are used for setting the threshold)

Both tables affirm the conclusion from the ROC graphs that there is some improvement, but they also show that for some users the results were not as expected. This could be due to fact that some users were not comfortable with the setup or needed more time to get comfortable with it.

6.2.2 Privacy

To ensure privacy, we propose a key-binding cryptosystem as shown in Figure 42. During enrollment, the signature features are preprocessed into a binary string.Another user specific key is encoded using Reed-Solomon error correction encoding to yield a pseudo code of equal length to the binary bit string resulting from the processing of the haptic signature. Both codes are the XORed to result into the locked code. The locked code together with the hash of both user specific keys are then stored as the user template. These steps are shown in Figure 42 below.

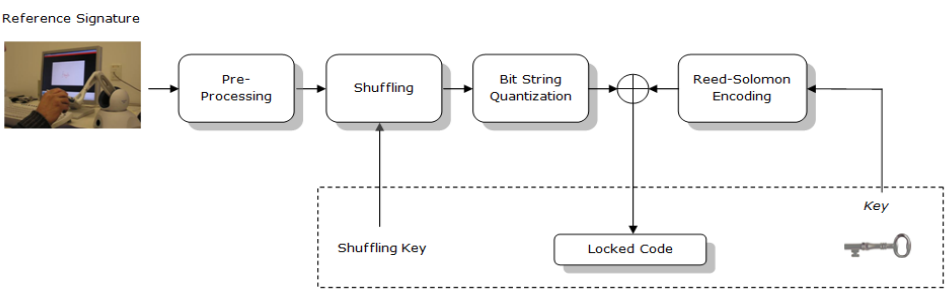

Figure 42 Enrollment scheme for proposed biometric cryptosystem for handwritten signatures with haptic information

During authentication the sample signature undergoes the same preprocessing, shuffling and quantization steps as during enrollment. The resulting bit string is the XORed with the saved locked code. The resulting code is the decoded using Reed-Solomon decoding algorithm. Successful authentication is achieved when the recovered key matches the stored user specific key. These steps are shown in Figure 43 below.

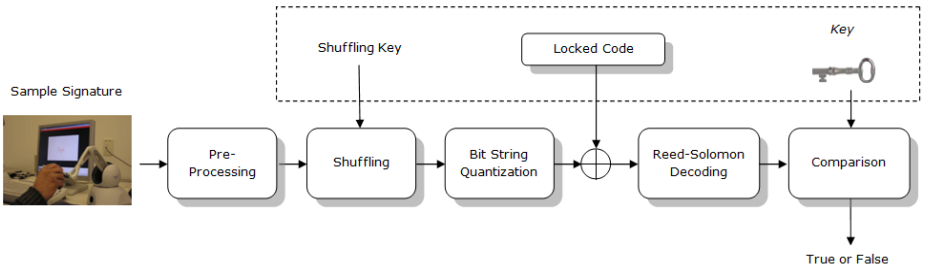

Figure 43 Authentication scheme for proposed biometric cryptosystem for handwritten signatures with haptic information

6.2.3 Performance

To evaluate our proposed system we have to calculate the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The False Acceptance Rate is calculated as the percentage of signatures from imposters are accepted as genuine by the authentication system, while False Rejection Rate refers to the percentage of signatures from genuine users that are rejected by the authentication algorithm. In our experiments we used a 500 sample signature code. The following table summarizes the results of our experiments, where m refers to the message length in bits that comprises the blocks that are fed into the error correction module. The Reed-Solomon code outputs n blocks for an input of (n-2t) blocks, where t is the number of error blocks that can be corrected by the Reed-Solomon encoding. Each block contains m bits. The key length is calculated as m* (n-2t).

				FAR	FRR
(Before Shuffling)				0.0030	0.881
(After Shuffling)				0	0.0057
Error Correction Coding					
m	n	t	key		
10	400	50	3000	0	0.0284
10	400	75	2500	0	0.0057
10	400	100	2000	0	0

Table 9 Results of the proposed system before and after error correction coding with different parameters.

From Table 9 we can see that there is a tradeoff between key length and recognition performance of the proposed system. The signature template is very long and hence even with the smallest key we have a 2000 bit key that is computationally hard to guess for an intruder.

6.2.4 Security

For the artificial neural network based recognition system the security of the proposed system is two-fold. First, the shuffling algorithm that is user specific and provides up to 25! permutations. Second, the use of ANN ensures that the template is never revealed, which adds yet another layer of security to the system. While neural networks provide security, the shuffling algorithm ensures revocability, so that databases using the same technology for authentication cannot be cross matched.

In the case of k nearest neighbour algorithm the shuffling algorithm still provides revocability and some security, but the algorithm is not secure in its nature the same way artificial neural networks are.

In our proposed bio-cryptosystem in this new field we introduced two layers of security for handwritten signatures with haptic information; first, a user specific key that is used for the shuffling algorithm. The key is used as a seed for the random generator function. Second, another user specific key is used for the error correction module of the proposed system. As we can see from Table 9, the keys that are used are a very long key, which makes them computationally hard to guess. These two security measures ensure that only the locked code and the hashed keys are stored in the database or on a smart card. The locked code does not reveal the original signature features or the key. The shuffling algorithm also ensure revocability, which means that in the case that the database is compromised, a new "signature template" can be created from the original signature without the need for re-enrollment.

6.2.5 Discussion

In recent years virtual environments and haptic devices are becoming more popular in medical, educational and entertainment fields. The field of recognizing people by their

behavioral interactions with a haptic device is still a new field of research and security of such systems will be a major factor in promoting public acceptance of the use of such system for authentication in large scale applications.

In this Chapter we propose a shuffling algorithm that enhances security, in providing revocability, as well as improves the overall performance of the authentication process. Artificial neural networks provided better security, because the templates and measured attributes are never stored, instead only weights and strength of the neurons are. K nearest neighbor algorithm is not as secure as the artificial neural network based system, but it does give better results in the overall performance with regards to the false accept and false reject rates.

We also propose a biometric cryptosystem that enhances security and provides revocability, while maintaining and, in fact, improving the performance of the biometric authentication system. Biometric cryptography is a field that combines the convenience and portability of biometrics with the security of cryptography. We were only able to test our algorithm on a small proprietary database and more experiments have to be done on a larger database to ensure efficacy of the proposed algorithm.

From Figure 39 we can see that there is no real separation between the genuine and imposter hamming distance distributions, which could imply that the great results we achieved are mainly due to the shuffling algorithm and the separation it created between those two distributions. Hence, more research needs to be done in order to determine the features of the haptic signature that are more user dependant. These need to be tested against some forgeries as is the case with 2D handwritten signatures.

We can, therefore conclude that there is still a lot of research that needs to be done to establish this new biometric trait as an authentication approach. Also, more research needs to be done in the field of securing the templates used in haptic based authentication systems and explore more ways and incorporating cryptography and other well established secure algorithms to benefit this newly developing area of research. Integrating security when designing haptic based authentication systems will be an essential point in establishing this new technology in the ever growing field of virtual environments.

Chapter 7 Conclusion and Future Work

7.1 Conclusion

This thesis has explored different ways of securing templates in iris based biometric authentication systems. Compromising the template database poses two major risks: first, it enables attackers to create spoofs from the template, which in turn enables them to access other biometric based authentication systems using the same biometric trait. Second, compromised templates enable the cross-referencing between databases using the same trait without the user's consent.

To address this issue, several solutions were presented in this research and all of them were tested using the same iris database to allow for an objective comparison. And all developed systems were evaluated according to the criteria set in the literature for any successful template protection scheme: revocability, privacy, security and performance.

To our knowledge, prior research done in this area was mostly focused on fingerprint and face recognition. Research done on iris based templates in an effort to use existing established scheme mostly had to redesign iris recognition systems to incorporate template security schemes. In our research, we thus focused on designing all our schemes in a way that can be added to already existing and established iris recognition systems that are currently using binary templates. This posed a lot of hurdles that had to be overcome to successfully achieve our goals. We were able to successfully design and implement four schemes:

The first scheme designed used watermarking to secure the iris templates. We combined Discrete Wavelet Transform together with the last significant bit watermarking to be able to withstand minor geometrical and frequency attacks. To ensure revocability we implemented a shuffling algorithm that divides the iris template into blocks and then reorders the blocks using a user specific key. Watermarking ensures the privacy by hiding the template into a cover work. Security is guaranteed by the use of two user specific keys: a $4*10^7$ user specific key is used for embedding the watermark and a 210 bit user specific key is used for shuffling the iris template. The suggested system's performance is evaluated by calculating the FAR and FRR values, which were 0.1 and 1.28%

respectively and is able to withstand minor frequency and geometrical attacks with only degradation in the FRR up to 9.2% while maintaining a low 0.2 % FAR.

The second system designed and developed is a biometric cryptosystem that uses error correction coding to account for intra-user variability. The system uses Hadamard coding to account for random errors caused by the environment, like position, light, etc. Hadamard coding is then concatenated with Reed Solomon coding to account for burst errors caused by eyelid occlusion or eyelashes, etc. We used the iris shuffling algorithm to introduce revocability. A pseudo iris code is created after a user specific key is encoded using the concatenation of Hadamard and Reed Solomon encoding. Privacy is achieved by only storing the shuffled iris code XORed with the pseudo iris code. Security is guaranteed by using two user specific keys: a 128 bit key used for the iris shuffling algorithm and a 445 bit key used to generate the pseudo iris code using error correction coding. We also introduced a CRC module that eliminates the need to store the second user specific key used in the error correction module. The performance achieved was 0% FAR and 0.66% FRR.

The third scheme implements a fuzzy vault scheme to secure iris templates. The fuzzy vault scheme is a well established scheme used to secure biometric templates by mapping the unordered feature set on a user specific polynomial. The mapped points are stored together with other points that do not lie on the polynomial to conceal the genuine points. All points together form the fuzzy vault. For authentication, again the feature sets are mapped on the user specific polynomial and then the mapped points are used to guess the nearest genuine points from the fuzzy vault, which enables the calculation of the user specific polynomial using Lagrange interpolation. In our implementation, we were able to overcome the fact that iris templates are not comprised of an unordered feature set, by using a modified fuzzy vault that uses the positions in a matrix instead of the polynomial. Iris template shuffling was used to ensure revocability, and privacy achieved by concealing the positions in the fuzzy vault matrix by filling the rest of matrix with elements in the same value range. The 128 bit key used for shuffling and the 324 bit key used in the creation of the modified fuzzy vault ensure the security of the proposed fuzzy vault scheme. The proposed system achieved a 0% FAR and 0.93% FRR, which is suitable for real life applications on a large scale.

Table 10 below gives a summary and comparison of the different systems and how they compensate for inter-user variability, which data is stored and the security guarantee given in each case.

Scheme	***Watermarking***		***Bio-cryptosystem***		***Feature Transformation***	
	Space	**Transform**	**Key-generating**	**Key-binding**	**Invertible**	**Non-invertible**
Inter-user Variability	Original Matching Scheme		Error Correction Coding		Matching in the transformed Domain	
Data Stored	Cover Work & Key		Helper Data & Key		Transformed Template & Key	
Security Guarantee	Key Security		Key Security & Amount of data leaked by Helper Data		Key Security	Key Security & Non-invertability

Table 10 Comparison of the different iris template protection schemes

Our last scheme we proposed in our research is a scheme that combines one-way transformations, bio-cryptosystems and watermarking into one iris template security scheme with three layers of security. One-way transformation ensures revocability through iris template shuffling. A pseudo iris code is generated from a user specific key that is encoded using concatenated Hadamard and Reed Solomon encoding. The pseudo iris code is then combined with the shuffled iris code and then hidden into some cover work using LSB and DWT watermarking. This ensures the privacy of the iris template. Security is dependent on the use of three user specific keys: a 120 bit key used for iris template shuffling, a 210 bit key for the error correction coding module and a $4x10^7$ bit key for the watermarking module. A 0% FAR and 0.93% FRR shows a performance that is superior to watermarking only approach and results suitable for large scale practical applications. This system combines the advantages and minimizes the limitations of each of the methods on its own as listed in Table 11.

Scheme		*Advantages*	*Limitations*
Watermarking	**Space**	- Use of key increases Inter-user variability and enables revocability - Template is invisible and inseparable from cover work	- Integrity of templates depends on robustness of watermarking algorithm. - Size of the cover work has to be chosen to accommodate template size.
	Transform		
Bio-cryptosystems	**Key-generating**	- Key generation from biometric templates eliminates the need for a matching module.	- Very difficult to generate stable keys from iris templates with high enough entropy.
	Key-binding	- Easier to implement using existing well researched error correction coding techniques.	- On its own bio-cryptosystems do not offer revocability of iris templates.
Feature Transformation	**Invertible**	- Easy to implement and enhances inter-user separation	- Is only as secure as the key used to perform the transformation.
	Non-invertible	- Offers security for templates even if the key used for transformation is compromised.	- Challenging to find a transform that preserves inter-user discriminability while ensuring non-invertability
Hybrid		- Offers many layers of security, so even if one layer is compromised, the template would still be protected	- More complicated to implement and hence will probably be slower for online applications

Table 11 Advantages and limitations of the different iris template protection schemes

All of the results of implementations of different algorithms were all tested using the same database [45] and where all chosen to complement existing binary iris template databases so they can enhance the security of the system without the need to redesign already established iris-based biometric authentication systems [44].

In the last chapter we started the research in the novel field of securing haptic biometric templates

From the experimental results of the evaluation of the proposed system, the following must be put into consideration:

- Building an iris template security on already existing established binary iris templates is possible and the results are very promising.

- One way transformations are the simplest way to secure iris templates. It is complicated to design non-invertible one way transforms that maintain user template uniqueness and inter-user variablities.

- Watermarking offers a field of securing iris templates that has many possibilities. Our suggested systems that use existing watermarking techniques to secure iris template give acceptable results for large scale applications.

- Biometric cryptosystems can be adapted to secure binary iris templates with results that not only maintain original iris recognition performance, but actually improve the overall performance and especially when it comes to False Acceptance Rates that have always resulted as 0% in our implementations and tests.

- Combining all three categories for securing iris templates, while increasing the complexity of the proposed system, it significantly increase the security and privacy of the iris templates while offering performance rates that are suitable for large scale high security applications, like airport checking and border crossing.

7.2 Future Work

A need for identity management and protection is growing in a word growing closer and more complicated every day. Biometric authentication offers a very promising method to ensure security as well as convenience. But they also face many challenges that can limit

their use on a large scale. One of the most important vulnerabilities is the biometric template database that, if compromised, cannot be revoked and can be used for cross-referencing among different databases using the same biometric trait.

Although progress has been done in this research there still remain several points that can be improved on in future research:

- Develop and implement a non-invertible transform that will maintain uniqueness of iris templates while allowing revocability. More research is thus needed to overcome the challenges facing the development of such a transform.

- Using a lossless transform like the redundant discrete wavelet transform (RDWT) with watermarking to secure iris templates. RDWT is a discrete wavelet transform that does not include downsampling or upsampling in the decomposition and reconstruction of the image. It would be interesting to test if the decimation process would affect the retrieval of the iris template.

- For future research, also the possibility of implementing iris recognition and iris template security algorithms on hardware to enable faster real time implementations.

- Protecting Haptic based biometrics is still in its infancy and more research has to be done to both improve the recognition algorithms as well as securing the stored templates especially in a word were 3D and virtual environments applications are exponentially increasing.

References

[1] A. K. Jain, S. Pankanti, and R. Bolle, eds., "***BIOMETRICS: Personal Identification in Networked Society***", Kluwer Academic Publishers, 1999.

[2] F. Petitcolas, R. Anderson and M. Kuhn. "***Information Hiding – A Survey***", Proceedings of the IEEE., 87(7):1062–1078, July 1999.

[3] B. Schneier, "***The uses and abuses of biometrics***", Communications of the ACM, 42(8):136, August 1999.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "***Enhancing security and privacy in biometrics-based authentication systems***", IBM Systems Journal, 40(3):614-634, 2001.

[5] A. K. Jain, A. Ross, and S. Pankanti, "***Biometrics: A Tool for Information Security***", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.

[6] I. Buhan and P. Hartel, "***The State of the Art in Abuse of Biometrics***", Centre for Telematics and Information Technology, University of Twente, Technical Report TR-CTIT-05-41, December 2005.

[7] A. Edler, "***Can sample images be regenerated form biometric templates***", Proceeding of Biometrics consortium conference 2003, Hyatt Regency Crystal City, Arlington, VA, USA

[8] P. Syverson, "***A Taxonomy of Replay Attacks***", in Proceedings of the Computer Security Foundations Workshop (CSFW97), Franconia, USA, June 1994, pp. 187–191.

[9] K. Lam and D. Gollmann, "***Freshness Assurance of Authentication Protocols***", in Proceedings of European Symposium on Research in Computer Security, Toulouse, France, 1992, pp. 261–272.

[10] K. Lam and T. Beth, "***Timely Authentication in Distributed Systems***", in Proceedings of European Symposium on Research in Computer Security, vol. 648, Toulouse, France, 1992, pp. 293–303.

[11] R. M. Bolle, J. H. Connell, and N. K. Ratha, "***Biometric Perils and Patches",*** Pattern Recognition, vol. 35, no. 12, pp. 2727–2738, 2002.

[12] N. Ratha, and J. Connell, "***Cancelable Biometrics***", presented at Biometric Consortium 2000 Conference, Sept. 13-14, 2000.

[13] J. L. Cambier, U. M. Cahn von Seelen, R. Glass, R. Moore, I. Scott, M. Braithwaite, and J. Daugman; "***Application-Specific Biometric Templates.***", IEEE Workshop on Automatic Identification Advanced Technologies, Tarrytown, NY, p.167-171, March 14-15, 2002

[14] A. K. Jain, K. Nandakumar and A. Nagar, "***Biometric Template Security***", EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, January 2008.

[15] A. K. Jain, A. Ross, and U. Uludag, "***Biometric Template Security: Challenges and Solutions***", Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.

[16] Biometric System Laboratory - University of Bologna, "***FVC2006: The Fourth International Fingerprint Verification Competition***," Available at http://bias.csr.unibo.it/fvc2006/default.asp.

[17] P. J. Phillips, W. T. Scruggs, A. J. O´ Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, and M. Sharpe, "***FRVT 2006 and ICE 2006 Large-Scale Experimental Results***," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 5, pp 831-846, May 2010.

[18] P. Kenny, P. Ouellet, N. Dehak, V. Gupta, and P. Dumouchel, "***A Study of Inter-Speaker Variability in Speaker Verification***, " IEEE Transactions on Audio, Speech and Language Processing, July 2008.

[19] I.J. Cox, M. Miller, J. Bloom, "***Digital Watermarking***", Morgan Kaufmann Publishers, 2002.

[20] S. Katzenbeisser, F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 1999.

[21] G. Voyatzis, N. Nikolaidis, I. Pitas, "***Digital Watermarking: An Overview***", 9th European Signal Processing Conference (EUSIPCO'98), 1998

[22] X. Ye Z. He W. Zhang , "***A data hiding method for improving the self-security of iris recognition***", International Conference on Communications, Circuits and Systems, ICCCAS, pp. 762-766, May 2008.

[23] M. Kutter, F. Jordan, and F. Bossen, "***Digital Signature of Color Images Using Amplitude Modulation***", Proc. SPIE, vol. 3022, pp. 518-526, 1997.

[24] S. Katzenbeisser, F.A.P. Petitcolas, "***Information Hiding Techniques for Steganography and Digital Watermarking***", Artech House, 1999.

[25] J. Dong, T. Tan, "***Effects of Watermarking on Iris Recognition Performance***", 10th Intl. Conf. on Control, Automation, Robotics and Vision, pp. 1156-1161, December, 2008.

[26] B. Chen and G. W. Wornell, "***Quantization index modulation methods for digital watermarking and information embedding of multimedia***", Journal of VLSI Signal Processing 27, pp. 7-33, 2001.

[27] K. R. Park, D. S. Jeong, B. J. Kang, E. C. Lee, "***A Study on Iris Feature Watermarking on Face Data***", ICANNGA(2), pp. 415-423, 2007.

[28] M. Vatsa, R. Singh, P. Mitra, A. Noore , "***Digital watermarking based secure multimodal biometric system***", IEEE International Conference on Systems, Man and Cybernetics**,** Vol. 3, pp: 2983- 2987,October 2004.

[29] M. Vatsa, R. Singh, P. Mitra, A. Noore, "***Comparing robustness of watermarking algorithms on biometrics data***", Proceedings of the Workshop on Biometric Challenges from Theory to Practice – ICPR Workshop, pp. 5–8, 2004.

[30] M. Vatsa, R. Singh, A. Noore, M. M. Houck and K. Morris, "***Robust biometric image watermarking for fingerprint and face template protection***", IEICE Electron. Express, Vol. 3, No. 2, pp.23-28, (2006).

[31] J. Lim et al., "***Invertible Watermarking Algorithm with Detecting Locations of Malicious Manipulation for Biometric Image Acquisition***", LNCS, vol. 3832, pp. 763-769, 2006.

[32] H. Lin and K.J Anil.., "***Integrating Faces and Fingerprints for Personal Identification***", IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998

[33] A. K. Jain, U. Uludag, "***Hiding Biometric data***", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo1.25, No.ll, November 2003

[34] A. K. Jain, U. Uludag and R. Hsu, "***Hiding a Face in a Fingerprint Image***", Proc. of Int. Conf. on Pattern Recognition. vol. 3, pp. 756-759, 2002

[35] M. M. Yeung and S. Pankanti, "***Verification Watermarks on Fingerprint Recognition and Retrieval***", Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents, vol. 3657, 1999.

[36] M. Fouad, A. Elsaddik, and E. Petriu, "***Combining DWT and LSB Watermarking to Secure Revocable Iris Templates",*** International Conference on Information Sciences, Signal Processing and their Applications, ISSPA 2010.

[37] M. Fouad, A. Elsaddik, J. Zhao, and E. Petriu; "***Combining Cryptography and Watermarking to Secure Revocable Iris Templates***", International Instrumentation and Measurement Technology Conference, I2MTC 2011.

[38] M. Fouad, A. Elsaddik, J. Zhao, and E. Petriu; "***A Fuzzy Vault Implementation for Securing Revocable Iris Templates***", IEEE International Systems Conference, SysCon 2011.

[39] M. Fouad, A. Elsaddik; "***Using cyclic redundancy check to eliminate key storage for revocable iris templates*** ", Canadian Conference on Electrical and Computer Engineering, CCECE 2011.

[40] http://www.nysoa.org/index.php?page_id=131

[41] J. Daugman, "***How iris recognition works***", IEEE Transactions on Circuits Systems and Video Technology, vol.14, pp.21–30, 2004.

[42] J. Daugman, "***Recognizing Persons by their Iris Patterns***", Biometrics: Personal Identification in Networked Society, A. K.Jain, R. Bolle, and S. Pankanti, Eds. London, UK: Kluwer Academic Publishers, 1999, pp. 103–122.

[43] J. Daugman, "***Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons***", Proceedings of the IEEE, vol.94, pp.1927–1935, 2006.

[44] J. G. Daugman, "***High confidence visual recognition of persons by a test of statistical independence***," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, pp. 1148–1161, Nov. 1993.

[45] **CASIA** Iris Database of The Chinese Academy of Science, http://www.sinobiometrics.com/resources.htm (accessed April 2009)

[46] J. Zuo, N.K. Ratha and J.H. Connell , "***Cancelable iris biometric***", 19th International Conference on Pattern Recognition (ICPR), pp.1-4, December 2008.

[47] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "***Biometric Cryptosystems: Issues and Challenges***", Proceedings of the IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948-960, June 2004.

[48] F. Hao, R. Anderson and J. Daugman, "***Combining crypto with biometrics effectively***", IEEE Transactions on Computers 55, pp. 1081–1088, 2006.

[49] S.S. Agaian, "***Hadamard Matrix and Their Applications***", LNM, Springer Verlag, 1985.

[50] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zémor, "***Optimal iris fuzzy sketches***", IEEE First International Conference on Biometrics: Theory, Applications and Systems, BTAS'07, 2007.

[51] G. I. Davida, Y. Frankel, and B. J. Matt, "***On enabling secure applications through online biometric identification***" in Proc. 1998 IEEE Symposium on Privacy and Security, pp. 148–157, May 1998.

[52] G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "***On the relation of error correction and cryptography to an offline biometric based identification scheme***," in Proceedings of the Workshop of Coding and Cryptography, pp. 129–138, 1999.

[53] J.P. Linnartz, P. Tuyls; "***New shielding functions to enhance privacy and prevent misuse of biometric templates***". In Proceedings of the 4th International Conference on Audio and Video Based Biometric Person Authentication, Guildford, UK, pp. 393-402, 2003.

[54] E. Verbitskiy, P. Tuyls, D. Denteneer, J.P. Linnartz; "***Reliable biometric authentication with privacy protection***". In: Proceedings of the 24th Symposium on Information Theory in the Benelux, Veldhoven, The Netherlands, 2003.

[55] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. "***Practical Biometric Authentication with Template Protection***", Proceedings of Fifth International Conference on Audio-and Video-based Biometric Person Authentication, pp. 436-446, July 2005.

[56] Y. Sutcu, H. T. Sencar, and N. Memon; "***A secure biometric authentication scheme based on robust hashing***", In Proceedings of ACM Multimedia and Security Workshop (MM&Sec'05), New York, NY, pages 111-116, 2005.

[57] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. "***Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data***", Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, in Lecture Notes for computer Science, vol. 3027, Springer, 2004.

[58] M. Savvides and B. V. K. Vijaya Kumar, "***Cancellable Biometric Filters for Face Recognition***," in Proceedings of IEEE International Conference Pattern Recognition, vol. 3, Cambridge, UK, August 2004, pp. 922–925.

[59] Y. Sutcu, Q. Li, and N. Memon. "***Protecting Biometric Templates with Sketch: Theory and Practice***", IEEE Transactions on Information Forensics and Security, 2(3):503-512, September 2007.

[60] W. W. Peterson and E. J. Weldon, "***Error Correcting Codes***". Cambridge, MA: MIT Press, 1988.

[61] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, "***Biometric Encryption™***", Chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nicholls, pp. 649-675, McGraw Hill, 1999.

[62] A. Juels and M. Wattenberg, "***A fuzzy commitment scheme***," CCS 1999: Proceedings of the 6th ACM conference on Computer and communications security, pp. 28-36, 1999.

[63] A. Juels and M. Sudan. "***A fuzzy vault scheme***", A. Lapidoth and E. Teletar, editors, Proc. IEEE International Symposium on Information Theory, page 408, 2002.

[64] C. S. Chin, A. B. J. Teoh, and D. C. L. Ngo, "***High Security Iris Verification System Based On Random Secret Integration***", Computer Vision and Image Understanding, vol. 102, no. 2, pp. 169–177, May 2006.

[65] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "***Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs***", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 1892–1901, December 2006.

[66] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "***Biometric Key Binding: Fuzzy Vault based on Iris Images***", Proceedings of Second International Conference on Biometrics, Seoul, South Korea, pp. 800–808, August 2007.

[67] O. T. Song, A. B. J. Teoh, and D. C. L. Ngo, "***Application-Specific Key Release Scheme from Biometrics***", International Journal of Network Security, vol. 6, no. 2, pp. 127–133, March 2008.

[68] E. Srinivasa Reddy, I. Ramesh Babu, I.; "***Authentication Using Fuzzy Vault Based on Iris Textures***", Second Asia International Conference on Modeling & Simulation, AICMS 08, 13-15 May, pp: 361 – 368, 2008.

[69] E.S. Reddy, I.R. Babu; "***Performance of Iris Based Hard Fuzzy Vault***"; IEEE 8th International Conference on Computer and Information Technology Workshops, 8-11 July, pp:248 – 253, 2008.

[70] X. Wu, N, Qi, K, Wang, D. Zhang, "***A Novel Cryptosystem Based on Iris Key Generation***", ICNC Fourth International Conference on Natural Computation, vol. 4, pp.53-56, 2008.

[71] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, J. Kim, "***A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System***", IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, pp. 1302-1313, Volume: 38, Issue: 5, 2008.

[72] A. S. Bakhtiari, A. A. B. Shirazi, and B. Zamanlooy, D. Mery and L. Rueda (Eds.), "***An Efficient Biocryptosystem Based on the Iris Biometrcs***", PSIVT 2007, Lecture Notes in Computer Science 4872, pp. 334 – 345, 2007.

[73] F. Monrose, M. K. Reiter, and S. Wetzel. "***Password hardening based on keystroke dynamics***", In Proceedings of the 6th ACM conference on Computer and Communications Security, pages 73–82, November 1999.

[74] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. "***Cryptographic key generation from voice***", In Proceedings of IEEE Symposium Security & Privacy, pp. 202–213, 2001.

[75] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, B. Dorizzi; "***Three factor scheme for biometric-based cryptographic key regeneration using iris***", Biometrics Symposium, BSYM '08, pp: 59-64, 23-25 Sept. 2008.

[76] S.Kanade, D. Petrovska-Delacretaz, B. Dorizzi,; "***Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data***", IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2009, pp. 120 – 127, June 2009.

[77] X. Wu, N. Qi, K. Wang and D. Zhang, "***An Iris Cryptosystem for Information Security***", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1533-1536, 2008.

[78] L. Zhang, Z. Sun, T. Tan, S. Hu: "***Robust Biometric Key Extraction Based on Iris Cryptosystem***", International Conference on Biometrics, ICB 2009, pp.1060-1069, 2009.

[79] F. H. Álvarez, L. H. Encinas, C. S. Ávila; "***Biometric Fuzzy Extractor Scheme for Iris Templates***", Proceedings of The 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing, WORLDCOMP 2009.

[80] F. H. Álvarez, L. H. Encinas, "***Security Efficiency Analysis of a Biometric Fuzzy Extractor for Iris Templates***", Computational Intelligence for Information Systems, vol. 63, pp.163-170, Springer, 2009.

[81] N. K. Ratha and S. Chikkerur and J. H. Connell and R. M. Bolle, "***Generating Cancelable Fingerprint Templates***", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, pp. 561-572, 2007.

[82] Y. Sutcu, H. T. Sencar and N. Memon, "***A Geometric Transformation to Protect Minutiae-Based Fingerprint Templates***", In SPIE International Defense and Security Symposium, 2007.

[83] A. Nagar, S. Chaudhury, "***Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme***", Proceedings of the International conference on Pattern Recognition, pp. 537-540, 2006.

[84] X. Ye, Z. He, and Z. Zhao, "***A data hiding approach for the self-security of iris recognition***", Chinese Optics Letters, vol. 6, pp. 487-490, 2008.

[85] N. K. Ratha, J. Zuo, and J.H. Connell, "***Cancelable iris biometric***", 19th International Conference on Pattern Recognition (ICPR), pp.1-4, December 2008.

[86] A.S. Tanenbaum, "***Computer Networks***", 4th edition, Prentice-Hall International, Inc,2003

[87] M. Rahmani, W. Hintermaier, B. Mueller-Rathgeber and E. Steinbach: "***Error Detection Capabilities of Automotive Network Technologies and Ethernet – A Comparative Study***", in Intelligent Vehicles Symposium, 2007 IEEE, p. 674–679, Istanbul, Turkey, June 2007

[88] P. Koopman; "***32-Bit Cyclic Redundancy Codes for Internet Applications***". The International Conference on Dependable Systems and Networks: pp.459-468, 2002.

[89] O. Rioul , M. Vetterli , "***Wavelets and signal processing***", IEEE Signal Processing Magazine, vol. 8, no. 4, pp. 14–38, 1991.

[90] L. Masek, P. Kovesi. "***MATLAB Source Code for a Biometric Identification System Based on Iris Patterns"***. The School of Computer Science and Software Engineering, The University of Western Australia. 2003.

[91] A. El Saddik, M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler. ***"A Novel Biometric System for Identification and Verification of Haptics Users".*** IEEE Transaction on Instrumentation and Measurement, Vol.56, No. 3, June 2007.

[92] F. A. Alsulaiman, J. Cha, and A. El Saddik, M. Ferre (Ed.) ***"User Identification Based on Handwritten Signatures with Haptic Information"*** Haptics: Perception, Devices and Scenarios, Springer Berlin / Heidelberg, 2008, 5024, 114-121

[93] F. Monrose, A. Rubin, ***"Authentication via keystroke Dynamics".*** In Proc 4th ACM Conference of Computer and Communication Security. 1997. pp. 48-56

[94] E. Maiorana, P. Campisi, A. Neri, ***"Feature Selection and Binarization for On-line Signature Recognition"***, The 3 rd IAPR/IEEE International Conference on Biometrics (ICB 2009), June 2009, Alghero , Italy

[95] M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler, A. El Saddik. ***"Haptic-Based Biometrics: A Feasibility Study"***. In Proc. Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems. 2006. pp. 256-271.

[96] M. Orozco, B. Malek, M. Eid, A. El Saddik, ***"Haptic-Based Sensible Graphical Password"***. In Proc. Virtual Concept 2006, Playa Del Carmen, Mexico, November 2006.

[97] I. Witten and E. Frank, ***"Data Mining: Practical Machine Learning Tools and Techniques"*** Morgan Kaufmann, 2005

[98] D. Aha, D. Kibler, and M. Albert, ***"Instance-Based Learning Algorithms",*** Machine Learning, 1991, 6, pp.37-66.

[99] M. Fouad, A. Elsaddik, and E. Petriu; " ***Revocable Handwritten Signatures with Haptic Information"***, IEEE International Symposium on Haptic Audio-Visual Environments and Games, HAVE 2011.

[100] http://www.iriscan.com/solutions.php?page=2