

**Biometric layering: template security
and privacy through multi-biometric
template fusion**

by

Muhammet Yıldız

Submitted to
the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

SABANCI UNIVERSITY

May 2016

BIOMETRIC LAYERING: TEMPLATE SECURITY AND PRIVACY THROUGH
MULTI-BIOMETRIC TEMPLATE FUSION

APPROVED BY

Prof. Dr. Berrin YANIKOĞLU
(Thesis Supervisor)




Prof. Dr. Albert LEVİ



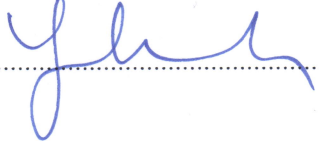
Assoc. Prof. Dr. Hakan ERDOĞAN



Assoc. Prof. Dr. Mehmet GÖKTÜRK



Asst. Prof. Dr. Yakup GENÇ



DATE OF APPROVAL: 31.05.2016

©Muhammet Yıldız 2016
All Rights Reserved

To my family...

Acknowledgements

I wouldn't have achieved this dissertation without the help of numerous people. Firstly and most importantly, I would like to express my sincere gratitude to my thesis advisor, Prof. Berrin Yanikođlu, who has been tirelessly helpful to me during my entire work for her patience, guidance and precise vision. I learned so much from her deep understanding of the field. This work would never come out without her assistance and guidance. Additionally, I would like to thank my thesis committee members Prof. Albert Levi, Prof. Hakan Erdoğan, Prof. Mehmet Göktürk, Prof. Yakup Genç and Prof. Selim Balcısoy for their valuable contribution and guidance to my work.

Working a Ph.D. and taking care of a family are the same pole of two magnets, pushing each other away. Without the support of a thoughtful family, one cannot achieve a Ph.D and be married with children at the same time. Therefore, I would like to thank my beautiful wife and kids for their support and patience during my Ph.D study.

Finally, I would like to thank to TÜBİTAK BİLGEM for supporting my Ph.D. during my employment as a researcher.

Biometric layering: template security and privacy through multi-biometric template fusion

MUHAMMET YILDIZ

CS, Ph.D. Thesis, 2016

Thesis Supervisor: Berrin Yanikoğlu

Keywords: biometrics, multibiometrics, fingerprint, voice, minutiae, layering.

Abstract

As biometric applications are gaining popularity, there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. Biometric template protection mechanisms suggested in recent years aim to address these issues by securing the biometric data in a template or other structure such that it is suitable for authentication purposes, while being protected against unauthorized access or cross-linking attacks.

We propose a biometric authentication framework for enhancing privacy and template security, by *layering* multiple biometric modalities to construct a multi-biometric template such that it is difficult to extract or separate the individual layers. Thus, the framework uses the subject's own biometric to conceal her biometric data, while it also enjoys the performance benefits because of the use of multiple modalities. The resulting biometric template is also cancelable if the system is implemented with cancelable biometrics such as voice. We present two different realizations of this idea: one combining two different fingerprints and another one combining a fingerprint and a spoken passphrase. In either case, both biometric samples are required for successful authentication, leading to increased security, in addition to privacy gains.

The performance of the proposed framework is evaluated using the FVC 2000-2002 and NIST fingerprint databases, and the TUBITAK MTRD speaker database. Results show only a small degradation in EER compared to a state-of-the-art fingerprint verification system and high identification rates, while cross-link rates are low even with very small databases.

Biyometrik Katmanlama: çoklu-biyometrik şablon karışımı ile şablon güvenliği ve mahremiyeti

Biometric layering: template security and privacy through multi-biometric template fusion

MUHAMMET YILDIZ

CS, Doktora Tezi, 2016

Tez Danışmanı: Berrin Yanıkoğlu

Anahtar Kelimeler: biyometri, çoklu biyometri, parmak izi, ses, öznelik noktası, katmanlama.

Abstract

Biyometrik uygulamaların kullanım alanı genişledikçe merkezi veritabanlarında tutulan biyometrik bilginin mahremiyeti ve olası kötüye kullanımı noktasında endişeler artmaktadır. Son yıllarda biyometrik şablon muhafazası konusunda yapılan çalışmalar bu problemleri şablonun kendi içinde veya doğrulama mekanizmalarını etkilemeyecek başka bir veri yapısı ile izinsiz kullanım ve çapraz karşılaştırma saldırılarına karşı korumaya yönelik çözümleri kapsamaktadır.

Bu tez çalışmasında birden fazla biyometrik bilgiyi tek bir şablon üzerinde *katmanlayarak* bir çoklu biyometrik yapı oluşturma ve bilgilerin karışımından faydanlanarak bu bilgilerin güvenliğinin ve mahremiyetinin korunması amacı ile bir yöntem sunulmaktadır. Bu yöntem kişilerin biyometrik bilgilerini yine aynı kişilerin biyometrik bilgileri ile korumayı amaçlamaktadır ve böylece sadece biyometrik temelli bir çözüm sunmaktadır. Kullanılan yöntem çoklu biyometrik bilgiyi işleyip değerlendirdiği için geleneksel tek biyometrik yöntemlere göre daha başarılı sonuçlar vermektedir.

Sunulan yöntem değiştirilebilen biyometrik bilgi ile icra edildiği durumlarda biyometrinin iptal edilebilirliği (yenilenebilirliği) de sağlanmış oluyor. Değiştirilebilen biyometrik bilgiye örnek olarak bu çalışmada ses biyometrisi kullanılmaktadır. Kişilerin kendi seslerini kullanarak kendi belirledikleri bir gizli sözcüğü söylemesi ve bu bilginin biyometrik katmana karıştırılması ile oluşturulan kayıtlar, ileride kişinin başka bir gizli sözcüğü tercih etmesi neticesinde değiştirilebilir, iptal edilebilir ve yenilenebilir olma özelliklerine de kavuşmaktadır.

Önerilen çoklu biyometrik katmanlama yöntemi FVC 2000-2002 ve NIST parmak izi veri kümelerinin yanısıra TÜBİTAK MTRD ses biyometrisi veri kümesi kullanılarak deneylerden geçirilmektedir. Test sonuçları önerilen yöntemin, alanında öncü biyometrik doğrulama sistemleri ile karşılaştırılınca Eşit Hata Oranı'nda (EHO) çok yakın sonuçlar elde edildiği gözlenmektedir. Mahremiyetin korunması noktasında tekli biyometrik bilgi ile yapılan veritabanı saldırılarının ve çapraz karşılaştırma ile kimlik teşhisi saldırılarının oldukça düşük sonuç verdiği; böylece sunulan yöntemin beklenen performansı sergilediği gözlemlenmiştir.

Contents

Acknowledgements	iv
Abstract	v
Abstract	vi
List of Figures	x
List of Tables	xi
Abbreviations	xii
1 Introduction	1
1.1 Background	1
1.2 Motivation	7
1.3 Contributions	9
1.4 Thesis Organization	10
2 Related Work	11
3 Thin Plate Spline (TPS) Matcher	17
3.1 Overview	17
3.2 Mathematical Background	20
3.2.1 Sample Applications with TPS Modelling	24
3.3 Minutiae Matching Using Thin Plate Splines	25
3.3.1 Local Matching	26
3.3.2 Global Matching	28
4 Biometric Layering with multiple biometrics	34
4.1 Overview	34
4.2 Symbols	37
4.3 Multi-biometric templates using multiple fingerprints	38
4.3.1 Enrollment	38
4.3.1.1 Feature Extraction	38
4.3.1.2 Multi-biometric Template Generation	39

4.3.1.3	Hiding Angle Information	40
4.3.1.4	Using a Subset of the Minutiae	41
4.3.1.5	Layering Three Fingerprints	41
4.3.2	Verification	42
4.4	Multi-Biometric Templates Using Fingerprints and Voice	44
4.4.1	Enrollment	44
4.4.1.1	Feature Extraction	44
4.4.1.2	Minutiae Generation	46
4.4.1.3	Multi-biometric Template Generation	46
4.4.2	Verification	47
5	Evaluation	50
5.1	Overview	50
5.2	Databases	51
5.2.1	Fingerprint Databases	51
5.2.2	Voice Database	53
5.3	Template Security and Privacy Evaluation	55
5.4	Evaluation Results Using Fingerprints (FP-FP)	57
5.4.1	Uni-modal Verification Results	57
5.4.2	Multi-modal Verification Results of the Proposed Scheme	60
5.4.3	Multi-modal Score Level Fusion	62
5.4.4	Template Security and Privacy Test Results	65
5.5	Evaluation Results of Multi-Biometric Templates Using Fingerprint and Voice	68
5.5.1	Uni-modal and Multi-modal Verification Results	69
5.5.2	Template Security and Privacy Test Results	70
5.6	Entropy and Information Leakage Analysis	72
5.7	Time Cost for Enrollment and Verification	75
6	Summary and Conclusion	77
6.1	Summary	77
6.2	Conclusions	80

List of Figures

1.1	Various biometric modalities and their applications	2
1.2	A sample biometric verification scheme that consists of two phases: Enrollment and verification	4
1.3	An illustration of a score distribution	5
1.4	An illustration of a det curve depicting FAR vs. FRR	5
2.1	Random codeword selection and δ calculation in fuzzy commitment	12
3.1	A sample fingerprint and two minutae	18
3.2	Elastic Deformation Model [1]	19
3.3	Simple Affine Transform (Only shear)	21
3.4	Three Constant, One Moving points	25
3.5	Extreme Warp	25
3.6	A minutia (m) and its five nearest neighbors forming neighborhoods (triplets-triangles).	27
3.7	Three sample triangles compared in terms of <i>Edge-Angle-Edge Similarity</i>	28
3.8	Non-Aligned fingerprints	30
3.9	Fingerprints aligned using <i>Rigid Matcher</i>	31
3.10	Fingerprints aligned by using <i>TPS Matcher</i>	31
3.11	An ROC plot displaying the GAR-FAR performance of the <i>Rigid Matcher</i> and <i>TPS Matcher</i>	33
4.1	Overview of the proposed system.	36
4.2	Sample multi-biometric templates	39
4.3	Verification Process	43
4.4	Feature extraction through HMM alignment of the MFCC features.	46
4.5	Transformation of the binarized MFCC feature into voice minutiae.	46
4.6	Verification Process for FP+Voice	48
5.1	FVC2000 Sample images of four subgroups of FVC2000 [2].	53
5.2	FVC2002 Sample images of four subgroups of FVC2002 [3].	53
5.3	Two sample fingerprints from NIST fingerprint database-2 [4].	54
5.4	DET Plots for the uni-modal and suggested multi-biometric system with FP-FP layers for FVC 2000 in (a,c) and FVC 2002 in (b,d). For ease in comparison, corresponding plots share the same color, with different markers.	61
5.5	ROC Plots corresponding to Table 5.8 (<i>FP=Fixed Password, PP=Private Password, FP+PP=Concatenated voice</i>).	72
5.6	A sample template divided into a grid of $d \times d$ sized cells.	73

List of Tables

1.1	Different biometric modalities and the related research work grouped with respect to their types	2
3.1	Error rates obtained from the Rigid vs. TPS Matcher on the NIST Fp. Database	32
5.1	Fingerprint databases used in this thesis (FVC 2000,2002 and NIST). . .	52
5.2	Voice databases used in this work (TUBITAK Speaker Database).	55
5.3	Probability $P(K)$ of K or more correct minutiae points in a given random split, for $N = 32$	56
5.4	Verification performance (% EER) with FP-FP layers.	59
5.5	Verification performance (% EER) of a multi-biometric system with score level fusion.	59
5.6	Identification and cross-link results for the NIST gallery consisting of 666 multi-biometric templates with FP-FP layers.	63
5.7	Identification and cross-link results for the FVC gallery consisting of 55 multi-biometric templates with FP-FP layers (36 Templates in <i>Method</i> ₄).	64
5.8	EER percent results for verification tests using fingerprints and voice. . .	69
5.9	Identification and Cross-Link results with a gallery consisting of 100 multi-biometric templates with fingerprint-voice layers. A and A' refer to fingerprint impressions and B , B' and C' are voice minutiae (FP+PP).	71
5.10	Estimated entropies according to different grid cell sizes ($d \times d$)	75

Abbreviations

EER	E qual E rror R ate
FAR	F alse A cept R ate
FP	F ingerprint
FPS	F ixed P assword S et
FRR	F alse R eject R ate
FTER	F ailure T o E nroll R ate
FVC	F inger V erification C hampionship
GAR	G enuine A cept R ate
GID	G enuine I dentification
HD	H amming D istance
HMM	H idden M arkov M odel
LPC	L inear P rediction C oding
MLLR	M aximum L ikelihood L inear R egression
NIST	N ational I nstitute of S tandards and T echnology
PLP	P erceptual L inear P redictive
PPS	P rivate P assword S et
SLF	S core L evel F usion
TPS	T hin P late S pline
NAI	N o A ngle I nformation
UMS	U ni- m odal S earch
UMV	U ni- m odal V erification
MMS	M ulti- m odal S earch
MMV	M ulti- m odal V erification
XLNK	C ross L ink S earch

Chapter 1

Introduction

1.1 Background

Biometrics is the science of establishing the identity of an individual based on the physical, chemical and behavioral attributes of the person [5]. The term is derived from the words “biology” and “metrics”. In today's technology, various biologic attributes (i.e. biometric traits) have started to be used as biometric discriminators. The grouping of biometric systems, depending on the type of the trait that it is based on, are called *biometric modalities*. There are various biometric modalities used in both industrial products as well as the academic research. In *Figure 1.1* various biometric systems built on different biometric modalities have been depicted.

Biometric modalities are mainly grouped into two types: *i*) physical/physiological and *ii*) behavioral modalities [6, 7]. Physiological biometric modalities depend on the physical characteristics of the human body and they either don't change or change very little with respect to the actions-movements of the subject. On the other hand, behavioral modalities emerge with respect to the subject's actions. While they also depend on the physiological characteristics, they still require an action to be detected. A list of different modalities along with the research work based on the corresponding modality has been given *Table 1.1*. The modalities are given with respect to their types.

Biometric Systems consist of components such as signal acquisition media (eg. fingerprint scanner, camera, iris scanner) for biometric information retrieval, storage media (eg. databases, smart-cards, secure execution environments) for storing the biometric

where the personal information is retrieved, and biometric verification is performed between the biometric data that is stored in the smart card and the biometric data that she provides to the sensor attached to the card reader. An example to *biometric identification* is the retrieval of a list of suspects from a database with respect to a latent fingerprint found in a crime scene.

Biometric data is generally processed and converted to a format that is understood by the decision software prior to being saved in the database. This processing is called *feature extraction* and the newly created data is generally called a *biometric template*. Some systems purge the original (raw) data after the biometric template extraction since it will not be used again.

Biometric authentication systems work in two phases: i) *enrollment phase* and ii) *verification/identification phase*. In the enrollment phase the acquired biometric signal is processed and stored in the target storage medium (smart-card or central database). In the verification/identification phase the matching of a newly obtained candidate template (i.e. *probe template*) is compared to either the stored template (if the user is known) or the entire database (if the user is to be found). A sample *biometric verification* scheme has been depicted in *Figure 1.2*.

The matching decision routine compares the probe biometric sample to the template that has previously been stored in the database and generates a similarity score as the matching result. After obtaining a similarity score, the two candidate sets are considered as a *match* if this score is above a certain threshold. The threshold can be determined by several experiments on a training set, or may be adjusted with respect to the precision requirements of the biometric system.

The value of the threshold determines the *false reject rate (FRR)*, which is the probability for a true user identity claim to be rejected, which is considered inconvenient, and *false accept rate (FAR)*, which is the probability for a false (impostor) identity claim to be accepted, and fraud condition to occur [27]. There are also two other complementary measures, namely *genuine accept rate (GAR)*, which is the probability for a true identity claim to be accepted and *genuine reject rate (GRR)*, which is the probability of a false identity claim to be rejected.

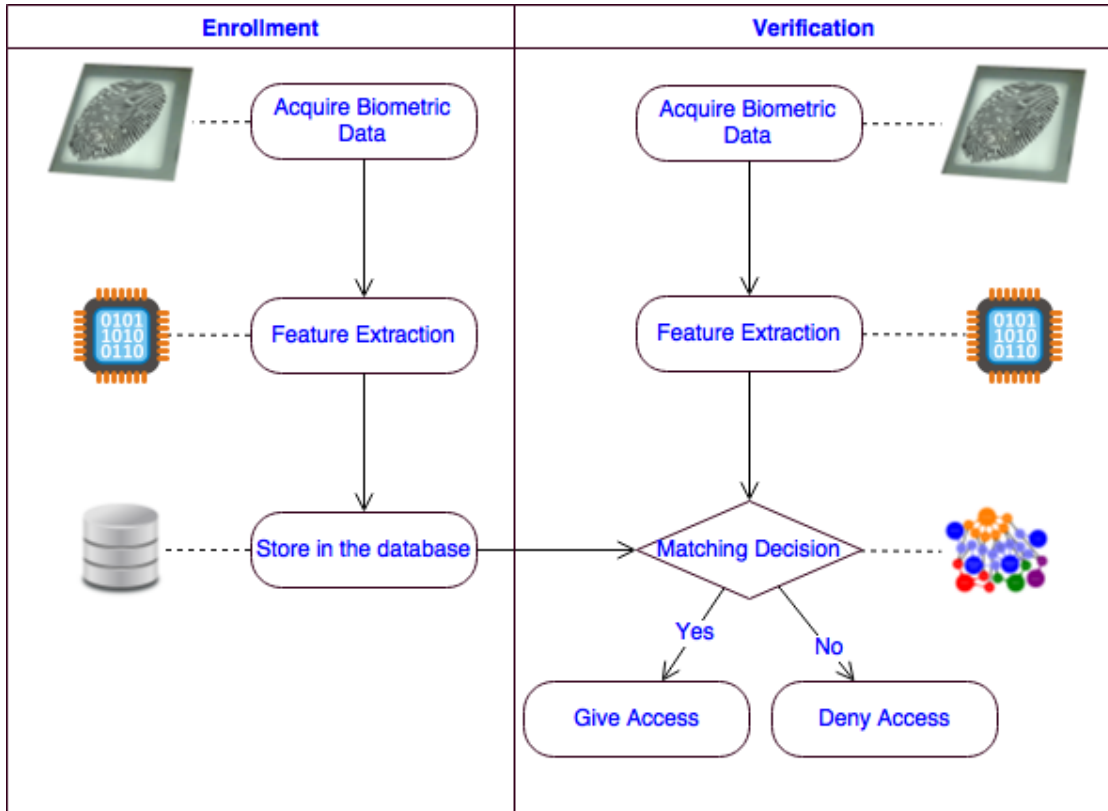


FIGURE 1.2: A sample biometric verification scheme that consists of two phases: Enrollment and verification

Biometric system performances may be measured with respect to FAR and FRR values. Their values tend to increase and decrease inversely due to the changes in the threshold. Usually, low FAR values indicate high FRR values and vice versa. However, an ideal biometric system is the one that keeps very low rates for FRR and FAR, and this has been a challenge for both the academic research and the industry.

It is possible to determine the success (i.e. performance) of a biometric system by inspecting FAR and FRR values it emits with respect to varying threshold values. As mentioned before, when FAR increases, FRR tends to decrease. At a specific point, these two values cross each other, where they become equal and the *equal error rate (EER)* value is observed.

A sample score distribution graph is given in Figure 1.3 as probability density functions for impostor and genuine verification attempts where the horizontal axis refers to the value of the score. The point of intersection of the two graphs corresponds to the EER value. The fraction of the impostor scores that stay above the threshold determine the

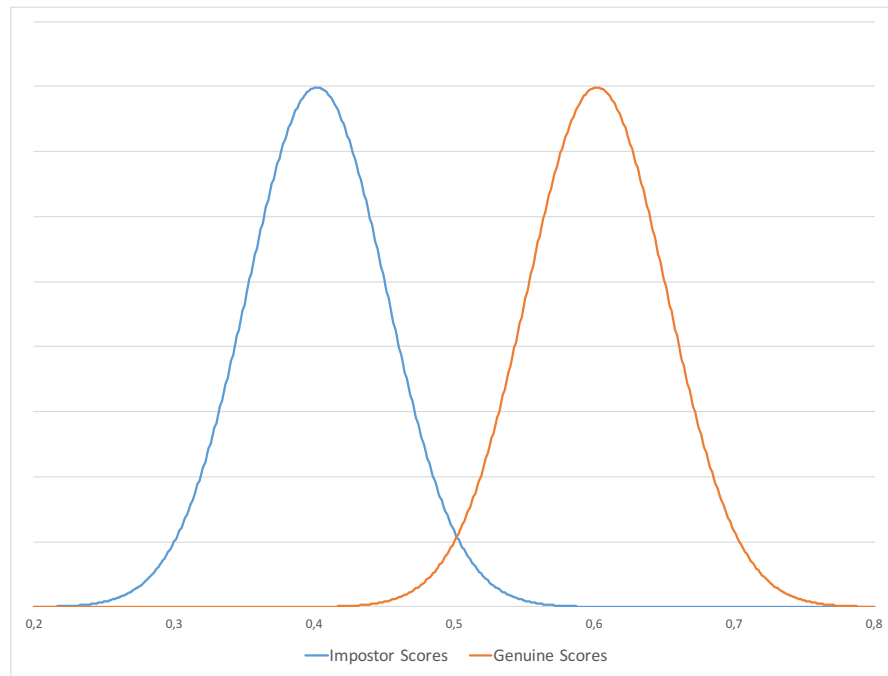


FIGURE 1.3: An illustration of a score distribution

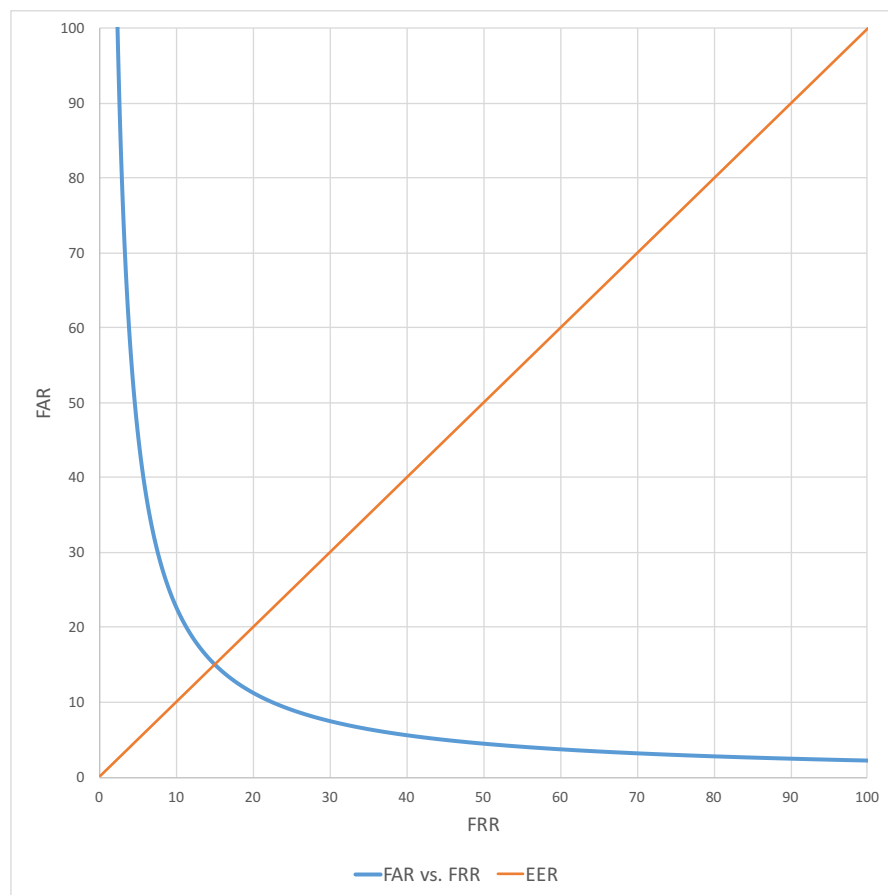


FIGURE 1.4: An illustration of a det curve depicting FAR vs. FRR

FAR and the fraction of the genuine values that fall below the threshold determine the *FRR* value.

A sample DET (Detection error tradeoff) curve that depicts the relation between FAR and FRR, has been given in Figure 1.4. It can be observed that the two values are inversely proportional. The 45° line is the EER line, intersection of which with the DET graph is the point where the FAR and FRR values are equal to each other.

1.2 Motivation

The tremendous speed in the evolution of technology has caused the computers and networked systems to enter our daily lives. With the increasing use of computers and networked systems, the identification, authentication and authorization of the system users have gained a level of extreme importance. As the academic research has advanced, it has provided users with the ability to use several security and privacy factors (i.e. personal passwords, tokens, PIN codes, SMS codes, one time passwords, etc...) and access regions that are restricted to their private possession (e.g online bank account, personal-work email).

An important security factor that has also been used in such systems is *biometric authentication*. It is increasingly being employed in authentication and identification of individuals. It might be considered as either a candidate for replacing the token and password-based security systems or a brother in arms for those security factors in the aim of establishing a more solid and secure system.

The usage of biometric data as a security factor is possible after a process called "*Extraction*", which involves the removal of unnecessary data and attainment of the useful data, called "*Biometric template*", from the raw (unprocessed) data. In biometric authentication, a questioned biometric template (i.e. *probe template*) is verified against the previously registered biometric template (i.e. *target template*), which has been captured and stored during the registration ("*Enrollment*") phase.

There are two approaches for storing biometric templates during the enrollment phase. In one alternative, the user carries a smart card containing her biometric template, and the verification of questioned sample is done within the smart card, without ever being stored in a repository (i.e. *match-on-card*). In the second alternative, the enrolled users' biometric templates are kept at a central repository and authentication is carried out by matching the query template with the target template stored at the repository. There are advantages and disadvantages associated with each of these two approaches.

The advantage of the *match-on-card* scheme is the privacy of the biometric template. Since the matching process takes place on the smart card, it does not disclose the biometric data to the outer world. This is valid even if the smart card is somehow compromised. Since the smart card application is set up not to reveal the biometric

data during the life-cycle of the card, even if the PIN number is known, or any other authentication scheme like (e.g. symmetric authentication) is achieved, it provides full privacy protection for the users' biometric templates. However, this scheme has some disadvantages that cause the real life adoption of it to fall short. The most commonly known disadvantages of this scheme are *i*) low matching performance due to the limited processing power and memory of the smart card chip, *ii*) vulnerability to *man-in-the-middle attacks* if the card generates plain matching results, *iii*) inconvenience of carrying the card and maintaining its physical security and *iv*) overhead associated with card issuance.

The usage of a central repository for the enrolled biometric data overcomes the drawbacks introduced by the *match-on-card* scheme. Since the space is not limited, the processing power is not limited to a simple smart card chip and much more powerful processing power and memory space can be employed during the verification of a biometric entity. Therefore, the use of central repositories are by far the more common of the two alternatives; however there is increased concern over the loss of *privacy* and potential misuse of biometric data held in central repositories. In this manner, it can be said, the *match-on-card* scheme and central repository schemes seem to complement each other. However, it is technically not convenient to use the two schemes at the same time since the addressed problem (storing information) is the same for both schemes. Therefore, the research goes in two diverse directions, *i*) increase the processing power of the smart cards or find better algorithms that will require minimal processing power and high accuracy or *ii*) finds solutions for ensuring the *security* of the biometric data residing on a central server, consequently preserving the *privacy* of the user and maintain the ability to use high processing power.

The term *security* is defined as the computational hardness to obtain the original biometric data from the data saved in the database [28]. On the other hand, the term *privacy* is difficult to precisely define, as it has different meanings in different contexts and cultures. The common denominator can be stated as keeping personal information, such as one's actions, whereabouts, or personal information, from others' view. Within the biometric domain, loss of privacy occurs if the biometric data is compromised or accessed to obtain unintended information about a person (such as their health condition). Loss of privacy also occurs if the biometric data is used to track individuals by linking biometric databases belonging to different applications. On the other hand, keeping

biometric data in smart cards has its own problems. In particular, it is not applicable to remote applications and forgers can claim that their card is broken and avoid biometric verification altogether.

While the privacy definition is elusive, biometric *template protection* is seen as a direct way to address privacy concerns and has been an active research area in biometrics for the last 10 years. Template protection refers to storing a transformed or modified version of a biometric template in such a way that it is impossible to reconstruct or reveal the original biometric template from the stored version. Ideally the protected biometric template need not be revealed and verification should be done in the protected template domain. This may be possible with one-way functions that are applied to both the reference and the query biometrics which allow matching to be done in the transformed space [29]. While this is a novel idea, finding such one way functions that are applicable to noisy/fuzzy biometrics has been challenging, along with the need to register the biometrics before applying the transform. Similarly, the biometric data can not be directly used as an encryption key within the framework of well-established cryptographic algorithms because of the noisy/fuzzy nature of biometrics. Providing *cancellability* and *renewability* are two other important properties. Since people can not change their biometrics as they can change their passwords, if the existing template is compromised, it should be cancelled or revoked, and ideally a new template is generated from the same biometric data. A good treatment of these concepts is given in [30].

1.3 Contributions

This thesis is concerned with the privacy protection and security of biometric templates. Biometric layering is proposed as a solution to this problem and is analyzed both theoretically and empirically. For the empirical tests, a state of the art fingerprint minutiae matcher is implemented to handle the cases where the minutiae orientations are modified for additional security.

The idea of layering multiple-biometrics has been suggested before [31, 32], although with limited experimental and theoretical evaluation that would show the viability of the system.

In this thesis, the mentioned works are extended by:

- introducing three new methods that aim to *i)* make it more difficult to separate the multi-biometric template into its constituent biometric samples (*Method₂*), *ii)* prevent the possibility of full leakage of the original template (*Method₃*) and *iii)* explore the limits of biometric layering with 3 modalities (*Method₄*);
- presenting new theoretical and experimental evaluation of security and privacy aspects of the proposed method;
- using state-of-the-art fingerprint matchers for improved results: one commercial ([33]) and the other one being the *TPS Matcher* as explained in *Chapter 3* in order to work with minutiae locations only (i.e. ignoring the minutia orientation information), as required in the algorithm;
- performing experiments on large and public databases (all subsets of FVC and NIST databases, as well as the TUBITAK MTRD Voice Database);
- achieving results that are close to the state-of-the-art verification performance using the FVC dataset, while demonstrating increased difficulty in cross-linking databases.

1.4 Thesis Organization

The organization of this thesis is as follows. In Chapter 2, the previous state-of-the art research on privacy preservation and protection for biometric systems is reviewed. The enhanced triplet based template matcher called *TPS Matcher* is described in Chapter 3 by providing experimental results with a common rolled-scanned fingerprint database (NIST). Then, the Biometric Layering (multi-biometric template fusion) method is described for two separate implementations (*i) using two fingerprints and ii) using a fingerprint and voice pass-phrase*) in Chapter 4 with four different variations in constructing the multi-biometric templates. The experimental results of the two implementations are provided and discussed in detail in Chapter 5. Finally, the strengths and weaknesses of the proposed system and the conclusions are summarized in Chapter 6.

Chapter 2

Related Work

Several schemes have been proposed in recent years for protecting the biometric templates [34? –37]: in particular the *fuzzy vault* [38], *fuzzy commitment* [35] and *biohash* [37] schemes are successfully implemented with many biometric modalities. However, research is active in finding better methods that provide template protection, while not inconveniencing the user or degrading system performance.

In one of the earliest works, Tomko proposed the use of biometric data as an encryption key that would be used to encrypt/decrypt his/her PIN number (of which there can be many) [39, 40]. In this way, the fingerprint, which uniquely identifies the person, is not stored in the database, eliminating any privacy concerns. Indeed, this would be ideal method, however obtaining a unique encryption key from a biometric data, such as a fingerprint, remains a challenge. Each impression of a fingerprint for instance is slightly different from another, due to many factors, such as cut marks, moisture, finger being pressed differently, different sensor types etc., making the task of key generation less than straightforward.

Ratha et al. [29] suggested a framework of cancelable biometrics, where a biometric data undergoes a predefined non-invertible transformation during both enrollment and verification phases. If the transformed biometric is compromised, the user is re-enrolled to the system using a new transformation. Likewise, different applications are also expected to use different transformations for the same user. While this work has been influential, finding one-way transformations that preserve distances has been elusive. Furthermore, managing the transform functions is also an issue. Those functions must

either be kept in a smart-card at the user’s possession or in a central database and protected with a user specific password. In these cases, a stolen card or password and a stored transformed biometric will lead to compromise. This framework also introduces the management of transform databases.

Among the practical template protection schemes is the *fuzzy commitment*, a secure key release scheme proposed by Juels and Wattenberg [35], which has been inspired by error correcting codes and has shed light to many research efforts afterwards. Their idea is based on error correcting codes, where the biometric template is seen as a “corrupted codeword”. Let c be a randomly selected codeword from a set W of evenly distributed codewords in a d dimensional space. Then a difference vector $\delta = t - c$ is calculated from a biometric template t and c . Then, the tuple $(h(c), \delta)$ is saved as the biometric record into the database, where h is a hash function. During verification, a probe template t' is used to obtain a probe word as $w' = t' + \delta$. Then c' , the closest codeword to w' is selected from W . If $h(c') = h(c)$ then the verification succeeds. The calculation of the difference vector and selection of the random codeword has been depicted in *figure 2.1*.

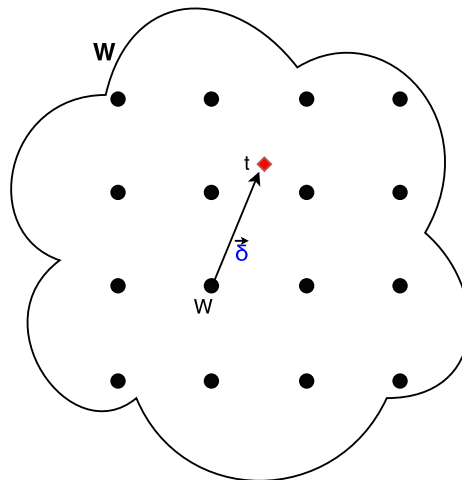


FIGURE 2.1: Random codeword selection and δ calculation in fuzzy commitment

In traditional biometric systems, the information is noisy and thus one cannot create exactly the same vector at each enrollment. Whereas, in fuzzy commitment, since biometric verification requires a fuzzy match, the two codewords will match if the error is small. In this sense, it can be thought of as a *cryptographic key release scheme*.

Fuzzy commitment is used in several studies. Hao et al. [41] have used *iris* biometrics to generate a repeatable and thus reliable cryptographic key up to 140 bits which is enough to be used in AES-128 symmetric encryption system. Bringer et al. seek for the best error correcting code and show that two-dimensional iterative min-sum decoding leads to results near the theoretical limits[42]. The enrollment and verification methods described in this study are inspired by and modified on the original Fuzzy Commitment. A random codeword c is selected in a Hamming space $\mathcal{H}(0, 1)^n$ and saved $z = c \oplus b$ in the database, where b is the biometric template obtained from the user. During verification, c is decommitted as $c = z \oplus b'$ which is $(c \oplus b) \oplus b' = c \oplus (b \oplus b')$. If the Hamming distance $d_{\mathcal{H}}(b, b')$ is small, recovering c is possible.

Juels and Sudan introduced the scheme called *fuzzy vault* which is another important template protection scheme [38]. The fuzzy vault is a general scheme to hide some data in a vault, such that it can only be released when a sufficiently matching data is provided; as such, it is very suitable for biometric template protection and indeed several applications have been implemented using fingerprints [43–46]; face [46]; and iris [45, 46]. To obtain a fingerprint vault, the minutiae are stored among a large number of chaff points that are generated to hide the minutiae, such that a user who provides a certain number of genuine minutiae points can unlock the vault.

Another important method is the *Biohash* scheme that projects the biometric features onto a lower dimensional space using a random key [37]. Randomness (and secrecy) of this key, that can be stored in a user-specific physical token, provides non-invertibility. Furthermore, matching accuracy increase is also gained, as the biometric signal is combined with an added source of entropy. However, (i) the need to store/access a random bit string which requires a token (with the well-known disadvantages of token-based authentication, such as loss, theft, etc. of the cited token) and (ii) the assumption that the keys are not known, are pointed out as the problems of these schemes [47].

The privacy protection and security methods provided above are focused on a single biometric modality (mostly fingerprint minutiae). There are also several studies that make use of multiple biometric modalities in order to create better biometric systems in terms of privacy protection and/or higher biometric authentication performance. Especially fuzzy commitment and fuzzy vault schemes have been extensively studied on multi-modal biometrics. We provide some of those works below.

Nagar et al. propose a framework for multi-modal template protection, which utilizes *secure sketch* and feature level fusion of participating biometric traits [46]. The work outlines building blocks of the framework and demonstrates preliminary implementations using fuzzy commitment and fuzzy vault based template protection for the iris, fingerprint and face multi-modal system.

Sutcu et al. [48] use fuzzy commitment in a multi-biometric system comprised of fingerprint and face biometrics. They use a method proposed in [49] to obtain a fixed length feature vector from fingerprint minutia and obtain face features using an *SVD* based algorithm. They finally perform a feature level fusion to obtain a combined template later used in Fuzzy Commitment scheme.

In [31], Yanikoglu and Kholmatov proposed to combine multiple biometrics in order to increase both privacy and security. Specifically, minutiae points from two distinct fingers of the same person were superimposed to create a multi-biometric template, which was shown to be more robust against privacy leaks. They also showed that the system provides higher level of security as well, because of the multi-biometric nature where the contribution of multiple biometric data or modalities introduced extra information to the verification phase, eventually increasing the performance of the overall system. However, the algorithm they used for verification does not use the orientation information which has an extreme significance in modern fingerprint matchers.

There exist several studies aiming to increase accuracy by applying fusion, at decision, score or feature level, with score level fusion being the most common method [9, 50–57]. However, the difference is that motivation in these works is increased security only, not template protection. In this thesis, we also provide a score level fusion test in parallel to the proposed method, which is based on feature level fusion, so as to measure the performance loss introduced to the system due to the fusion of the features.

Brunelli and Falavigna used the hyperbolic tangent for normalization and weighted geometric average for fusion of voice and face biometrics [51]. These modalities have also been fused by Ben-Yacoub et al., who considered several strategies such as support vector machines, tree classifiers and multilayer perceptrons [55]. Kittler et al. have experimented with fusion techniques of face and voice on the matching score level [56]. Hong and Jain proposed an identification system using face and fingerprint, where the

database was pruned via face matching before fingerprint matching [58]. The multibiometric scheme presented in this thesis will contribute to the literature as it effectively fuses multiple fingerprints and fingerprint and voice biometrics at feature level and benefits from a second biometric modality to conceal the first one for better cancelability.

The use of multi-biometric templates provides another alternative for template protection [31, 32, 59, 60]. In this approach, the template is constructed from multiple biometrics or one biometric is used to hide another biometric data, rather than using data hiding or cryptographic techniques.

Yanikoglu and Kholmatov proposed multi-biometric templates in order to increase privacy as well as security in [31]. They combined minutiae points from two distinct fingers of the same person using superimposition, creating a template with two biometric layers. The created multi-biometric template was shown to be more robust against privacy leaks. While multi-biometric systems were proposed for increased security before [9, 50–57], to the best of our knowledge, this was the first work that used multi-biometrics for increased privacy and template protection.

As an extension of this work, Camlikaya et al. combined fingerprint minutiae with a spoken password [32]. In this way, cancelability was introduced to the system; since the spoken password can be replaced, if the template is compromised.

Along this line of work, Othman and Ross proposed an approach for creating synthetic fingerprint images for a person, by mixing complementary phase components of two corresponding fingerprints [59]. The advantage of this method is that it can be easily integrated to any existing fingerprint verification system, where the created virtual fingerprints would be used for authentication instead of real ones. Mixing two different fingers from the West Virginia University database, authors report a rank-1 accuracy of $\sim 85\%$ and an EER of $\sim 6\%$ on a data set with a total of 500 fingers. In another experiment, they evaluated a property named *changeability* and showed that the mixed fingerprints do not match well (30% rank-1 accuracy) with the original ones. To evaluate cancelability, they ran matching and identification tests involving templates obtained from two impressions of the same fingerprint that were combined with 500 separate fingerprints. They obtained a high 85% identification rate, and 7% EER, showing the promise of the model, despite having similar templates in the gallery. One issue is

that to obtain realistic looking fingerprints, their constituents must pass a compatibility criterion.

In another work combining two fingerprints, Li and Kot propose an approach where the combined fingerprint template is created using minutiae locations of one of the fingerprints whose angles are replaced with ridge orientation angles from the other one [60]. The coupling between the minutiae and their replaced angles is performed after alignment of both fingers about their corresponding reference points. During verification, two candidate fingerprints are similarly combined and matched against the template, obtaining 0.4% false reject rate at 0.1% false accept rate using the FVC 2002-DB2-A database.

To evaluate privacy of their proposed methods, Li et al. defined two types of attacks based on their scheme: using the combined template to attack a database that contains (i) the first fingerprint (using the minutiae location correlation) and (ii) the second fingerprint (using the minutiae angle correlation). They call the two attacks *Attack Type A* and *Attack Type B* respectively. Using FVC 2002-DB2_A and generating databases of 100 combined templates, they report low rank-1 rates of 25% for *Attack Type A* and 57.5% for for *Attack Type B*, showing the promise of the system. The main issue with this technique is the need for detecting reference points, which may not exist or be located reliably. The main benefit of the algorithm is that it theoretically augments the number of possible enrollments for a person. However, the created template reveals minutiae locations and may thus be susceptible to cross linking attacks.

Finally, the *visual cryptography* method that decomposes a private image into desired number of noise like images (sheets), was applied to protect fingerprint, iris and face biometrics, by Ross and Othman [61]. When a predetermined number of sheets are superimposed, the encrypted image is revealed with some degradation in its quality; otherwise reconstruction is computationally hard. To assure privacy of corresponding biometrics the use of separate servers that would store constituent sheets is proposed. As can be deduced, the need for separate servers is the main technical drawback for that approach.

Chapter 3

Thin Plate Spline (TPS) Matcher

3.1 Overview

Many biometric systems use fingerprint biometrics as their authentication building block. Fingerprints are shaped by the ridges and valleys that resemble to a stream of regular liquid flow. This is due to the nature of the fingerprints as the cells that form them are randomly moved by the amniotic fluid during the fetal phase [62]. The ridges start and end at different locations harmoniously. These discontinuities of the ridges are called *fingerprint minutiae* [9].

There are two types of fingerprint minutiae. When a ridge ends at a certain point and forms a minutia, it is either forked and two new ridges are emerged from it, in which case the minutia is a *bifurcation*, or the ridge is simply finished and there is no continuation, in which case it is an *ending*. The fingerprint minutiae also emit other properties such as their $2D$ location and the angle of the ridge tangent at the minutia location (i.e. *orientation*). Consequently, a fingerprint minutia M is a $4D$ feature vector such that

$$M = (x, y, \theta, type)$$

where (x, y) is its location on the $2D$ coordinate system, θ is the orientation (in radians or degrees), and $type$ is a boolean (i.e. $type \in \{0, 1\}$) value indicating an *ending* or a *bifurcation*. A sample fingerprint annotated with two sample minutiae is given in *Figure 3.1*



FIGURE 3.1: A sample fingerprint and two minutiae

A common approach for fingerprint minutiae matching is to find the best alignment between two different minutiae sets and measure the similarity between the two sets [63]. A simple similarity measure is the number of *well aligned* minutiae pairs divided by the number of total minutiae in the two candidate sets. In other words, let A and B be the two minutiae sets to be verified against each other; then after an optimal alignment,

$$Score = 2 \times \frac{|Pairs|}{|A| + |B|}$$

where $|X|$ is the number of minutiae in set X [31]. Multiplication by 2 ensures a scale between 0 and 1.

There are also other score calculation techniques, such as using multiplication instead of averaging [64, 65], introducing additional similarity measures to the overall averaging fraction [66] and so on.

During fingerprint matching, most modern minutiae based matchers use the orientation information as a mandatory building block for their algorithm. The commercial *Nuerotechnologia (NT)* matcher that was employed throughout this work does not have a software mode, or a setting to disable the usage of orientation angles. Although the orientation information positively contributes to the performance of the matchers, in some cases that will be explained in the following chapters, this information needs to

be discarded. This requirement can be satisfied by a minutia matcher does not use the orientation information and works accurate enough to compensate the information loss.

The triplet based matcher that is proposed by Bazen and Gerez [65] has been chosen in this thesis as the best fit for the aforementioned requirement, because this novel approach is based on the comparison of minutiae triplets (triangles that are created with the minutiae) and does not need the orientation information during 2D point set registration. While the original study does not use the orientation information, the method has been improved here so that the minutia orientation information can still be included in the matcher for extra accuracy. This provides with the flexibility of enabling/disabling orientation check during tests.

Another novel side of Bazen and Gerez's work is the way it handles the elastic deformations that occur on fingerprints. The matcher uses Thin Plate Splines for modelling the elastic deformations that occur mainly due to the mapping of a 3D surface (i.e. finger surface) to a 2D plane (the surface of the sensor). The deformations become even more important when the user accidentally or intentionally skews her finger in an arbitrary direction as in *Fig. 3.2* during the enrollment.

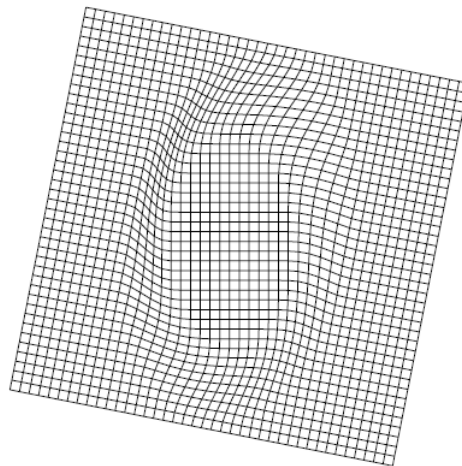


FIGURE 3.2: Elastic Deformation Model [1]

While adopting their baseline approach, in order to increase and speed, we provided improvements and introduced assumptions (e.g assume a maximum rotation of 45n both sides during fingerprint image acquisition)

3.2 Mathematical Background

TPS Stands for **T**hin **P**late **S**pline. It is a 2D analog of 1D cubic splines [67].

A linear transformation of an image can be described with a translation vector, a rotation matrix and a scaling matrix. The combination of the three matrices introduces an LTI system (T being Space here rather than time). Consider the following setup:

$$T = \begin{bmatrix} t_x \\ t_y \end{bmatrix}$$

$$R = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$S = \begin{bmatrix} s_x & 0 \\ 0 & s_y \end{bmatrix}$$

Combining all together, we will have an affine transformation matrix that performs the given operations at once on source points.

$$AF = \begin{vmatrix} s_x * \cos(\theta) & -s_y * \sin(\theta) & t_x \\ s_x * \sin(\theta) & s_y * \cos(\theta) & t_y \\ 0 & 0 & 1 \end{vmatrix}$$

The matrix given above can handle any kind of linear transformation as in *Figure 3.3*. However the problem becomes more complex when the transformation is not linear. In other words if there are nonlinear displacements on specific points, then we have to fit another model that will also handle these nonlinear warps in the grid.

This is where TPS modelling comes into play. When we have n source points called as *landmarks* on a 2D function and if we know their exact mapping as n target points called as *targets* on another 2D function, it is possible to model existing nonlinear deformations with TPS. In other words, if we warp a smooth surface by moving some arbitrarily selected points and create a new nonsmooth surface, we could model the deformation via TPS. In this sense, we define an interpolation between *landmarks* and *targets*. Although we may not represent the actual underlying function in the new mapping exactly, we

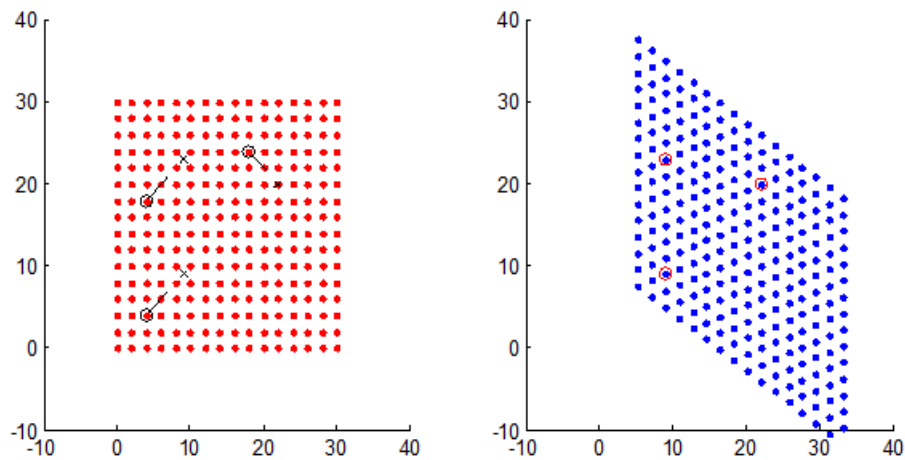


FIGURE 3.3: Simple Affine Transform (Only shear)

perform an approximation using TPS modeling. That is why the term Spline is used here. We are interpolating the predefined destination points so that we get an approximation.

TPS modelling provides an approximation that minimizes the bending energy defined on a surface as follows:

$$I(f) = \iint_{R^2} (f_{xx}^2 + f_{yy}^2 + f_{xy}^2) dx dy$$

In other words, we get the smoothest approximation that has one basis vector for translation, two for affine transform and at most n radial basis vectors that of each are defined by the *landmarks*.

The approximation function looks like:

$$f(x, y) = a_1 + a_x * x + a_y * y + \sum_{i=1}^n w_i * U(|P_i - (x, y)|)$$

where a_1 is translation vector, a_x and a_y are affine transformations and the rightmost term is the *weighted sum of the nonlinear deformation effect of each landmark on the current variable (x, y)*. $U(r) = r^2 \log(r^2)$ is the kernel function - the radial basis function. The P matrix constitutes of each *landmark* point as given below, and $|P_i - (x, y)|$ is the

Euclidean distance between *landmark* (x_i, y_i) and (x, y) .

$$P = \begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ \vdots & \vdots & \vdots \\ 1 & x_n & y_n \end{vmatrix}$$

The points given as (x_i, y_i) in the P matrix are the *landmarks* that cause the deformation to occur on the source surface. This can be imagined as placing an arbitrary number of pins on an elastic surface and moving each pin to a different location. If we have at most three pins, we will obtain an Affine transform. However, for at least four pins, we get a non-linear deformation and for each new pin, we have to put a new U - (*kernel*) into the equation.

As can be seen, the only unknowns in the equation $f(x, y)$ are the weights (w_i) of each non-linear components. We can obtain the unknowns using the *Least Squares* method. We know that every *landmark* has a specific effect defined by the $U(r)$ function, whereas we do not know how much this effect is.

To calculate the weights, we first have to represent the function in matrix notation and solve the obtained system. To do this we first define a K matrix as follows:

$$K = \begin{vmatrix} 0 & U(r_{12}) & U(r_{13}) & \cdots & U(r_{1n}) \\ U(r_{21}) & 0 & U(r_{23}) & \cdots & U(r_{2n}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ U(r_{n1}) & U(r_{n2}) & \cdots & \cdots & 0 \end{vmatrix}$$

where each of r_{ij} is the Euclidean distance between source *landmark* $_i$, and *landmark* $_j$.

We also define

$$\omega = \begin{vmatrix} w_{1x} & w_{1y} \\ w_{2x} & w_{2y} \\ \vdots & \vdots \\ w_{ix} & w_{iy} \\ \vdots & \vdots \\ w_{nx} & w_{ny} \end{vmatrix}$$

as the collection of weights for each $landmark_i$ and

$$W = \begin{array}{c|c} & \omega \\ & T \\ & AF \end{array}$$

where T is the translation t_x, t_y and AF is the affine transformation matrix. We also define the *targets* as

$$V = \begin{array}{c|c} \hat{x}_1 & \hat{y}_1 \\ \hat{x}_2 & \hat{y}_2 \\ \vdots & \vdots \\ \hat{x}_i & \hat{y}_i \\ \vdots & \vdots \\ \hat{x}_n & \hat{y}_n \\ \hline 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{array}$$

where each \hat{x}_i, \hat{y}_i is a point on the destination transformation that corresponds to $landmark_i$.

Next, we define matrix L as follows:

$$L = \begin{array}{c|c} & K \\ & P \\ P^T & \begin{array}{c} 0 \ 0 \ 0 \\ 0 \ 0 \ 0 \\ 0 \ 0 \ 0 \end{array} \end{array}$$

where $[P^T|0] * W = 0$ is the boundary condition for TPS which provides the energy minimizing factor. Now we are ready to express the function in terms of L , W and V which is indeed as follows: $L * W = V$. To solve this linear equation, we can invert the equation: $L * W = V \rightarrow W = L^{-1} * V$. Having obtained the W , we decompose it easily to ω , T and AF . T and AF provide three basis vectors. To compute the degree of freedom on ω , we can apply *Eigen Value Decomposition* on W . This will provide us the actual underlying nonlinear warping vectors. And the eigen vectors will represent the principal warps. The correspondence between the number of *landmarks* (n) and

the number of eigen-vectors (N) is as follows:

n	N
1	0
2	0
3	0
4	1
5	2
\vdots	\vdots
m	$m - 3$

The table above implies the fact that, when $n \leq 3$ there is no principal warp. But when $n > 3$ there should be at most $n - 3$ principal warps. That is because for $n \leq 3$ an affine transformation is sufficient to model the function.

3.2.1 Sample Applications with TPS Modelling

The first sample constitutes of only a shear (*See Figure 3.3*). In this sample, there are only three landmarks and three targets. Two of the landmarks move on the same direction with the same magnitude, whereas one of them moves down. Since we have three points, there is actually no nonlinear deformation here. The setup is represented as only a shear.

In the next sample there were 4 landmarks where 3 of them have been stabilized (i.e. kept in their position), and one of them moves along a direction. This causes a warp to occur in the direction of that moving point *See Figure 3.4*.

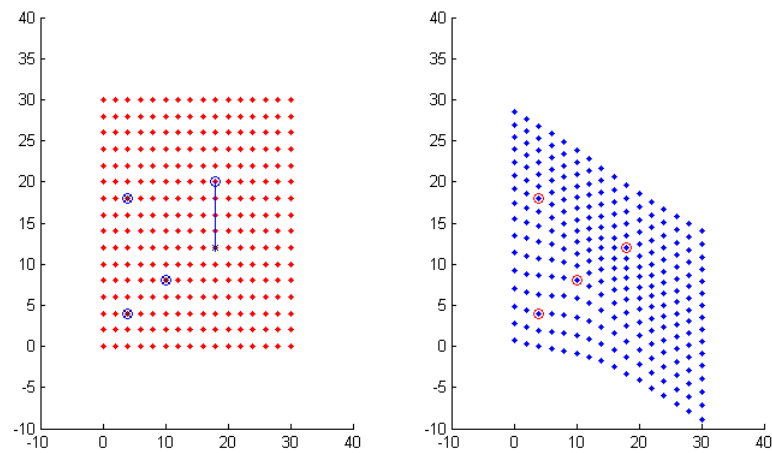


FIGURE 3.4: Three Constant, One Moving points

In the final example only one point remains stationary while others move randomly. The result is given in *Figure3.5*.

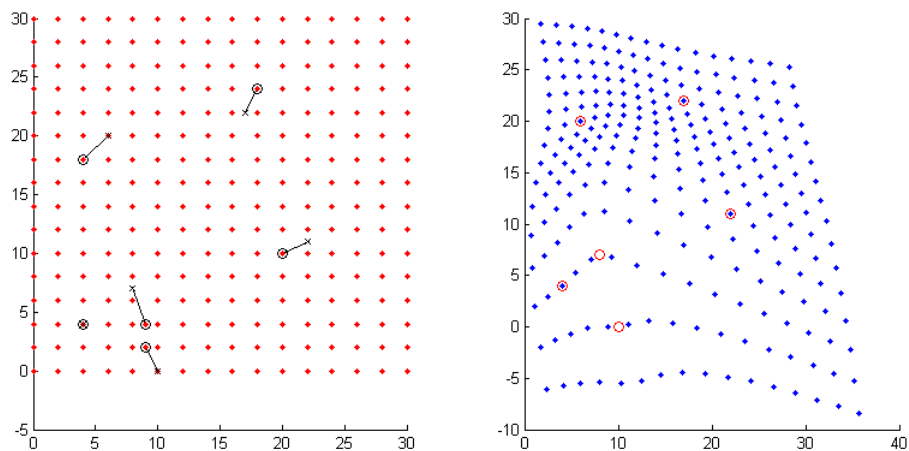


FIGURE 3.5: Extreme Warp

3.3 Minutiae Matching Using Thin Plate Splines

Another application of the TPS model, and as anticipated, the actual reason of adoption of this model is its application to fingerprint minutiae matching. The initial work was proposed by Bazen and Gerez [65], who provided a baseline algorithm to represent the proof-of-concept. We adopted and improved the algorithm both in terms of its logic

and implementation to handle larger databases faster. The TPS matcher works in two phases, namely Local and Global Matching.

3.3.1 Local Matching

Our algorithm is essentially a 2D point set registration and closest pair counting algorithm. Our points are fingerprint minutia set with their *location* (x, y) and *orientation* (θ) information. In order to find an optimal alignment between two different point sets we have to search and find the best alignment (registration) parameters, namely scale, rotation and translation. This operation is performed during the local matching phase in three steps.

Step 1: The minutia neighborhoods for each minutia in the target template (A) and the probe template (A') are determined. A neighborhood for a minutia m is defined as “the triangle that a minutia m creates using two of its close neighbors” (see Figure 3.6). We collect ten neighborhoods for each minutia as follows: Let $\{m_1, m_2, m_3, \dots, m_n\}$ be the neighbors of m in increasing Euclidean distance, the neighborhoods we choose are $\{m, m_1, m_2\}$, $\{m, m_1, m_3\}$, $\{m, m_1, m_4\}$, $\{m, m_1, m_5\}$, $\{m, m_2, m_3\}$... $\{m, m_4, m_5\}$. In fact the number of selected neighbors depends on the performance expectations and computational power. In the original proposal, the authors use the three smallest neighborhoods. Although this speeds up the algorithm, the verification performance does not meet the requirements of our multi biometric scheme. We compensated the speed decrease by modifying the original algorithm to work in a parallel fashion on multicore CPU's.

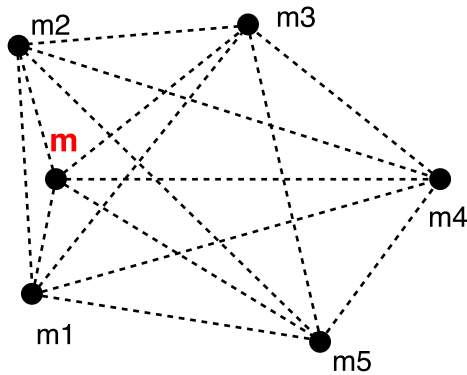


FIGURE 3.6: A minutia (m) and its five nearest neighbors forming neighborhoods (triplets-triangles).

Step 2: The neighborhoods of A are locally aligned to those of A' to obtain local registration parameters. For each comparison, a t (translation), r (rotation) and s (scale) triplet is calculated in a least squares manner and the triplet pairs that emit high alignment error are omitted. Another contribution to the original proposal is the different technique we apply for triplet pair alignment error measurement. In the original study, they omit the triplet pairs for which the sum of the squared distance between the corresponding minutiae locations and the difference of angles of minutiae is above a threshold. In addition to this, we also employ the geometric definition of triangular similarities to make sure that correct triplets are aligned. This is achieved by first calculating the *Edge-Angle-Edge Similarity* between triplets and ignore the ones that are not similar in the sense of a predefined threshold. Consider the example given in *Figure 3.7*; where the triangles $\triangle Y (y_1, y_2, y_3)$ at the lower left and $\triangle C (z_1, z_2, z_3)$ at the lower right corner are compared to the triangle $\triangle X (x_1, x_2, x_3)$ at the top of the figure. By *Edge-Angle-Edge Similarity*, we can conclude that $\triangle X \sim \triangle Y$ (i.e. $\widehat{x_1, x_2, x_3} \sim \widehat{y_1, y_2, y_3}$) whereas $\triangle X \not\sim \triangle Z$ (i.e. $\widehat{x_1, x_2, x_3} \not\sim \widehat{z_1, z_2, z_3}$).

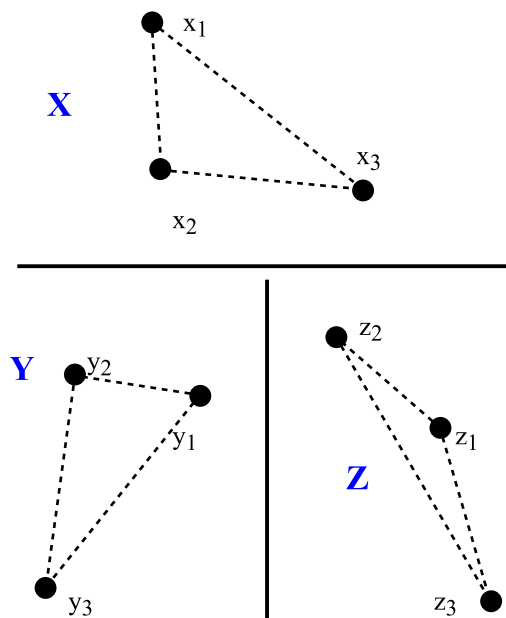


FIGURE 3.7: Three sample triangles compared in terms of *Edge-Angle-Edge Similarity*

As a result of this step a *selected parameter set*, that contains the candidate registration parameters (t, r, s) triples is accumulated.

Step 3: Finally the most voted translation, rotation and scaling values (t, r, s) are selected from the *good parameter set*. This is done by running a window for each of registration parameters. Then all the triplets that stay within the boundaries of the most frequent registration parameters are selected. The corresponding minutiae in all the triplets are considered as the matches and they are aligned in a least squares sense. At this point, we obtain the optimal global affine transform parameters, and are ready to perform global matching.

3.3.2 Global Matching

After the local matching phase, minutiae pairs are aligned via the optimal registration parameters. For each minutia in A' the nearest minutia of A that stays within a radius of $r = 15$ pixels is selected to be the match. Here an elimination is again performed using the angle values of the minutiae if the angles are configured to be checked. Then the *TPS model* is applied to A' where the *landmarks* correspond to minutiae in A' ; the *targets* correspond to minutiae in A ; and A' is warped onto A .

The application of *TPS model* is as follows:

1. For the *landmarks* on A' and the *targets* on A , a *TPS approximation* is applied, as described in *Section 3.2*.
2. The proximity radius (r) is decreased and the matches staying within the new r are counted and stored again for a new *landmarks* and *targets* set pair.

The above alignment and r reduction procedure is applied in a loop until the number of the minutiae within the radius for each *landmark* minutia converges.

The final matching score S_{tps} is calculated over the number of matches n as follows:

$$S_{tps} = \frac{n^2}{|A| * |A'|}$$

The advantage of applying the *TPS Model* is that it provides more robustness by handling the elastic deformations. Since Bazen et. al. performed bad quality fingerprint image elimination, providing results in comparison to their original proposal will not be healthy. However, in order to provide measurement of the contribution of *TPS Model* to the system, we provided a baseline implementation called the *Rigid Matcher*, that uses the same procedure in the local matching phase and differs in the global matching phase by only counting the matches for the *landmark* minutiae within their $r = 15$ pixel proximity for once (i.e. does not apply any *TPS modelling*).

Below we have provided figures for a *Rigid Matcher* vs. *TPS matcher* comparison. The figures belong to two imprints of the same subject taken from the *NIST Fingerprint Database* (See *section 5.2*). *i*) A figure with two non-aligned fingerprints given in *Figure 3.8*, *ii*) an alignment is done using the *Rigid Matcher* in *Figure 3.9*, and *iii*) another alignment performed via the *TPS Matcher* in *Figure 3.10*. It may be seen that in the TPS modelled matching scheme, the points are registered better.

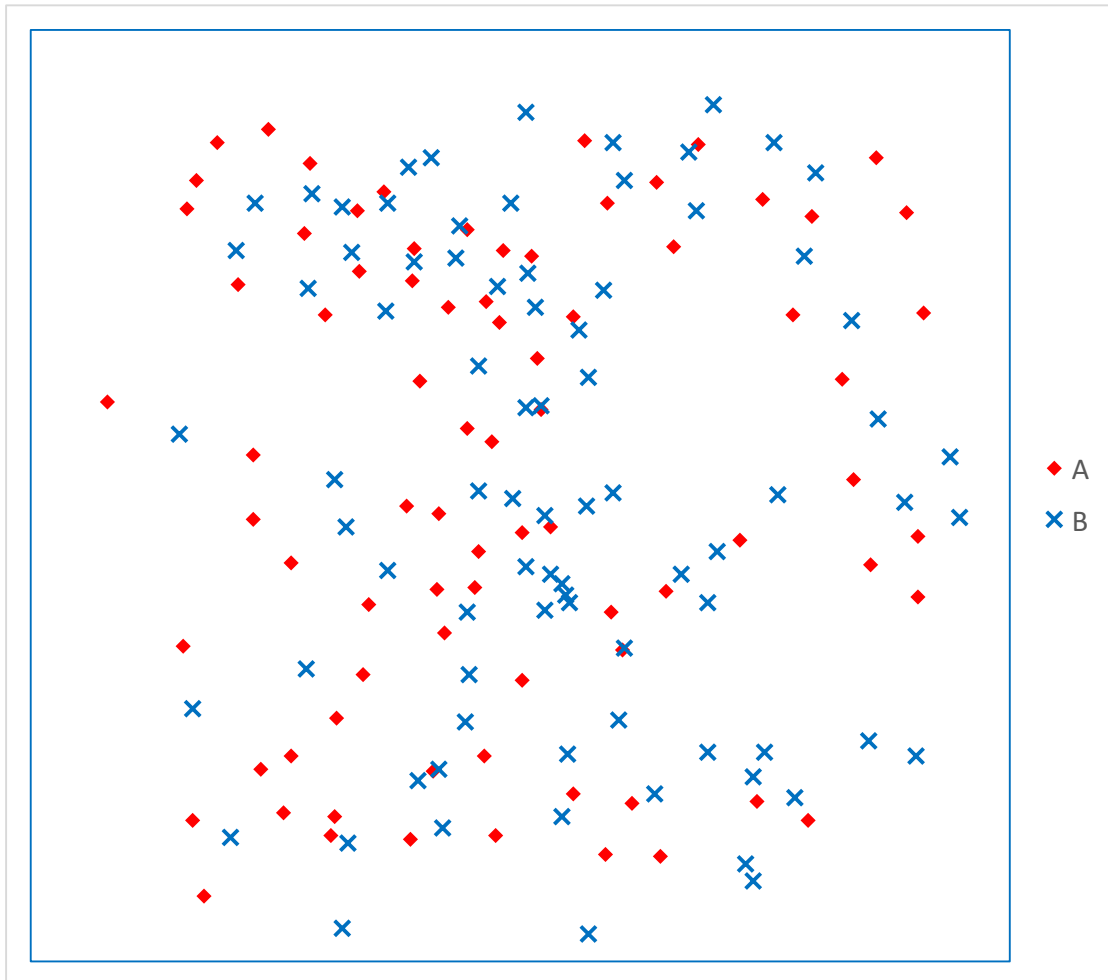
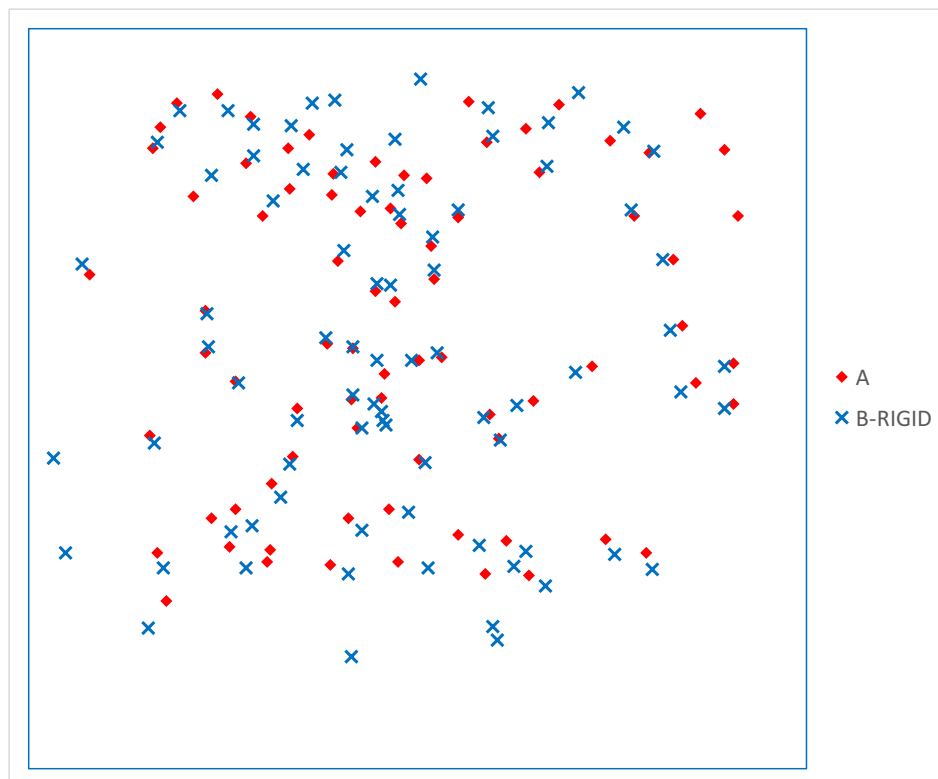
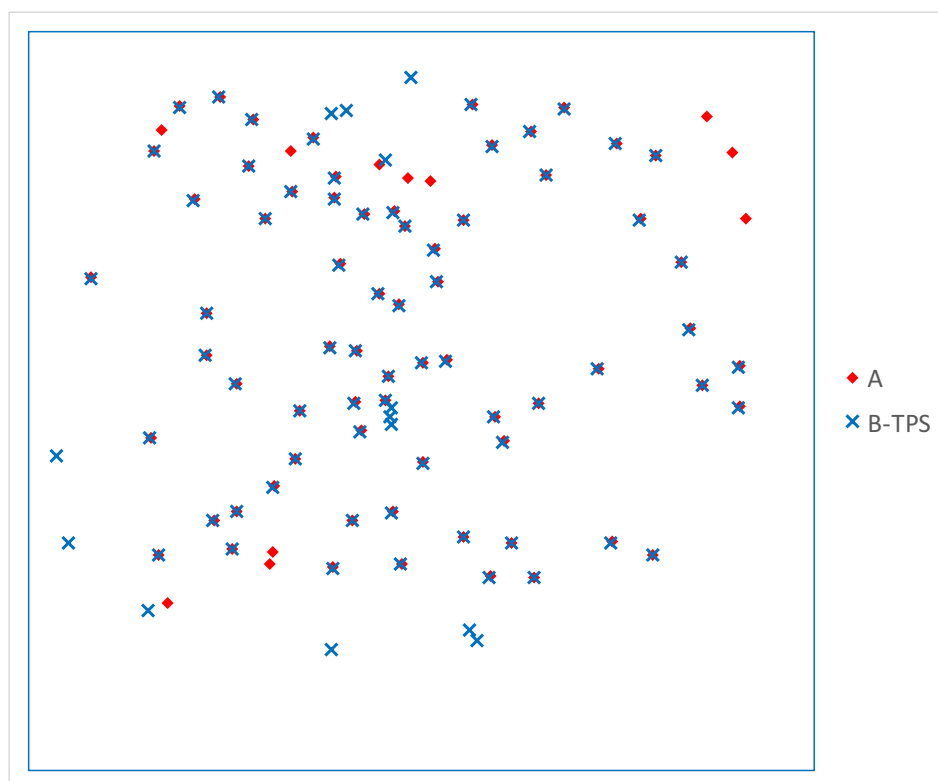


FIGURE 3.8: Non-Aligned fingerprints

FIGURE 3.9: Fingerprints aligned using *Rigid Matcher*FIGURE 3.10: Fingerprints aligned by using *TPS Matcher*

We performed a test on the *NIST Fingerprint Database* (See section 5.2) to measure the improvement of *TPS Modelling* by comparing the *Rigid Matcher* to the *TPS Matcher*. The selection of the NIST database was because the fingerprints in this database are rolled-scanned, which implies that we expect high amount of elastic deformations compared to a regular database such as *FVC*. We created a genuine test set of 2000 records and a forgery test set of ~ 100000 records.

The Rigid Matcher and the TPS Matcher performed an EER of 4.5% and 4.3% respectively. The experiment showed the superiority of TPS Modelling for handling the elastic deformations in fingerprint matching. The EER/FAR/FRR values of this test have been provided in *Table 3.1*. A ROC plot that shows the difference between the *TPS matcher* and the *Rigid Matcher* is given in *Figure 3.11*. We also provide the verification and identification performances of the *TPS matcher* in comparison to the commercial *NT Matcher* in *Section 5.4.2*.

Matcher	ERR	FAR	FRR
Rigid Matcher	4.5	3.0	6.0
TPS Matcher	4.3	2.7	6.0

TABLE 3.1: Error rates obtained from the Rigid vs. TPS Matcher on the NIST Fp. Database

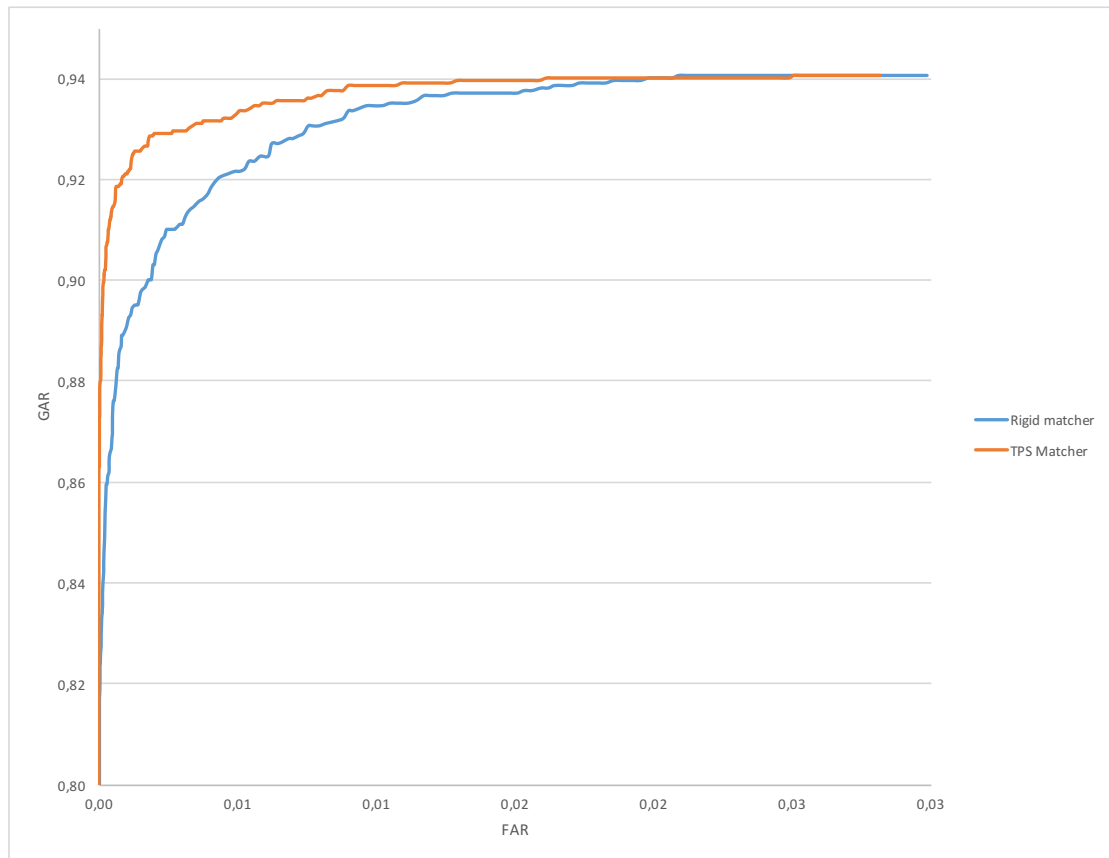


FIGURE 3.11: An ROC plot displaying the GAR-FAR performance of the *Rigid Matcher* and *TPS Matcher*

On a 4-core CPU, our *TPS matcher* has an average matching speed of 3 ms/match, (i.e a frequency of 330 matches/second).

Chapter 4

Biometric Layering with multiple biometrics

4.1 Overview

In this thesis, we propose a multi-biometric authentication framework to increase security of the biometric system and as well as the privacy of the enrolled biometric templates. The framework is based on feature level fusion of multiple biometric templates represented as fingerprint minutia. The main principle of the framework is to conceal the biometric of a person using another biometric, rather than a cryptographic construct to protect the constituent modalities.

In particular, we demonstrate two implementations of the proposed framework: one, combining multiple fingerprints and another one, combining one or two fingerprints along with a spoken password (voice biometric). With the latter implementation, one further obtains a cancelable template that can be renewed/reissued by simply uttering a different password.

As will be seen in *Chapter 5*, the proposed method, called *Biometric Layering*, is robust against privacy leaks and achieves a higher level of security due to its use of multiple modalities, in comparison to corresponding unimodal systems.

The proposed scheme consists of combining multiple biometric modalities into a single multi-biometric template, concealing the constituent biometrics within each other.

While the main aim is to protect the biometric data, the scheme also enjoys increased security for the overall system due to the multi-modal biometric paradigm. It can also be used to create different biometric templates for different security applications, by combining different constituent biometrics (e.g. two different fingerprints) for each application or by using behavioral biometrics that can be changed for each application (e.g. a spoken password). The scheme is based on the fact that without possession of genuine biometric data, it is computationally hard for a forger to separate the combined template into its constituent layers. Moreover, additional modification on the source template such as randomizing minutia angles and randomly deleting some minutia creates a securer multi-biometric template, at some cost in performance.

In one of the implementations shown in this thesis, two fingerprint minutiae sets are superimposed to form a multi-biometric template comprised of two biometric layers. In the second implementation, the first layer is obtained from a fingerprint and the second layer from voice, providing cancellability for the created templates. Furthermore, three biometrics are layered (three fingerprints or two fingerprints and a voice template) to explore the capacity of the proposed system.

The overall workflow of the system can be defined in two phases; namely *Enrollment* and *Verification*. In the *Enrollment* phase, the acquired biometric signals are processed and each one is converted into a set of feature points (e.g. minutia points of fingerprints) and mixed together to create the multi-biometric template. In the *Verification* phase, the user is verified when she presents query samples of each of the constituent biometric modalities; whose features are matched and removed from the multi-biometric template, each match resulting in a match score.

The matching scores obtained at each step are then linearly combined to obtain a final matching score. The overall process is depicted in *Fig. 4.1*.

The implementation is explained in detail for the case of multiple fingerprints in *Section 4.3*, and for fingerprints with a spoken password in *Section 4.4*. The fusion method for both cases is the same except for voice (as well as any other possible modality other than fingerprints) where an additional phase of *conversion of the raw biometric to fingerprint minutiae* takes place. The newly created template is called *voice minutiae*.

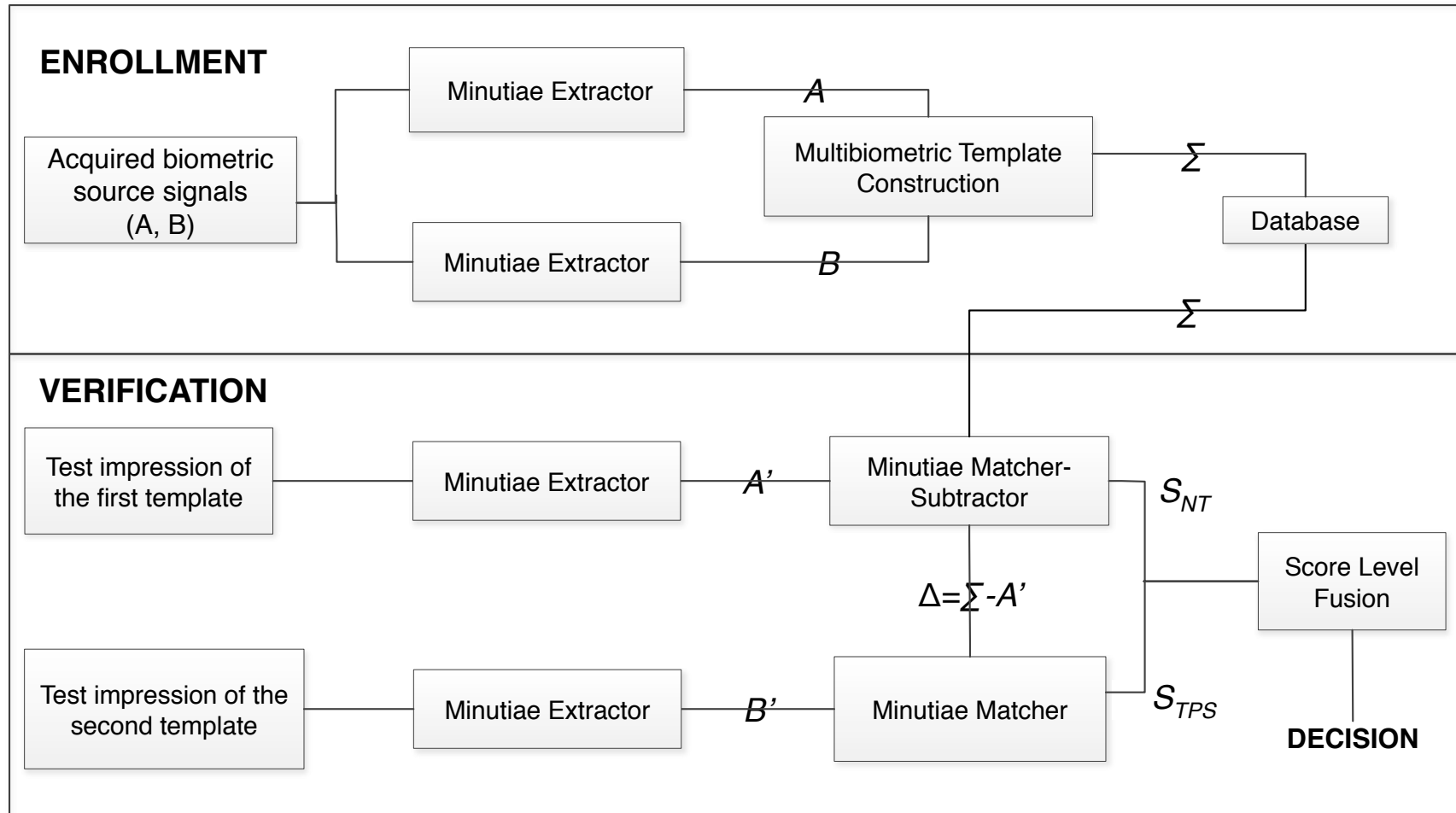


FIGURE 4.1: Overview of the proposed system.

4.2 Symbols

The symbols provided in this section are used consistently from Chapter 4 until the end of the thesis, in order to assist the reader with the coherence in the terminology. Symbols that are not included below, are explained immediately before they are used in their context. The list of symbols is given below.

- A : First minutiae set obtained from a fingerprint during enrolment.
- B : Second minutiae set obtained from a fingerprint during enrolment.
- Σ : Multi-biometric template created: $\Sigma = A \cup B$.
- A' : Second impression of the first fingerprint used in query.
- B' : Second impression of the second fingerprint.
- Δ : The remaining template after removing the first layer: $\Delta = \Sigma - A'$
- S_{NT} : Proprietary integral score returned by the NT matcher. It has a minimum of 0, a threshold value that mostly occurs on the range $[0 - 50]$ and no maximum. It represents the similarity between two different templates.
- S_{TPS} Fractional score obtained from the match with Δ vs. B' , using the TPS matcher (*Section 4.3.2*).
- S_{HD} Hamming distance score obtained from Δ vs. B' , when B and B' are voice minutia (see *Section 4.4.2*).
- $\mathcal{T}(S_{NT})$ A hyperbolic tangent function used for normalization of S_{NT} to the range $[0 - 1]$ so that it can be fused with S_{TPS} to obtain the final score (*Section 4.3.2*).
- $Method_1$: Template construction with the superimposition of two minutiae sets.
- $Method_2$: Template construction method with the superimposition of two minutiae sets where the second minutiae set is assigned pseudo-random angles.
- $Method_3$: The proposed method, same as $Method_2$ except for using only 75% of the minutiae from the first template (A).
- $Method_4$: Same as $Method_1$ except for using 3 fingerprints and 75% of each minutiae set.

4.3 Multi-biometric templates using multiple fingerprints

4.3.1 Enrollment

In order to achieve a successful enrollment, a person provides impressions from two different fingers, (i.e. A and B). Minutiae points defined by ridge endings and bifurcations on the fingerprint pattern are used as features (see Section 4.3.1.1). Then, the center of masses of the two minutiae sets are aligned and one set is superimposed on the other so as to minimize the number of the overlapping minutiae (see Section 4.3.1.2). Therefore, the created multi-biometric template (Σ) consists of two *biometric layers* and becomes the biometric ID/template of the person, stored into the database.

A sample biometric template is shown in Fig. 4.2, where the two distinct fingerprint minutiae templates A and B , given in a) and b) form the multi-biometric template. In c), the template Σ is obtained using superimposition (*Method₁*). In d), the template Σ is modified so as to hide the angles of B (*Method₂*). In e), the template Σ is modified so as to randomly contain only 75% of the minutiae of A (*Method₃*). '⊙' is used for A and '⊠' is used for B , but this information is only for visual depiction only and is not stored in the final template.

4.3.1.1 Feature Extraction

We extract and use minutiae points as the features representing a fingerprint. In our case, we only keep the 2-dimensional coordinates and the ridge orientation of a minutiae point, while other systems may use more information, such as the type of the discontinuity.

In the literature, there are several methods proposed for the automatic extraction of minutiae points [71, 72], which commonly follow well-known image enhancement, binarization, thinning and detection steps. This process can sometimes result in spurious minutiae; hence it is also common that minutiae points found through image processing operations are later verified using various post-processing techniques [73]. After minutiae extraction, minutiae alignment and matching steps are performed for two fingerprints. In this process, the main challenges are partial-overlap between two fingerprints and the non-linear deformation of the fingerprint that unevenly alters minutiae positions.

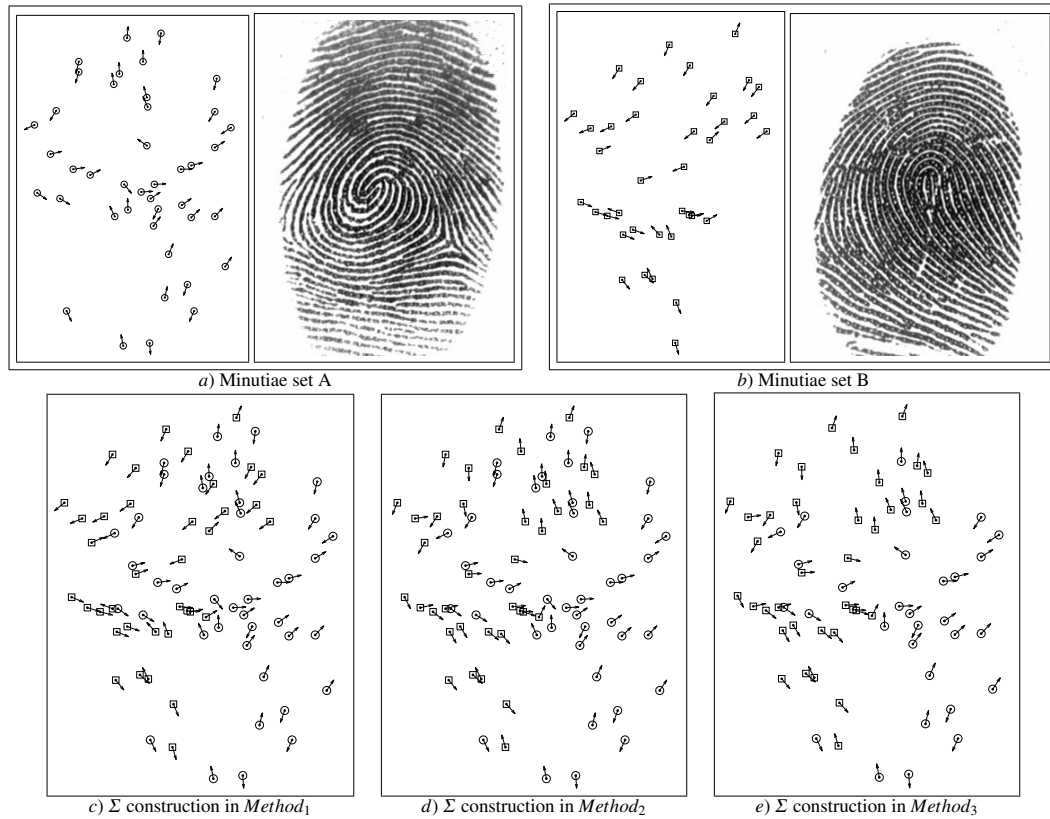


FIGURE 4.2: Sample multi-biometric templates

Please see *Chapter 3* where a matching algorithm that handles non-linear deformations has been provided.

Since the aim of this thesis is to demonstrate the concept of multi-biometric security and privacy, we preferred to use a commercial, state-of-the-art fingerprint minutiae extractor [33]. In this way, we can demonstrate real life feasibility of the proposed concept, while avoiding errors due to a sub-optimal feature extraction system. After the extraction process, all of the information, except the coordinates and ridge angles of the minutia (e.g. core type and location), are discarded in order to get *minutiae only* templates.

4.3.1.2 Multi-biometric Template Generation

The creation of a multi-biometric template (Σ) is a simple analytic process where the two minutiae sets (A and B) are mixed with respect to their x, y coordinates. The important issue in creating the multi-biometric template is that the constituent biometrics should

not be easily separated. In order to merge the two minutiae sets as much as possible, we follow these steps:

- Create an empty template that will include both A and B
- To minimize the number of overlapping minutiae in Σ , we translate B with respect to A by 50 pixels in each of the four directions. The translation amount was decided to allow some flexibility, while still overlapping the majority of the two minutiae sets.
- Superimpose the two minutiae sets (A and B) with respect to the optimal translation found in the previous step and store that combined point set as the combined multi-biometric template (Σ).

A sample multi-biometric template generated using this procedure is shown in Fig. 4.2.c, for two minutia sets shown in 4.2.a-b. This method forms the first and simpler template creation method (called *Method₁* from now on).

4.3.1.3 Hiding Angle Information

Considering that it may be possible to separate the minutiae of Σ into their corresponding source sets using the coherence of minutiae angles within local regions [74], we propose an alternative method for template generation. In this method, we use an extra step wherein the minutiae angles of the minutiae set B are replaced to mimic those of A . This method enhances the privacy of the user since it should be more difficult to separate the two fingerprint templates A and B apart.

In this method (called *Method₂* from now on), in addition to the template creation step given in 4.3.1.2, we take the following steps to replace the orientation angles of the B 's minutiae:

For each minutia m of B in Σ :

1. Find the minutiae of A within an arbitrarily chosen proximity of 30 pixels to m and create a histogram of their angles (L).
2. Quantize the angles of the minutiae in L to 8 directions and find the most frequent quantized angle as q .

3. Set m 's angle to a random angle in the range $[q-22.5, q+22.5]$ (A total range of 45° corresponding to 8 directions).

The perturbation is done so as to reduce the chances of clustering minutiae points of the same source fingerprint using minutiae angle coherence.

The multi-biometric template obtained in this way is shown in *Fig 4.2.d*. Note that this template is similar to the one generated by *Method₁* (shown in *Fig 4.2.c*) except for the modified angles of the second minutiae set.

It is important to note that the previous studies [31, 32] don't make use of minutiae orientation information during the verification step and therefore ignore this information. However, most modern minutiae based biometric systems use this information.

4.3.1.4 Using a Subset of the Minutiae

Modifying the angles of the second the fingerprint (B) makes it more difficult to isolate constituent fingerprints; something that could be done with some success, by considering minutiae angles [74]. However the minutiae of the first fingerprint (A) are used as is, in the multi-biometric template. Therefore, after a successful verification, this fingerprint is exposed to the system, to a large extent (except for extra and missing minutiae points resulting from an error-prone matching of the first template (A)).

To remedy this situation, in this section we propose a new method called *Method₃* that is identical to *Method₂*, except for the fact that it only uses a subset of A 's minutiae. In the experiments (*see Chapter 5*), we have tried using 50% and 75% of the minutiae points, with acceptable verification performance being obtained with the latter.

4.3.1.5 Layering Three Fingerprints

In order to explore the capacity of biometric layering, we propose a new method, *Method₄* that combines three fingerprints into one multi-biometric template.

In this method, 75% of the minutiae points in each fingerprint is used so as to prevent full leakage of any of them during a successful match. Since an attack in the form of separating the three fingerprints using minutiae orientation angle coherency, is deemed

very difficult if not impossible, the minutiae angle orientations are kept intact, unlike *Method₂* and *Method₃*.

The tests for *Method₄* are performed only with the FVC database, as the NIST database fingerprints contain very large number of minutiae points (average of 195 minutiae points, compared 32 in FVC database), so that combining three of them is not feasible.

4.3.2 Verification

When a subject is to be authenticated, she gives two query fingerprint impressions (A' and B') (and a third one as C' in case of *Method₄*). These impressions are matched against the combined template Σ . The matching is done by finding the correspondence between the minutiae of these two query fingerprints and multi-biometric template Σ :

Each query fingerprint is successively matched to and subtracted from the multi-biometric template. At each subtraction step, a matching score is obtained. Finally, all the matching scores are linearly fused to obtain a final matching score. The person is authenticated if the fusion of the scores obtained from the two steps is above a certain threshold. This process is depicted in *Figure 4.3*.

In *Step 1*, the Neurotechnology Fingerprint Matcher (*NT Matcher*) is used for matching A' against Σ . The proprietary match score S_{NT} is obtained for this first match and the matching minutiae are then removed from the template, unleashing Δ :

$$\begin{aligned}\Sigma \text{ vs. } A' &\longrightarrow S_{NT} \\ \Sigma - A' &\longrightarrow \Delta\end{aligned}$$

Step 2 continues with furthermore processing of Δ to produce the second ingredient of the final score (i.e. the TPS Matcher Score). The remaining template Δ is matched to B' using the *TPS Matcher* having been adjusted to ignore the orientations of the minutiae during the matching procedure. In fact, this is the reason for using different matchers for the two steps; the *NT Matcher* depends on minutiae angles for its successful performance, while the minutiae of the second fingerprint are modified in *Method₂*. The

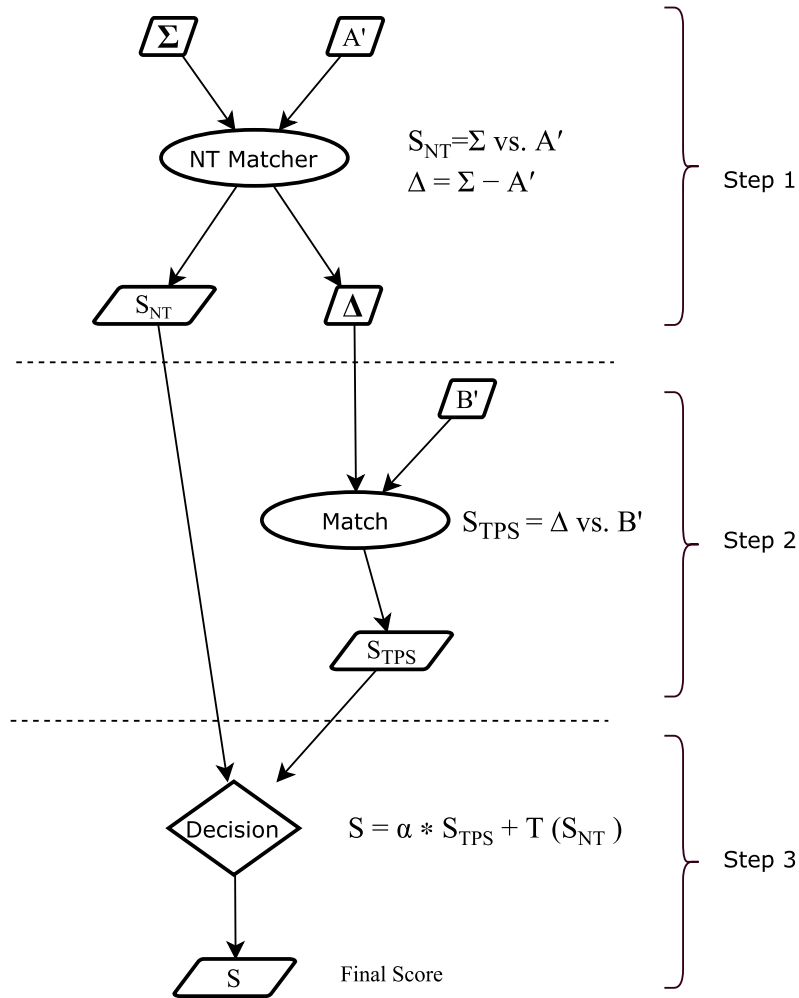


FIGURE 4.3: Verification Process

S_{TPS} score is calculated to measure the success of this second step.

$$S_{TPS} = \sqrt{\frac{|\Delta \cap B'|^2}{|\Delta| * |B'|}}$$

The $|\Delta \cap B'|^2$ is the the square of the number of matching minutia between Δ and B'

In the final step (*Step 3*) the final score is obtained by linearly combining the two match scores after normalizing S_{NT} , to bring it to the same scale with S_{TPS} :

$$S = \alpha * S_{TPS} + \mathcal{T}(S_{NT})$$

$$\mathcal{T}(S_{NT}) = \left(\frac{2}{1 + e^{\sigma * S_{NT}}} - 1 \right)$$

While the combination is essential to bring together all the sources of information, the accuracy is not very sensitive to the weighting coefficient α , and we have obtained the reported results with $\alpha = 1$.

In *Method*₄, the final score is the average of three matching scores from the *NT* matcher.

4.4 Multi-Biometric Templates Using Fingerprints and Voice

4.4.1 Enrollment

During the enrollment phase, the user submits a fingerprint and utters her selected password, from which minutiae points and voice minutiae are extracted respectively.

The main steps of the enrollment and verification stages are similar to the case of two fingerprints (see 4.3), except for their implementations. In particular, the extraction of the voice features from which voice minutiae are generated, as well as the template generation and matching stages, are described in the following sections.

4.4.1.1 Feature Extraction

The features employed in speaker recognition systems should successfully be able to define the vocal characteristics of the speaker and distinguish it from the voices of other speakers. Short spectra of speech signals give information about both the spoken words and the voice of the speaker.

Short-time spectral analysis is the most common way to characterize the speech signal [75]. Although, wide range of possibilities exist for parametrically representing the speech signal for the speaker recognition task, such as Linear Prediction Coding (LPC), perceptual linear predictive (PLP) codes [76] or maximum likelihood linear regression (MLLR) coefficients [77], Mel-Frequency Cepstrum Coefficients (MFCC) are perhaps the best known and most popular voice features used in speaker recognition. MFCC's are based on the known variation of the human ear's critical bandwidths with frequency [78]. Due to their representation capability and simplicity, we use the MFCC features of the enrolment pass-phrase, and use them in one layer of the multi-biometric template.

After all the spoken passwords are collected from the speakers, each utterance of every speaker is divided into 25ms frames with 10ms overlap and cepstral analysis is applied to each frame. As a result, each 25ms frame is represented by a 13 dimensional vector $\langle c_1, \dots, c_{13} \rangle$ consisting of MFCCs.

Since speech signals can vary in length, each password is then aligned with a Hidden Markov Model (HMM) of the corresponding password, in order to determine the correspondence between individual frames and phonemes. The HMM used for this alignment is obtained by concatenating previously trained, speaker- and text-independent phoneme models corresponding to the phonemes of the password. This way, each frame in each utterance is identified as one of the phonemes that may occur in the utterance of the passwords.

The global phonetic Hidden Markov Models used for the alignment are 3-state mono-phone phonetic models which have previously been trained using voice samples collected from various users. After this alignment, frames which correspond only to the middle (2nd) state are kept while the first and final (1st and 3rd) states of phonemes are deleted. This step is done to reduce the effects of noise and speech variations.

At this point, mean vectors of cepstral coefficients for each phoneme are calculated by averaging the 13 dimensional vectors representing the frames within the same phoneme (middle state). Hence, the n^{th} segment (middle state of a phoneme) is represented by a 13-dimensional mean vector F_n . During the training and testing phases for the system, mean vectors of the phonemes will be used instead of single frame vectors. The feature extraction process is shown in *Fig. 4.4*.

In order to finish the feature extraction phase, the aligned voice features are binarized by thresholding them using a global threshold depending on the gender of the claimed speaker. The threshold is chosen such that approximately equal number of zeros and ones occur in the binarized feature vector. When there are multiple training utterances for a person, a single binary feature vector is obtained by majority voting of all binary feature vectors extracted from all utterances.

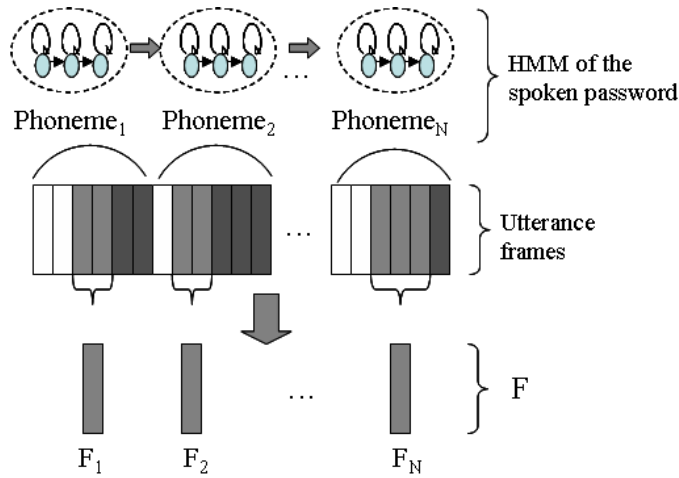


FIGURE 4.4: Feature extraction through HMM alignment of the MFCC features.

4.4.1.2 Minutiae Generation

For combining the voice features with the fingerprint minutiae, "voice minutiae", the points on the 2D Euclidean space, similar to fingerprint minutiae, are extracted. To achieve this task, the binarized voice features are divided into groups of 16 bits. Each group is then divided into two 8 bit numbers, namely (x, y) , defining a point on the 2D plane. This point set comprises the voice minutiae. The voice minutiae generation from the binary voice feature is shown in *Fig.4.5*.

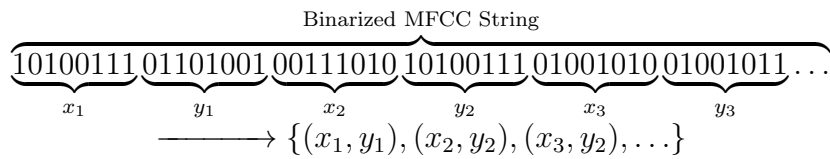


FIGURE 4.5: Transformation of the binarized MFCC feature into voice minutiae.

4.4.1.3 Multi-biometric Template Generation

The obtained voice minutia is scaled to match the width and height of the primary template and then combined with it as described in Section 4.3.1.2, with the fingerprint minutiae being A and the voice minutiae being B this time. The scaling step here is important; because the dimensions of the voice minutiae ranges in $[0-255]$, while the fingerprint minutiae coordinates may span a different, typically larger, range. Scaling thus guarantees that the voice minutia distribution is in the same range as the fingerprint

minutiae. Since we already know the size of the fingerprint templates, the scaling step is trivially undone during matching phase.

Since voice minutiae have no angle information, pseudo angles are assigned instead, as described in *Section 4.3.1.3*, in all methods. As a result, there is no *Method₁*. On the other hand, *Method₂*, *Method₃* and *Method₄* are exactly the same as with fingerprints except for the fact that voice minutiae is used instead of the last fingerprint.

4.4.2 Verification

During authentication, the user gives her fingerprint/s and utters the claimed person's password, which are then matched successively to the stored template. This scenario is a variant of the matching method explained in 4.3.2. The verification process is depicted in *Figure 4.6*.

In *Step 1*, the minutiae matched to the first fingerprint from Σ are deleted. This is done exactly the same way described in Section 4.3.2. For *Method₄* this subtraction is repeated for the second fingerprint as well, and the remaining minutiae in Δ are matched to the minutiae obtained from the query utterance. NT fingerprint matcher is used to match and remove the matching minutiae from Σ :

$$\begin{aligned}\Sigma \text{ vs. } A' &\longrightarrow S_{NT} \\ \Delta &= \Sigma - A'\end{aligned}$$

In *Step 2*, the remaining voice minutiae are transformed back into 8-bit binarized MFCC features, to match them to the feature vector obtained from the query password. For this, the coordinates of Δ is transformed (scaled down to) Δ_s , to undo the original scaling, using:

$$\begin{aligned}W &= \text{Width}(A), H = \text{Height}(A) \\ s_x &= \frac{256}{W} \\ s_y &= \frac{256}{H} \\ \Delta_s &= \Delta \times (s_x, s_y)\end{aligned}$$

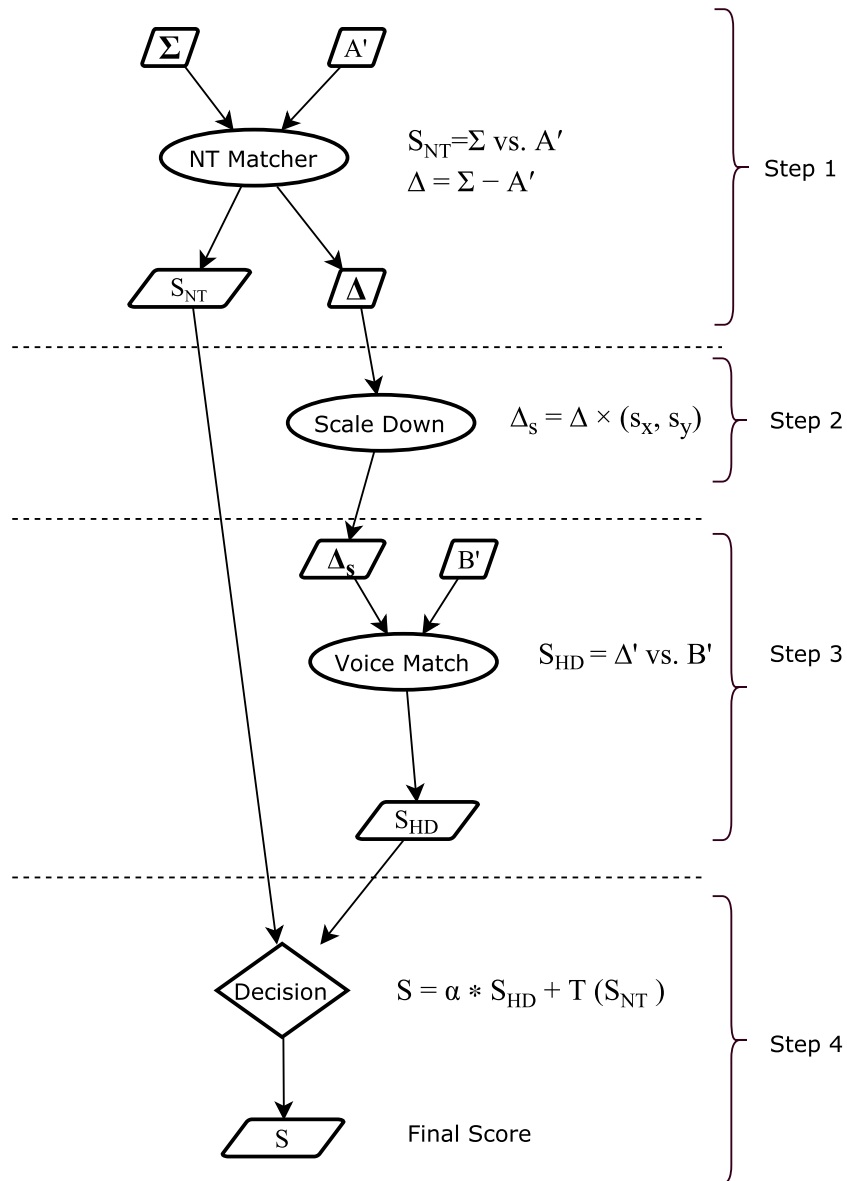


FIGURE 4.6: Verification Process for FP+Voice

In *Step 3*, the minutia coordinates of Δ_s (i.e. the (x, y) pairs) are bitwise concatenated as $x|y$ to obtain 16-bit sequences for all the minutiae in Δ_s . Note that since the relative order of these voice minutiae points are lost, every 16-bit sequence obtained from Δ is compared to every 16-bit sequence in B' using Hamming Distance and the sequences that emit the smallest distance are marked as a match. A distance of at most 3-bits of Hamming distance is considered a match and the ratio of the number total matches to the total number of the voice minutiae in Δ and B' form the matching score of this step (S_{HD}). For this matching phase, the Hamming distance is used, since the Euclidean Distance is not meaningful for comparison of bit strings.

$$S_{HD} = \Delta_s \text{ vs. } B'$$

Step 4 consists of the calculation of the final score S as a linear fusion of S_{HD} and the normalized S_{NT} 's obtained from the first step.

$$S = \alpha * S_{HD} + \mathcal{T}(S_{NT}).$$

Chapter 5

Evaluation

5.1 Overview

In this chapter the proposed multi-biometric layering method and its four different variants ($Method_{1-4}$) are evaluated in terms of their verification and identification performances, along with some measures of privacy enhancement. The method is implemented using two main models: i) multiple fingerprints and ii) fingerprint + voice and evaluated with four types of tests given below:

1. **Uni-modal System Performance:** These tests are performed to assess the baseline performance of matching algorithms employed in the proposed scheme, when applied to a single modality. Their results are compared against the multi-biometric tests in order to measure the performance enhancement of the proposed methods.
2. **Multi-modal Verification with the Proposed Scheme:** These tests measure the verification performance of the proposed schemes, where two query biometric samples (A' and B') are matched against the claimed multi-biometric template as described in *Section 4.3.2*.
3. **Multi-modal Identification with the Proposed Scheme:** In order to explore the identity discovery capabilities and the privacy protection power of the proposed scheme against attacks, genuine identification as well as identity search attacks (e.g. latent fingerprint attack) against a biometric gallery are applied with the

expectation of identification rates to be high and low for genuine and impostor searches respectively.

4. **Multi-modal Score Level Fusion:** Bio-layering method is based on the feature level fusion of the multiple biometric modalities represented as fingerprint minutiae. While it provides privacy and performance enhancements compared to a uni-modal biometric system, the feature level fusion of the biometric information is expected to introduce information loss compared to a multi-biometric system where the information is not mixed and is used separately. In order to evaluate the performance loss in this case, a multi-modal verification system based on score level fusion is implemented utilizing the same feature extraction and matching algorithms with the proposed system.

Using the results of the above evaluations, it is demonstrated that in terms of *technical performance*, as defined by Simoens et al. [30], the proposed framework achieves increased accuracy and privacy due to multi-biometric verification and encounters only a two-fold degradation in storage requirements and throughput, compared to the case of using a *single biometric* template, as a direct consequence of verifying two biometrics.

5.2 Databases

5.2.1 Fingerprint Databases

Three different fingerprint databases are used for evaluating the proposed system. First two databases are the FVC 2000 [2] and 2002 [3] databases, which are commonly used, including the public fingerprint verification contests. Each of these two databases consists of 4 subgroups (*namely DB1, DB2, DB3, DB4*), where each subgroup consists of 880 images (subjects(11) x fingers(10) x impressions(8)).

Sample images taken from FVC2000 and FVC2002 data sets are depicted in *Figures 5.1 and 5.2*, respectively. The properties of each subgroup for FVC databases are outlined in the *Table 5.1*.

	FVC 2000				FVC 2002				NIST
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4	
Sensor Type	Low-cost Optical	Low-cost Capacitive	Optical	Synthetic	Optical	Optical	Capacitive	Synthetic	Rolled&Scanned
Image Size	300x300	256x364	448x478	240x320	388x374	296x560	300x300	288x384	512x512
Num. Images	11 subjects \times 10 fingers \times 8 impressions								2000x1x2
Resolution	500 dpi					569 dpi	500 dpi		

TABLE 5.1: Fingerprint databases used in this thesis (FVC 2000,2002 and NIST).

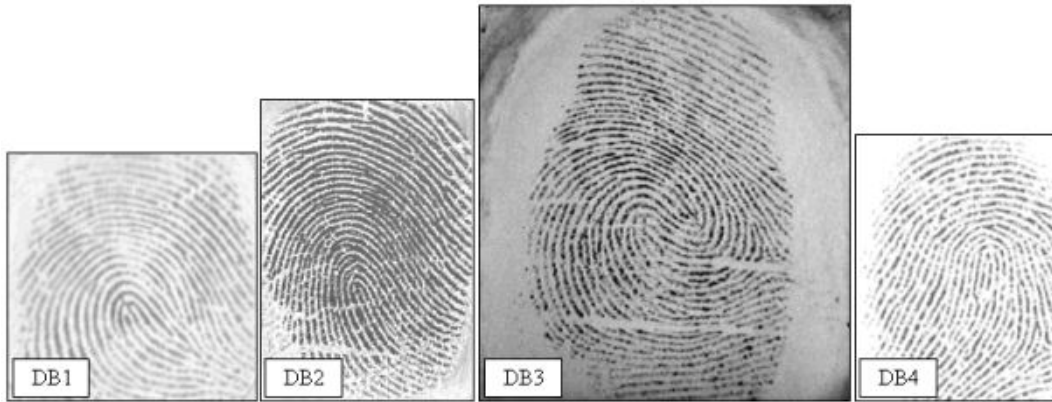


FIGURE 5.1: FVC2000 Sample images of four subgroups of FVC2000 [2].

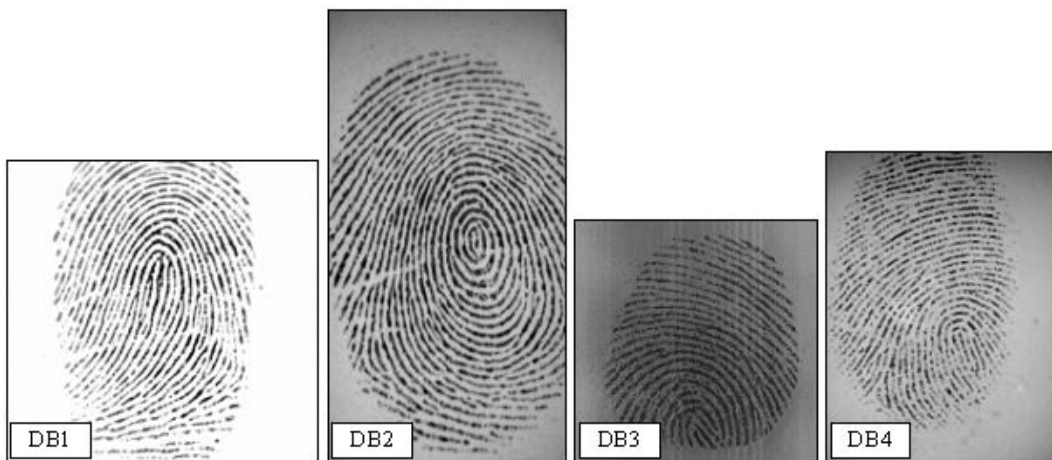


FIGURE 5.2: FVC2002 Sample images of four subgroups of FVC2002 [3].

The third data set used in the evaluations is the NIST's fingerprint database-4 [4]. In this database there are a total of 2000 subjects, where each subject has provided 2 impressions of only a single finger.

The main purpose of using the FVC databases is to measure the verification performance of the proposed method and compare it to the state-of-the-art, whereas the NIST database is used for the identification and cross-linking tests, as it includes more subjects compared to FVC data sets. Please see *Section 5.4.4* for further details.

5.2.2 Voice Database

The voice tests are performed using TUBITAK's speaker database [79]. The database is comprised of two subsets that differ by the types of the uttered phrases.



FIGURE 5.3: Two sample fingerprints from NIST fingerprint database-2 [4].

The first subset is the *Fixed Password Set* (FPS), which consists of 106 people (27 female and 79 male) all uttering the same numerical phrase 16 times. The phrase has been uttered as two three-digit numbers (815-364) both spoken in Turkish. The average number of voice minutiae obtained from this password set is 24; while the minimum and maximum number of voice minutiae obtained from the fixed password uttered by different people are 24 and 26, respectively.

The second subset, called the *Private Password Set* (PPS), consists of the same 106 subjects. In this set, each speaker has uttered his/her own name and surname 16 times (same names were replaced with a randomly selected different name). The average number of voice minutiae obtained from this password set is only 10, which is much smaller than the number obtained from the 6-digit fixed password string. This indicates that the names are much shorter on average, with the minimum and maximum number of voice minutiae obtained from the private passwords when uttered by different people are 7 and 18, respectively.

All utterances have been recorded in TUBITAK's semi-anechoic recording rooms utilizing the Roland UA-100 USB speech processing unit at 44100 Hz and 16-bit resolution in silent conditions.

Since the number of the minutiae points obtained from the voice data is small compared to the fingerprints, the fixed and private passwords of the users are employed in concatenation as well, to obtain longer voice samples. This set is referred to as *Combined Password Set* (CPS), in Tables 5.9 and 5.8.

	FPS	PPS
Language	Turkish	
Content	"815-364"	Subject's first and last name
Num. Subjects	107	106
Num. Samples	107 subjects \times 16 recordings	106 subjects \times 16 recordings

TABLE 5.2: Voice databases used in this work (TUBITAK Speaker Database).

5.3 Template Security and Privacy Evaluation

Using the biometric criteria defined in [30], the following claims that are explained here or in the subsequent experiments can be made:

- **Full-leakage irreversibility:** refers to the difficulty of determining, exactly or with tolerable margin, from the multi-biometric template, the biometric sample(s) or features used during enrolment to generate that template. Full-leakage irreversibility cannot be guaranteed with $Method_1$, as it may be possible to use minutiae angle coherence, using techniques similar to ones used in [80] to reconstruct the fingerprint image from minutiae angles. On the other hand, for $Method_2$ and $Method_3$, where the minutiae angle of the second template is modified, this requirement is satisfied as it is not feasible to split the multi-biometric template into its two constituent fingerprint minutiae sets since there are too many combinations to try in the absence of other information such as minutiae angles; and there is no way to verify that a successful split has been achieved. With these two schemes, the minutiae angle of the second template matches that of the first template locally, thus eliminating the potential use of minutiae angle information for finding the right split; or recovering the second template at all.

Altogether there are $C(2N, N)$ potential splits of the multi-biometric template into two equal parts, where N is the average number of minutiae in a single template. Hence the probability of finding the correct split is $1/C(2N, N)$. This number is roughly 0.56×10^{-18} for $N = 32$ which is the average number of minutiae in FVC fingerprint databases.

Moreover, in addition to modifying the angles of the second template (namely B), $Method_3$ randomly deletes a quarter of minutia in A while creating the multi-biometric template. Thus, both templates are modified in this method and it is

impossible to fully recover any of the individual templates. Since there will always be an uncertainty about the leaked information about the constituent biometrics even if the right split was found, the irreversibility is *unconditional*, according to the definition of [30].

As for *Method*₄, since only a portion of each of the constituent minutiae sets is used, it is guaranteed that there is no full leakage.

On average, only 55% of the minutiae points in the first matched template (*A*) are correctly identified during the verification step, as measured over the FVC dataset using *Method*₂ with two fingerprints. This is partly due to usual matcher errors and also the existence of the second template. Hence, it can be said that the original templates are not revealed fully, even after a successful matching step. Nonetheless, *Method*₃ is suggested to prevent this situation with certainty (all of minutiae points will not be revealed in full to the system that may potentially be unreliable).

- ***Authorized-leakage irreversibility***: refers to the difficulty of determining a biometric sample or features from the multi-biometric template, that would be useful for an attacker to break into an unprotected system (i.e. an unprotected uni-modal system).

The probability of one of the random splits to have K or more of its constituent minutiae points coming from the same fingerprint, when splitting a template with N points, is:

$$P(K) = \sum_{k=K}^N \binom{N}{k} p^k \times (1-p)^{(N-k)}$$

where p is 0.5. This probability is 0.0035 for $N=32$ and $K=24$ (if 75% or more of the minutiae in the chosen set is required to be correct); but drops sharply as K approaches N , as listed in *Table 5.3*.

K	P(K)
24	0.003500
25	0.001050
26	0.000270
27	0.000057
28	0.000010
...	...

TABLE 5.3: Probability $P(K)$ of K or more correct minutiae points in a given random split, for $N = 32$.

- **Revocability** is best seen as an aspect of operational performance that can be achieved by removing a compromised template from the system or by blacklisting it [30]. In this sense, the proposed system provides revocability.
- **Unlinkability** is demonstrated via cross-link tests involving templates sharing one of the constituent biometric samples and differing in the other (e.g. $\Sigma = A + B$ versus $\Sigma' = A' + X$). Moreover, uni-modal identification tests are done by cross-linking with an unprotected database (e.g. $\Sigma = A + B$ versus A'). Genuine identification rates are also reported as comparison. It is desirable for the system to obtain high genuine identification rates, while obtaining low cross-link and uni-modal search rates.
- **Renewability** refers to the ability to generate new templates from a biometric sample, in order to renew a revoked template. In this sense, renewability is available when the method is used with voice features; since the user can enrol with a new pass phrase to renew his/her biometric template. When the user provides a new pass phrase with a new impression of the subjects previous finger, it must be hard to link the new template to the old one. The cross-link tests given in *Table 5.9* with different voice templates provide a measure of how different the new template is from the revoked one. The low cross link rate (33%) shows that generating a new multi-biometric template by just changing the voice pass-phrase is quite successful. Renewability does not directly apply to the FP-FP method as the number of fingerprints of an individual is limited.

5.4 Evaluation Results Using Fingerprints (FP-FP)

5.4.1 Uni-modal Verification Results

The uni-modal verification performance results of the fingerprint matchers used in the proposed framework are reported here in order to establish the baseline performances of both the *TPS matcher* and the selected commercial fingerprint matcher from Neutechnology (*NT*) [33].

The reason for utilizing this particular commercial matcher is two-fold. First of all, it demonstrates the adaptability of the proposed framework to already available systems.

The other reason is that the *NT* has demonstrated a successful performance at FVC-2000 and 2002 evaluations, making it a good candidate to compare against. In particular, the average EER values reported for *NT* in FVC 2000 and 2002 are 1.37% and 0.99% respectively. The evaluations in this thesis show similar results for this matcher.

For these tests, all of the available impressions of genuine fingerprints are used in FVC2000 and FVC2002 databases. Since there are 110 different fingers and 8 impressions per finger in each database (11 persons \times 10 fingers), matching all impressions of the same finger to each other results in 28 genuine tests per finger. This gives a total of 3080 ($= 110 \times 28$) genuine tests for each FVC group. As for forgery tests, for each FVC group, every first impression of all the fingers is matched to the first impressions of all the other fingers, resulting in 5995 ($= 110 \times 109$) forgery tests.

The top two rows of *Table 5.4* indicate the *NT* and *TPS matcher* performance on the FVC and NIST databases, with an average EER value of 1.9% versus 3.7% for the FVC databases, respectively. The *NT* system has state-of-the-art performance and the *TPS matcher* has a moderate performance and is included here for completeness. In the proposed system, the *TPS matcher* is only used when the *NT* matcher does not perform well; namely when matching minutiae sets for which the angles are modified.

In that case, performance results are lower as expected: the average EER increases by about a factor of two for each database, becoming 7.5% and 9.7% for the FVC and NIST databases, respectively. The results for the case of modified angles are not reported for the *NT* system as it does not have an option to disregard the minutiae angle information.

Methods	FVC 2000				FVC 2002				FVC Avg.	NIST
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4		
UMV- <i>NT</i>	2.4	1.1	4.7	1.6	0.7	1.4	2.1	1.4	1.9	2.8
UMV- <i>TPS</i>	3.6	2.3	7.1	5.1	2.0	1.8	5.2	2.8	3.7	4.3
UMV- <i>TPS-NAI</i>	8.8	5.8	13.3	7.3	4.5	4.4	10.0	6.3	7.5	9.7
MMV- <i>Method</i> ₁	0.9	0.1	1.4	0.4	0.1	0.1	1.9	0.4	0.5	4.6
MMV- <i>Method</i> ₂	3.6	1.0	5.0	1.8	0.6	0.3	3.1	1.1	2.1	9.0
MMV- <i>Method</i> ₃	5.1	2.1	7.6	4.1	2.3	0.8	5.8	3.3	3.9	12.2
MMV- <i>Method</i> ₄	3.8	2.9	5.3	3.1	2.9	2.9	3.1	3.0	3.4	-

TABLE 5.4: Verification performance (% EER) with FP-FP layers.

Methods	FVC 2000				FVC 2002				FVC Avg.	NIST
	DB1	DB2	DB3	DB4	DB1	DB2	DB3	DB4		
<i>Multi-modal SLF</i>	0.4	0.0	1.0	0.4	0.0	0.0	0.8	0.0	0.3	1.2
<i>SLF (NAI)</i>	0.8	0.4	3.2	1.2	0.0	0.0	2.0	0.8	1.0	1.8

TABLE 5.5: Verification performance (% EER) of a multi-biometric system with score level fusion.

5.4.2 Multi-modal Verification Results of the Proposed Scheme

The lower part of *Table 5.4* reports the verification rates for the proposed scheme where multi-biometric templates are created with two fingerprints, using all four methods described in *Section 4.3*. *Method₁* constructs the template by simple layering, while in *Method₂* and *Method₃* the minutiae angles of the second constituent fingerprint are replaced, with or without using all the minutiae points, respectively. Finally, *Method₄* explores the capacity of biometric layering by combining three biometrics into one multi-biometric template.

For these tests, a gallery of 55 templates is created for each FVC subgroup, by pairing each two consecutive template into one multi-biometric template. As for the NIST database, it is possible to create a gallery of 2000 multi-biometric templates by following the same strategy used for each FVC subgroup. However, to accommodate cross-link tests as well, a gallery of $2000/3=666$ templates was created to be used in verification tests.

As can be seen in *Table 5.4*, using *Method₁*, the proposed method provides a 0.5% average EER over the eight FVC datasets on average, which is significantly better than the state-of-the-art uni-modal performance of the *NT* system.

Using *Method₂* that provides higher template security, the results are close to the state-of-the-art uni-modal performance, with 2.1% average EER on the FVC database. With *Method₃* and *Method₄* that trade verification performance for additional template security, the results are 3.9% and 3.4% average EER on the FVC datasets, respectively.

For all three methods, there is a significant decrease in comparison to the uni-modal systems, when using the NIST database. This can be explained by the fact that the fingerprints in the NIST database typically contain a very large number of minutiae points (195 versus 32 in FVC databases, on average), which causes a higher number of minutiae collision during multi-biometric template creation. *Method₄* was not tested with this database, because it was not deemed suitable due to the large number of minutiae points in the fingerprints in this database.

Although, there is performance degradation when using *Method₂* and even more in *Method₃*, compared to *Method₁*, the minutiae angle replacement and additional random removal of minutiae from the first template provide a stronger template security and resilience to privacy threats, which is discussed in *Section 5.4.4*.

An observation was that in the first match (Σ vs. A'), on average, 92% of all matched minutiae are correct, while 8% of the matched minutiae come from the second fingerprint, as calculated over the FVC datasets using *Method*₂. On average 55% of the minutiae points in A are correctly identified. Hence, the first match performance can be summarized as 0.92 precision and 0.55 recall.

DET plots for the performances of the three methods are given in *Figure 5.4*, along with uni-modal systems. In order to facilitate a better comparison of the performances of *NT* to *Method*₂ and *Method*₃ on FVC-2000 and FVC-2002, DET graphs are provided *Figures 5.4-a,c and 5.4-b,d* respectively. It can be observed from these two figures that the proposed schemes provide a verification performance comparable to the state-of-the-art uni-modal performance of the *NT* system.

As reported, the multi-modal matching performance for *Method*₁ are higher than *Method*₂ and *Method*₃ for all different *FAR* vs *GAR* data points.

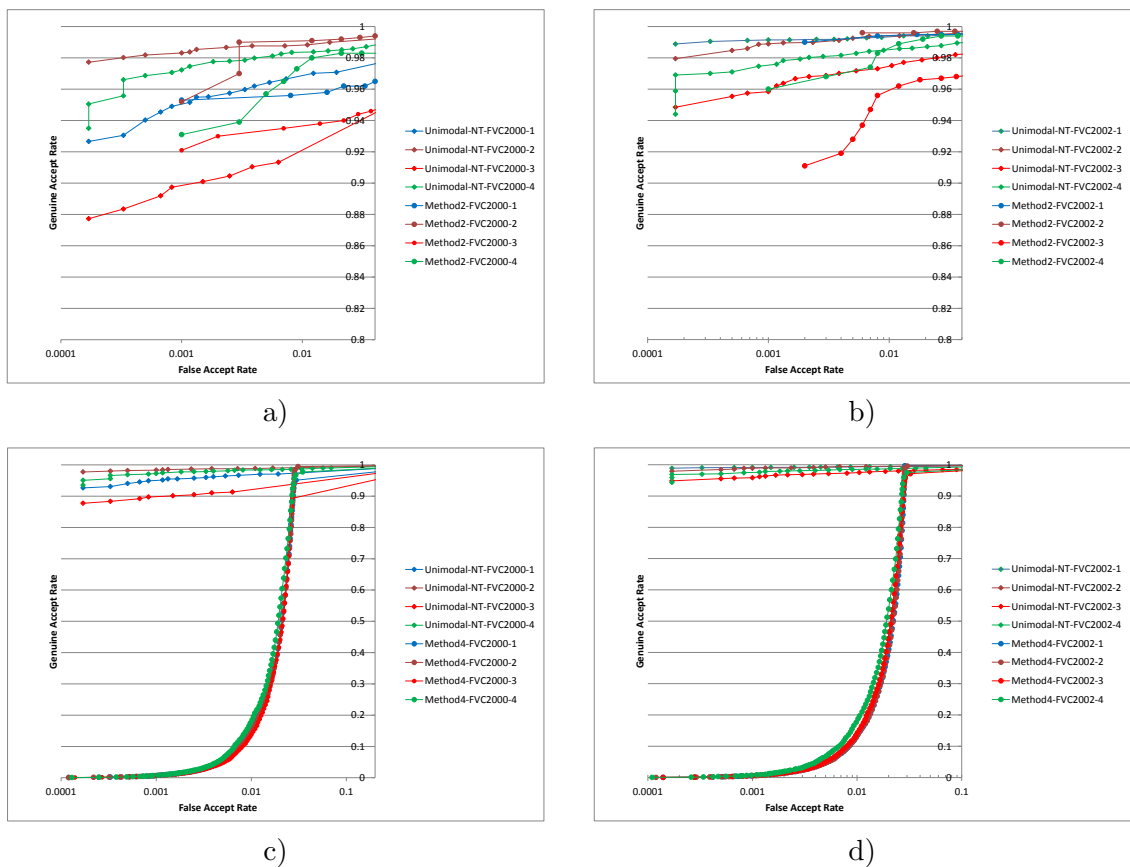


FIGURE 5.4: DET Plots for the uni-modal and suggested multi-biometric system with FP-FP layers for FVC 2000 in (a,c) and FVC 2002 in (b,d). For ease in comparison, corresponding plots share the same color, with different markers.

5.4.3 Multi-modal Score Level Fusion

For the sake of completeness and comparability with other multi-modal approaches, a multi-modal verification system using a simple score level fusion is also implemented using the *TPS Matcher*. Everything in this system is done the same way as for the proposed system whenever applicable. For instance the same feature extraction and matching algorithms are used as in the proposed system. During matching, two alternatives are tested in line with the proposed method: using the minutiae angles or ignoring them. In either case, the match score between two fingerprint templates is calculated as the ratio of the matched minutiae in the reference fingerprint. The individual scores obtained from the two matches are linearly combined for the final decision.

The EER results shown in *Table 5.5* are the lowest error rates for both the FVC and NIST databases, with 0.3% and 1.2% EER, respectively. The success of the fusion system is as expected, because on one hand it benefits from twice the discrimination power of two fingerprints (i.e. the multi-biometric nature) and on the other hand, it does not sacrifice anything for the sake of privacy and template security. The performance degradation that comes with the lost angle information in the fusion system (1.0 versus 0.3% for FVC) parallels that observed with the proposed schemes.

		GID	UMS		Cross Link Search	
		Σ vs. (A', B')	Σ vs. A'	Σ vs. B'	$\Sigma = (A + B)$ vs. $(A' + X)$	$\Sigma = (A + B)$ vs. $(X + B')$
<i>Method</i> ₁	Top-1	93	75	75	21	32
	Top-5	93	75	75	37	39
	Top-10	93	75	75	38	39
<i>Method</i> ₂	Top-1	82	74	40	20	10
	Top-5	85	75	46	33	16
	Top-10	86	75	51	34	19
<i>Method</i> ₃	Top-1	79	58	48	1	37
	Top-5	82	59	55	5	47
	Top-10	83	59	60	6	50

TABLE 5.6: Identification and cross-link results for the NIST gallery consisting of 666 multi-biometric templates with FP-FP layers.

		GID	Uni-Modal Search			Cross Link Search		
		Σ vs. (A', B')	Σ vs. A'	Σ vs. B'	Σ s. C'	$\Sigma = (A + B)$ vs. $(A' + X)$	$\Sigma = (A + B)$ vs. $(X + B')$	$\Sigma = (A + B + C)$ vs. $(A' + B' + X)$
<i>Method</i> ₁	Top-1	99	93	92	-	82	85	-
	Top-5	99	94	93	-	84	86	-
	Top-10	99	95	95	-	87	88	-
<i>Method</i> ₂	Top-1	97	96	81	-	85	5	-
	Top-5	98	96	82	-	87	16	-
	Top-10	98	96	96	-	90	29	-
<i>Method</i> ₃	Top-1	96	83	74	-	53	6	-
	Top-5	98	86	81	-	60	16	-
	Top-10	98	87	87	-	67	30	-
<i>Method</i> ₄	Top-1	100	76	77	77	-	-	63
	Top-5	100	78	80	79	-	-	68
	Top-10	100	80	83	82	-	-	75

TABLE 5.7: Identification and cross-link results for the FVC gallery consisting of 55 multi-biometric templates with FP-FP layers (36 Templates in *Method*₄).

5.4.4 Template Security and Privacy Test Results

Irreversibility, revokability, and renewability issues were addressed theoretically in Section *Section 5.3*; here the results of three types of tests are reported to demonstrate unlinkability, by showing decreased success in cross-link rates in comparison to genuine identification rates:

- Genuine identification- Σ vs. (A', B') : The aim of this evaluation is to measure the genuine identification rate of the system, when the multi-biometric template is searched using a genuine pair of query fingerprints within a gallery of templates. The identification is performed by sequentially matching the query pair to each of the multi-biometric templates in the gallery, using the method described in *Section 4.3.2*.
- Uni-modal search attack- Σ vs. A' , Σ vs. B' or Σ vs. C' : This attack measures how easily one can identify a person's template having only one matching fingerprint. Since the roles of all the fingerprints used in the template are not symmetric, the scenario is evaluated separately for the first, second and third templates, using the commercial *NT matcher*. Searching with the third template (C') is only meaningful for *Method₄* where the multi-biometric template consists of three layered fingerprints and the attacker has access to an imprint of the third fingerprint.
- Cross-link attack- $\Sigma = (A + B)$ vs. $\Sigma' = (A' + X)$ or $\Sigma' = (X + B')$: This is an attack scenario where the attacker is assumed to have access to two different multi-biometric databases and would like to find corresponding identities. During this attack, each multi-biometric template of a database is matched to all templates of the other database, as if they are uni-modal templates. In this attack scenario, corresponding templates may share the first fingerprint (A) or the second fingerprint (B), as in the two uni-modal attack types. Cross-link attack is also used to measure how different a new template is from a revoked one if the secondary template is a voice pass-phrase.

Identification of a correct template with only a single fingerprint is undesired, as it would lead to the identification of the user by searching with a latent fingerprint, or cross-linking with an unprotected database. Similarly, if a user is enrolled in multiple

databases, cross-linking may identify which templates in the two databases belong to the same person, posing a privacy threat.

FVC and NIST databases are used throughout these evaluations, with results given in *Tables 5.7 and 5.6*. While both databases are commonly used in the literature, they both present some challenges for these tests. The FVC database is very small to run multi-biometric tests (especially cross-link tests), while the NIST fingerprints contain very large number of minutiae points, which is not very amenable for the proposed method. Nonetheless, all the tests are included for both databases as applicable, with the only exception that *Method₄* is omitted on the NIST database.

To maximally use the NIST database, the 2000 fingers are grouped such that 3 fingers are used as if they belong to the same user. The two fingerprints (A and B) of one user are used to construct one multi-biometric template for the main gallery, for which the matching impressions (A' and B') are used for genuine identification and uni-modal search tests. Then, a third fingerprint (X) from another user is used to create two matching galleries ($A' + X$ and $X + B'$). In this way, a total of $2000/3=666$ multi-biometric templates are obtained in the three matching galleries.

Since there are only 11 subjects and 110 different fingers in each of the FVC subgroups, the genuine identification and uni-modal search attacks are run with a gallery of 55 templates, obtained by pairing fingerprint pairs (i.e. two-by-two), for each subgroup. For cross-link tests, the fingers are paired in triples (i.e. 3-by-3 such that 3 fingers are used as if they belong to the same subject), as was done for the NIST database. In this way, a very small gallery of 36 templates is obtained.

As an evaluation metric, the percentage of cases where identification returns the correct template among the top- k candidates is reported for top-1, top-5 and top-10.

During the fingerprints matching tests, the state-of-the-art *NT matcher* is used whenever possible, in order to obtain the most competitive results; however this matcher performs poorly when the minutiae angle is missing. Hence, the *TPS matcher* is used when angle information is missing or altered; namely in matching B and B' , in *Method₂* and *Method₃*.

For the larger NIST gallery, genuine identification rates of 93%, 82% and 79% are achieved using *Method₁*, *Method₂* and *Method₃* respectively, showing the premise of the

scheme for providing high identification performance. The genuine identification rate decreases as expectedly as more information is omitted in the template creation. The genuine identification rates are not very high, since fingerprints in the NIST database typically contain a very large number of minutiae points (195 on average), which is not very suitable for layering. However, results are comparable to the rank-1 identification rates ($\sim 85\%$ and $\sim 83\%$) reported in [59], obtained using a similar and alternative multi-biometric template creation scheme and a similar size database.

The uni-modal search evaluation that tests whether a multi-biometric template database can be searched with a single fingerprint, results in low identification rates as desired. When the test is carried out with an impression of the first constituent fingerprint (A'), the top-1 results are 75%, 74% and 58%, using *Method*₁, *Method*₂ and *Method*₃ respectively. Compared to genuine identification rates, there is about 20% points difference between genuine and uni-modal identification rates, for *Method*₁ and *Method*₃.

Uni-modal search with the second fingerprint achieves roughly the same rate as for the first fingerprint using *Method*₁, as the two fingerprints have a symmetric role in this method. However the top-1 identification rates drop even further, to 40% and 48%, using *Method*₂ and *Method*₃, respectively. As discussed before, with these two methods, the minutiae angles of the second fingerprint are modified to match the angles of the first fingerprint, when constructing the multi-biometric template.

Finally, both types of cross-link evaluations result in very low identification rates end up in low success rates, 20% and 10% using *Method*₂ and 1% and 37% for *Method*₃, supporting the claims that the proposed methods are strong against cross-linking attacks.

As for the FVC gallery, genuine identification rates are very high (99, 97, 96 and 100% for the four methods), as shown in *Table 5.7*. However, uni-modal identification rates are also very high except for *Method*₃ and *Method*₄. For these two methods, it can be observed that the uni-modal identification rates (83% and 74%) are significantly lower compared to genuine identification rates, as desired.

Cross-link rates are also low in this database; in particular for *Method*₃, a 53% rate is obtained when the first fingerprint is shared among the two corresponding multi-biometric templates and 6% when the second fingerprint is shared. *Method*₄ that combines three

fingerprints obtains even higher genuine identification rates and lower uni-modal search and cross-link rates (77% and 63% top-1 rates, respectively).

In summary, the results show that *Method*₃ obtains significantly lower uni-modal search rates compared to genuine identification rates, as well as very low cross-link rates for both databases. While not applicable in all applications and databases, *Method*₄ obtains even better results, with higher genuine identification rates and lower cross-link rates.

5.5 Evaluation Results of Multi-Biometric Templates Using Fingerprint and Voice

In this section, verification performance results of the system that combines fingerprint and voice templates are reported, so as to demonstrate applicability of the proposed framework to other biometric modalities and to demonstrate cancelability. Being a behavioral modality, the utilization of the voice biometric has the advantage of rather simple revocation if compromised and almost unlimited number of realizations due to the fact that user can have as many spoken passwords as she wishes to have.

For the evaluations, the FVC 2000-A fingerprint database discussed in Section 5.2 was combined with TUBITAK voice data subsets discussed in Section 5.2.2. For each voice subset, a gallery of 100 multi-biometric templates was generated, by pairing one voice sample of each user with a fingerprint from the FVC 2000-A database and repeating this for the whole database. This gallery is used in genuine identification tests, as well as uni-modal search tests.

In addition, two other galleries were created to be used in cross-link tests with the first gallery. For each multi-biometric template in the first gallery ($A + B$), a different fingerprint is combined with another utterance of the same voice sample used in the template, to obtain the template ($X + B'$) in the second gallery. Similarly, another impression of the fingerprint used in the template in the first gallery is combined with a different voice sample to obtain the matching template ($A' + X$) in the third gallery (*See Section 5.4.4*). Since *Method*₄ contains three biometric layers, where two of them are fingers and one is voice, the galleries generated for *Method*₄ contain 55 multi-biometric templates.

5.5.1 Uni-modal and Multi-modal Verification Results

The first two rows of *Table 5.8* show the uni-modal verification performances of the Hamming distance based matcher (*see Section 4.4*) using only the voice minutiae and the Neurotechnology’s matcher using only fingerprint minutiae, as the two components of the multi-modal system. The *NT* system using the fingerprint minutiae has a similar performance to what was obtained in *Section 5.4.1*, where another pool of fingerprints from the same dataset was used. Since, the same fingerprints are combined with all the multi-biometric galleries, the matcher performance is the same (2.1%) for all. With 12.1% and 8.7% and 7.8% accuracies on the three subsets, the verification results using voice features are roughly comparable with state-of-the-art speaker verification results. Note that during conversion of the voice templates to *voice minutiae*, the order of the actual bytes in the voice template are lost, necessitating that the Hamming distance comparison is performed in a brute force manner, which in turn leads to sub-optimal registrations.

Method	Modality	FPS	PPS	CPS
Hamming	Voice	12.1	8.7	7.8
<i>NT</i>	Fingerprints	2.1		
<i>Method</i> ₂	Both	1.9	1.6	2.0
<i>Method</i> ₃	Both	4.8	1.9	4.0
<i>Method</i> ₄	Both	3.0	3.0	3.0

TABLE 5.8: EER percent results for verification tests using fingerprints and voice.

Verification results for the multi-biometric system are shown in the last two rows of *Table 5.8*. The system obtains less than 2% EER with the three voice database subsets for *Method*₂. The error rates almost double with *Method*₃ that does not use all of the fingerprint template; but drop to 3.0% for all subsets, using *Method*₄. It is also important to note that the performance obtained for the second subset (*Private Passwords*) is better than the first subset (*Fixed Password Set*) where everyone utters the same string and the only distinguishing part is the vocal characteristics of the user.

In summary, the proposed multi-biometric template scheme implemented with a fingerprint and a voice password, obtains an improvement over both of the uni-modal systems

and comparable to those obtained with the implementation with two fingerprints. However the real benefit with this case is the renewability of the multi-biometric templates constructed with voice pass-phrases that can be easily changed.

5.5.2 Template Security and Privacy Test Results

To evaluate privacy enhancements, it is important to apply identification tests (genuine identification and attacks) on the fingerprint + voice case see '*Multi-modal Identification with the Proposed Scheme*' in Section 5.1. The databases for this test are constructed using FVC fingerprint databases and TUBITAK voice database as described in Section 5.2.2.

As can be seen in Table 5.9, top-1 genuine identification rates are very high for all three methods with 99% for both methods, as desired. As for the uni-modal searches, identification rates drop to 95% for *Method₂* and 88% for *Method₃*, when the fingerprint (*A'*) is used as query. The uni-modal search with voice (*B'*) obtains even higher identification rates of 89% and 91%, using *Method₂* and *Method₃*, respectively. The drop between genuine and uni-modal identification rates are small for *Method₂* and moderately good (around 10%) for *Method₃*; however it is expected that as the gallery size increases, uni-modal identification rates would drop much faster than genuine identification rates. *Method₄* that combines two fingerprint and voice shows the best results, with 99% genuine identification rate and only around 65% uni-modal search rate using fingerprints, and 77% using voice as the query.

		GID	UMS			XLNK	
		Σ vs. (A', B')	Σ vs. A'	Σ vs. B'	Σ vs. C'	Σ vs Σ' w/ different Voice	Σ vs Σ' w/ different FP
<i>Method</i> ₂	Top-1	99	95	89	-	83	65
	Top-5	99	95	95	-	87	85
	Top-10	100	95	99	-	88	88
<i>Method</i> ₃	Top-1	99	88	91	-	33	72
	Top-5	100	89	99	-	39	89
	Top-10	100	90	99	-	43	93
<i>Method</i> ₄	Top-1	99	64	66	77	33	11
	Top-5	100	66	68	95	48	30
	Top-10	100	69	70	98	59	52

TABLE 5.9: Identification and Cross-Link results with a gallery consisting of 100 multi-biometric templates with fingerprint-voice layers. A and A' refer to fingerprint impressions and B , B' and C' are voice minutiae (FP+PP).

As for cross-link rates, both $Method_3$ and $Method_4$ achieve a very low rate of 33% when the templates share a fingerprint and differ in the voice sample. This means that the voice data indeed works well to hide the original fingerprint template. The cross-link rate is higher for $Method_3$ (72%) when the voice sample is shared (last column); but it is still significantly lower than the genuine identification rate in this case. However, notably this is a less likely scenario as the voice is expected to be different in different galleries. The ROC plot for these tests is given in *Figure 5.5*.

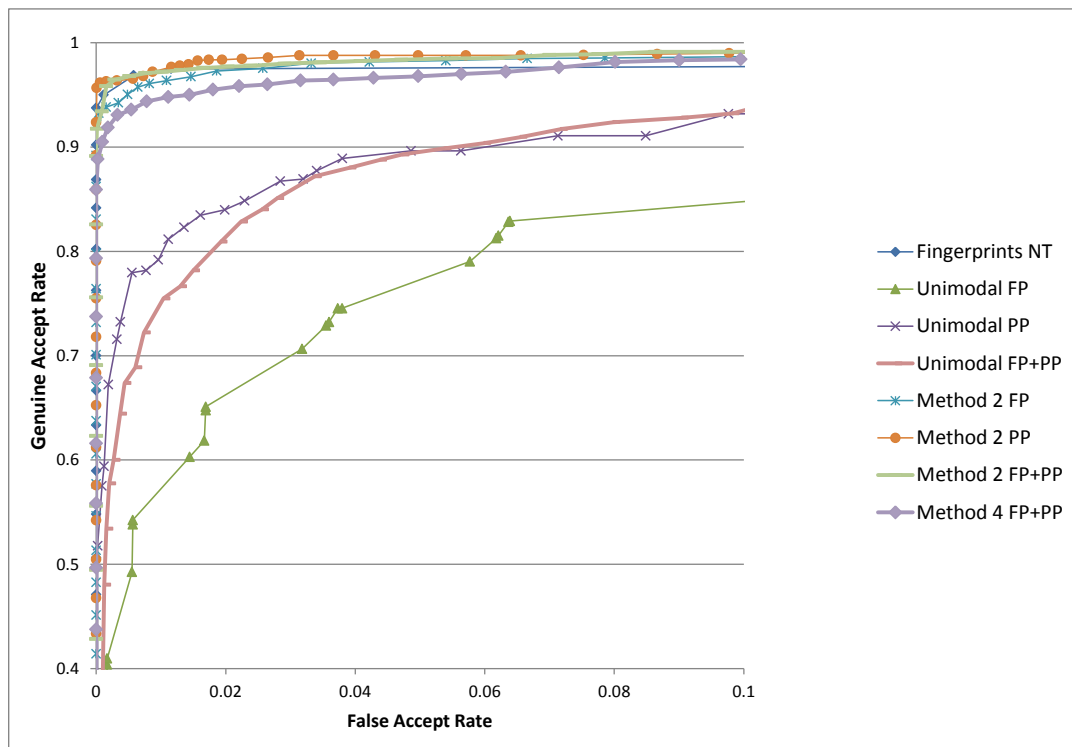


FIGURE 5.5: ROC Plots corresponding to *Table 5.8* ($FP=Fixed\ Password$, $PP=Private\ Password$, $FP+PP=Concatenated\ voice$).

5.6 Entropy and Information Leakage Analysis

The proposed multi-biometric template fusion methods described in this thesis are analyzed in terms of biometric system performances (i.e. verification and identification). It is also important to provide an information theoretical perspective on the claimed privacy protection scheme. This is achieved by calculating the entropy of the multi-biometric templates and comparing them to the randomly generated counterparts. Since the focus of this thesis is to show that multi-biometric templates that are generated with the

proposed scheme possess high entropy values, a rather simple and comparative approach has been taken.

A fingerprint template is divided into a grid of $d \times d$ pixels sized *cells*. The probability of the grid cell i to be occupied by at least one minutia is estimated by considering all the records in the dataset, as:

$$P(Y_i = 1) = \frac{n(i)}{N}$$

where $n(i)$ is the number of times grid cell i is found to contain at least one minutiae, over the total number of considered templates N . The random variable Y_i takes on value 1 if there is at least one minutia in grid cell i ; 0 otherwise.

A sample template divided into a grid is given in *Figure 5.6*. For a template of size $W \times H$, the total number of grid cells:

$$S = \frac{W \times H}{d^2}$$

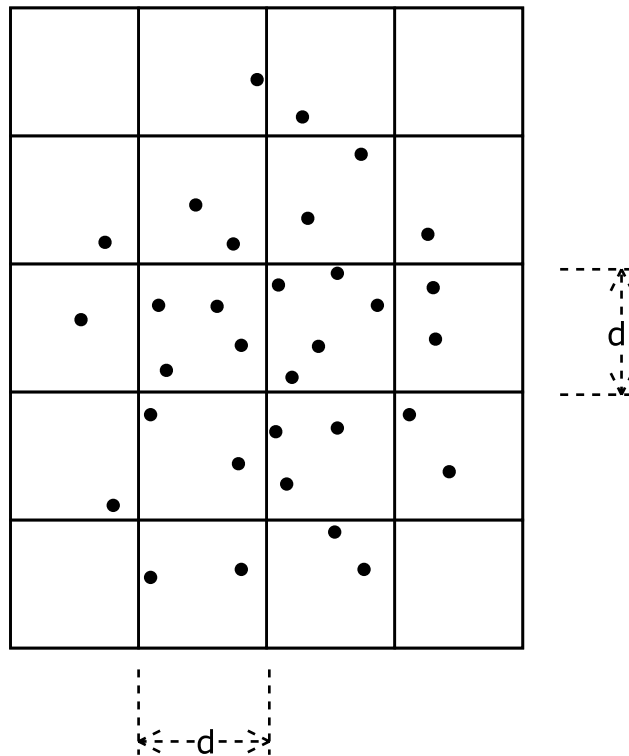


FIGURE 5.6: A sample template divided into a grid of $d \times d$ sized cells.

Assuming independence between Y_i and Y_j , the *Shannon Entropy* of the fingerprint template is estimated as:

$$H(Y) = \sum_{i=1}^S P(Y_i = 1) \log_2 P(Y_i = 1) + P(Y_i = 0) \log_2 P(Y_i = 0)$$

It should be noted that the entropy value depends on the value of d and we believe that a value between 10 and 20 may give a reasonable coarse estimate for the true entropy. As the main focus here is the change in entropy with respect to different templates (e.g. *random vs. actual*), a relatively simple approach has been employed.

The entropy analysis is performed on the *FVC 2000-a* and *NIST* datasets. The FVC dataset contains 55 records, whereas the NIST dataset contains 1000 records. Each record in a dataset is a vector $\{A, A^r, \Sigma, \Sigma', \Sigma^r\}$, where A is the primary template and Σ is the multi-biometric template (i.e. $\Sigma = A \cup B$). A^r and Σ^r are minutiae templates that contain randomly generated minutiae (chaff points) having the same number of minutiae as their counterparts A and Σ respectively. Σ' is a multi-biometric template $\Sigma' = A + B^r$ where B^r is a randomly generated template having the same number of minutiae points as B (i.e. the secondary template). The estimated entropy values are provided in *Table 5.10*, The absolute entropy values have been provided in the upper part, and the differences are provided in the lower part of the table. For instance for $d = 20$ we report the entropy of a single biometric template and a multi-biometric template as 108 and 220 respectively. For comparison, Ratha et. al report entropy for a fingerprint template of 30 minutiae to be around 100 bits [81].

The aim of the analysis is to estimate the randomness of the actual fingerprint templates. To achieve this, the entropy values of the actual fingerprint templates are compared to the random counterparts. In other words, we focus on the entropy differences. In particular, $A^r - A$ estimates the randomness of a single minutiae template, $\Sigma' - \Sigma$ measures the contribution of the secondary template (B) in terms of randomness, and $\Sigma^r - \Sigma$ provides information about the randomness of a multi-biometric template. The differences are important because they provide a measurement of the *information leakage* that might occur in a template compared to its random counterpart.

It can be seen that the entropy difference between the random data and the actual fingerprint data is mostly below 10%. The differences increase with respect to the

d (pixels)	FVC					NIST				
	1	5	10	15	20	1	5	10	15	20
A :	206	191	160	131	108	1034	737	552	439	357
A^r :	206	195	169	143	120	1043	769	585	473	392
Σ :	450	387	294	220	160	2010	1312	932	696	511
Σ' :	452	398	312	240	182	2028	1346	967	733	555
Σ^r :	452	403	316	246	188	2036	1359	980	749	575
$A^r - A$ (bits)	0.3	4.1	9.0	11.7	12.6	8.9	31.5	33.4	33.9	35.6
$A^r - A$ (%)	0.1	2.1	5.3	8.2	10.5	0.9	4.1	5.7	7.2	9.1
$\Sigma' - \Sigma$ (bits)	1.4	11.4	18.2	20.0	22.6	17.9	34.1	34.6	37.4	43.8
$\Sigma' - \Sigma$ (%)	0.3	2.8	5.8	8.1	12.0	0.9	2.5	3.5	5.0	7.6
$\Sigma^r - \Sigma$ (bits)	1.6	16.4	22.5	25.5	28.1	25.9	46.4	48.5	52.9	63.4
$\Sigma^r - \Sigma$ (%)	0.4	4.1	7.1	10.4	15.0	1.3	3.4	4.9	7.1	11.0

TABLE 5.10: Estimated entropies according to different grid cell sizes ($d \times d$)

increasing d values (i.e. larger cells). This can be explained by the fact that while a random template can have minutia at almost any location, the minutia tend to be closer to the center of the mass in an actual template due to the shape of the finger impression.

The $A^r - A$ values have been provided for comparison to the $\Sigma' - \Sigma$ and $\Sigma^r - \Sigma$ values. The closeness of the $\Sigma' - \Sigma$ values to the $A^r - A$ values implies that the information leakage caused by the inclusion of the secondary template is ignorably small when $d = 1, 5, 10, 20$ for FVC, and even decreased for $d = 15$ for FVC, and $d = 5, 10, 15, 20$ for NIST. On the other hand, the $\Sigma^r - \Sigma$ values are close to $A^r - A$, implying that the randomness of the multi-biometric template is sufficiently close to a single template.

Consequently, it can be stated that the proposed multi-biometric template protection method provides sufficient security of the constituent templates, hence protecting the privacy of the users.

5.7 Time Cost for Enrollment and Verification

The enrollment and verification phases take different amount of time for processing. Since the enrollment phase includes image processing steps as well (e.g. extracting the minutiae from the raw image), it takes much longer than the verification.

However, as the feature extraction process has been declared to be out of scope of this thesis, the enrollment times reported here include only the multi-biometric template creation from two existing minutae templates and the feature extraction costs are left out.

The multi-biometric template creation process takes 300ms for the FVC DB and 1s for the NIST DB. The matching process takes less than 10ms with the FVC DB for *Method*₁, and up to 50ms for *Method*₂ and *Method*₃; and for the NIST DB it takes less than 50ms for *Method*₁, and up to 500ms for *Method*₂ and *Method*₃. Note that, while verification times are longer than the commercial uni-modal system, they are still acceptable for use in a commercial application.

While the multi-biometric template creation process is fast, it is not regarded as the bottleneck of the system as it will be done rarely for a biometric system. On the other hand, for traditional fingerprint based biometric systems where the impressions are static (i.e. not rolled-scanned) the average number of minutiae (~ 32) allows quite fast matching 1s (1000 matches/second), which in turn proves that the system is suitable for both verification and identification scenarios. However, this speed decreases as the average number of the minutiae in a template increases, yielding a 10ms (100 matches/second) matching time and speed. Consequently, it can be summarized that although the algorithm provides high accuracy matching performance as shown throughout this chapter and is fast for small sized templates, it might need to be improved in terms of speed for larger templates such as the ones of the NIST DB.

Chapter 6

Summary and Conclusion

6.1 Summary

This thesis proposes and evaluates different variations of the suggested multi-biometric template construction method. The discussions about the relative merits of these variations, based on results observed on the FVC datasets are given below. These observations apply to the NIST database for the most part as well.

Using two fingerprints, *Method*₁ (first proposed in [31]) has very good verification rates that are better than the state-of-the-art fingerprint verification rates of the *NT* matcher (see *Table 5.4*) and its genuine identification rate is high, but its uni-modal search rates are also high (see *Table 5.7*). Furthermore, since the two fingerprints are layered without extra precaution, there may be a possibility of separating the two fingerprints using minutiae angle coherence.

As the methods try to protect the template more (*Method*₂ and *Method*₃), verification and identification rates fall, but unimodal search and cross-link rates also decrease as desired. In particular in *Method*₃, which is the suggested layering method for two fingerprints, the average verification rate for the FVC databases is quite good (*Table 5.4*) and the unimodal search (*Table 5.7*) and cross-link rates (*Table 5.6*) are very low as desired. Considering that the gallery sizes used for uni-modal search is very small and cross-link tests identification rates are already very low, the significant difference between these rates and the genuine identification rates show the potential of the method in increasing biometric privacy.

Finally, in *Method*₄, three different fingerprints are combined and even better results than *Method*₃ are obtained. Hence, if the application is suitable, at the cost of some inconvenience to the user, this is the proposed method. However due to a large number of minutiae in the template, this method is not suitable for applications requiring very low false accept rates (*Fig. 5.4*).

As for the fingerprint and voice combination, the best results are obtained when a longer voice pass-phrase is used (combination of fixed-password and user's name), as expected. In this case, all methods obtain better verification results compared to only unimodal verification with voice (*see Table 5.8*), while *Method*₃ also has low cross-link rates as given in (*Table 5.9*).

As with three fingerprints, combining two fingerprints and a voice pass-phrase, as done in *Method*₄ is the most successful and suggested method, if the application allows for the use of three modalities.

For the NIST database where the fingerprint templates contain an excessive number of minutiae points, identification and cross link rates are lower in general compared to the FVC database. Hence, while genuine identification rates are not as high as desired, cross linking rates are very low.

The NIST database wasn't used in fingerprint and voice combination, because the relatively small number of voice minutiae (average 19 per template) compared to the large NIST templates (average 195 per template) was not sufficient for protecting the fingerprint template.

In terms of comparison to other similar systems, the works of Othman and Ross [59] and Li and Kot [60] are considered. As summarized in *Chapter 2*, these two systems obtain high identification and verification rates and much lower cross-link rates as desired; however the bio-layering method proposed in this thesis does not have any requirements such as the need to have compatible fingerprints or locate reference points.

In [59], Othman and Ross report a rank-1 accuracy of $\sim 85\%$ and an EER of $\sim 6\%$ on a data set with a total of 500 fingers, obtained by mixing two different fingers from the West Virginia University (WVU) dataset. In another experiment, where they mix two different datasets (FVC 2002-DB2_A and WVU) creating a dataset of 200 test instances, they report a rank-1 accuracy of $\sim 83\%$ and an EER of $\sim 7\%$.

In [60] the authors create a multi-biometric template by combining the minutia locations of one finger with orientation information of another one. They use FVC 2002-DB2_A for their experiments, and report the lowest error rates with FRR=6% at FAR=0.1%.

To evaluate privacy of their proposed methods, Li et al. define two types of attacks based on their scheme: using the combined template to attack a database that contains (i) the first fingerprint (using the minutiae location correlation) and (ii) the second fingerprint (using the minutiae angle correlation). They call the two attacks *Attack Type A* and *Attack Type B* respectively. Using FVC 2002-DB2_A and generating databases of 100 combined templates, they report 25% for *Attack Type A* and 57.5% rank-1 hits for *Attack Type B*.

The bio-layering method superimposes the minutiae of two different templates on the same coordinate system. As a result, the generated multi-biometric template might look like a fuzzy vault with fewer minutia points, considering *A* as the primary template and *B* as the chaff point set.

As one of the prevalent template protection methods, the fuzzy vault is well-studied in terms of its practicality, security and privacy aspects [82]. The proposed technique may have two advantages over the fuzzy vault. One advantage comes naturally due to the multi-biometric use. However, the main advantage is that in the proposed scheme, the verification does not reveal one of the two biometric templates with certainty.

To unlock a fuzzy vault, a sufficient quality probe template (A') is provided by the user. If a sufficient number of genuine points in the template are matched, the polynomial can be reconstructed in some number of attempts. This in turn releases the secret encoded in the polynomial. As a result, the matching minutiae points in *A* are identified as being genuine, which constitutes an information leak.

In the bio-layering method, the secondary template *B* is analogous to the chaff points in the fuzzy vault. While trying to remove *A* using A' , as $\Delta = \Sigma - A'$, the system may incorrectly miss some minutiae points from *A* and remove some others from *B*. Moreover, Δ will be different every time a new A' arrives. Since there is no way to fully guarantee that the matched points belong to *A* or that the remaining points belong to *B*, it is not possible to fully recover the constituent biometrics (see Section 5.3). That

is why it can be claimed that the original templates are protected in a multi-biometric vault.

The weakness of the proposed method against the fuzzy vault is that the secondary template has a number of minutiae close to the size of the primary template. Since there is no way to guarantee a full recovery of the primary template (as in fuzzy vault) the secondary template that is used for hiding cannot be as large as the random set created for a fuzzy vault, as the verification performance would be poorer (consider FVC vs. NIST test results).

Another potential weakness is that if Σ is compromised, the attacker can break it into two templates in a random manner, obtaining two dummy constituent templates C and D . She can then use these two templates to break into the system, in *unattended* scenarios. However, note that the attacker does not obtain the real fingerprints and the success would be limited with *Method₂* or *Method₃* due to the replaced angles.

6.2 Conclusions

In this thesis a multi-biometric templates protection scheme is proposed for increased performance, template security and enhanced privacy. In this work, two realizations of this idea are demonstrated by combining two fingerprints in one realization and a fingerprint and voice pass-phrase in the other one. In each case, three different methods of constructing the multi-biometric template using fewer information of the constituent fingerprints are evaluated in order to explore different performance and template security levels; and a fourth method combining three biometric modalities.

Additionally, a fast and novel fingerprint matcher (*TPS Matcher*) has been developed that can be adapted to situations where minutia angles don't exist or might be ignored (*see Chapter 3*).

The results showed that the proposed method (*Method₃*) with two fingerprints provides near state-of-the-art verification performance on public databases. Furthermore, it was shown that the proposed method is highly resistant to attacks where an adversary might want to identify a person from a latent fingerprint or match users in two different

databases (cross-correlation attack), while providing high genuine identification rates (see Tables 5.7,5.6,5.9).

The alternative realization the multi-biometric template idea was provided by layering a fingerprint with a spoken password (see Section 4.4), in order to explore the multi-modal nature as well as to achieve cancelability. In this case, the system obtains very good verification performance, but more modest template security and privacy enhancements. In both cases, using a third biometric improves the success of the method (*Method₄*).

Bibliography

- [1] R. Cappelli, D. Maio, and D. Maltoni, “Modelling plastic distortion in fingerprint images,” *Lecture Notes in Computer Science*, vol. 2013, pp. 369–??, 2001.
- [2] FVC, “FVC2000 finger verification competition databases,” <http://bias.csr.unibo.it/fvc2000/databases.asp>, 2000, Accessed: 20/09/2014.
- [3] FVC, “FVC2002 finger verification competition databases,” <http://bias.csr.unibo.it/fvc2002/databases.asp>, 2002, Accessed: 20/09/2014.
- [4] NIST, “NIST special database 4,” <http://www.nist.gov/srd/nistsd4.cfm>, 2010, Accessed: 20/09/2014.
- [5] Anil Jain, Patrick Flynn, and Arun A Ross, *Handbook of biometrics*, Springer Science & Business Media, 2007.
- [6] Sushil Chauhan, A.S. Arora, and Amit Kaul, “A survey of emerging biometric modalities,” *Procedia Computer Science*, vol. 2, pp. 213 – 218, 2010, Proceedings of the International Conference and Exhibition on Biometrics Technology.
- [7] Georgios Goudelis, Anastasios Tefas, and Ioannis Pitas, “Emerging biometric modalities: a survey,” *Journal on Multimodal User Interfaces*, vol. 2, no. 3, pp. 217–235, 2009.
- [8] R. Chellappa, C.L. Wilson, and S. Sirohey, “Human and machine recognition of faces: a survey,” *Proceedings of the IEEE*, vol. 83, no. 5, pp. 705–741, May 1995.
- [9] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, London, second edition, 2009.

-
- [10] Wonseok Song, Taejeong Kim, Hee Chan Kim, Joon Hwan Choi, Hyoun-Joong Kong, and Seung-Rae Lee, “A finger-vein verification system using mean curvature,” *Pattern Recognition Letters*, vol. 32, no. 11, pp. 1541–1547, 8 2011.
- [11] Adams Kong, David Zhang, and Mohamed Kamel, “A survey of palmprint recognition,” *Pattern Recognition*, vol. 42, no. 7, pp. 1408–1418, 7 2009.
- [12] Ayman Abaza, Arun Ross, Christina Hebert, Mary Ann F. Harrison, and Mark S. Nixon, “A survey on ear biometrics,” *ACM Comput. Surv.*, vol. 45, no. 2, pp. 22:1–22:35, Mar. 2013.
- [13] M. Choras, “Image feature extraction methods for ear biometrics—a survey,” in *Computer Information Systems and Industrial Management Applications, 2007. CISIM '07. 6th International Conference on*, June 2007, pp. 261–265.
- [14] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, “Biometric identification through hand geometry measurements,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 22, no. 10, pp. 1168–1171, Oct 2000.
- [15] Kevin W. Bowyer, Karen Hollingsworth, and Patrick J. Flynn, “Image understanding for iris biometrics: A survey,” *Computer Vision and Image Understanding*, vol. 110, no. 2, pp. 281 – 307, 2008.
- [16] Richard Yew Fatt Ng, Yong Haur Tay, and Kai Ming Mok, “A review of iris recognition algorithms,” in *Information Technology, 2008. ITSIm 2008. International Symposium on*, Aug 2008, vol. 2, pp. 1–7.
- [17] 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, no. 11, pp. 1148–1161, 1993.
- [18] Hamid Tabatabaee, A Milani-Fard, and Hadi Jafariani, “A novel human identifier system using retina image and fuzzy clustering approach,” in *Proceedings of the 2nd IEEE International Conference on Information and Communication Technologies*, 2006, pp. 1031–1036.
- [19] Tomi Kinnunen and Haizhou Li, “An overview of text-independent speaker recognition: From features to supervectors,” *Speech communication*, vol. 52, no. 1, pp. 12–40, 2010.

-
- [20] Joseph P Campbell Jr, "Speaker recognition: a tutorial," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1437–1462, 1997.
- [21] Alisher Kholmatov and Berrin Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern recognition letters*, vol. 26, no. 15, pp. 2400–2408, 2005.
- [22] Berrin Yanikoglu and Alisher Kholmatov, "Online signature verification using fourier descriptors," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, pp. 12, 2009.
- [23] Marcos Faundez-Zanuy, "Signature recognition state-of-the-art," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 20, no. 7, pp. 28–32, 2005.
- [24] R. Plamondon and S.N. Srihari, "Online and off-line handwriting recognition: a comprehensive survey," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 22, no. 1, pp. 63–84, Jan 2000.
- [25] Fabian Monrose and Aviel Rubin, "Authentication via keystroke dynamics," in *Proceedings of the 4th ACM conference on Computer and communications security*. ACM, 1997, pp. 48–56.
- [26] Davrondzhon Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Annual Norwegian computer science conference*. Citeseer, 2007, pp. 19–21.
- [27] James Wayman, Anil Jain, Davide Maltoni, and Dario Maio, *An introduction to biometric authentication systems*, Springer, 2005.
- [28] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 113:1–113:17, Jan. 2008.
- [29] N.K. Ratha, R.M. Bolle, V.D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," in *Applications of Computer Vision, 2000, Fifth IEEE Workshop on.*, 2000, pp. 29–34.
- [30] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E.M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, March 2012, pp. 498–505.

- [31] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *International Conference on Pattern Recognition, BCTP Workshop, Cambridge, England*, Aug. 2004.
- [32] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multimodal biometric templates for verification using fingerprint and voice," in *SPIE Defense & Security: Biometric Technology For Human Identification V*, March 2008.
- [33] NEUROTechnology, "Neurotechnology, biometric and artificial intelligence technologies," <http://www.neurotechnology.com/>, 09 2014, Accessed: 20/09/2014.
- [34] G. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through on-line biometric identification," in *IEEE Symposium on Privacy and Security*, 1998, pp. 148–157.
- [35] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Conference on Computer and Communications Security*, ACM Press., 1999, pp. 28–36.
- [36] J.P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proceeding of International Conference on Audio and Video Based Biometric Person Authentication*, 2003, vol. LNCS 2688, pp. 393–402.
- [37] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, pp. 2245–2255, 2004.
- [38] A. Juels and M. Sudan, "A fuzzy vault scheme," *IACR Cryptology ePrint Archive*, vol. 2002, pp. 93, 2002.
- [39] G. Tomko., "Biometrics as a privacy-enhancing technology: Friend or foe of privacy?," in *In Privacy Laws & Business 9th Privacy Commissioners/Data Protection Authorities Workshop*, 1998.
- [40] G. Tomko., "Privacy implications of biometrics – a solution in biometric encryption," in *Eighth Annual Conference on Computers, Freedom and Privacy*, 1998.
- [41] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

- [42] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, “Optimal iris fuzzy sketches,” in *In Biometrics: Theory, Applications, and Systems*, 2007.
- [43] K. Nandakumar, A. Nagar, and A.K. Jain, “Hardening fingerprint fuzzy vault using password,” in *International Conference on Biometrics*, 2007, pp. 927–937.
- [44] U. Uludag, S. Pankanti, and A. Jain., “Fuzzy vault for fingerprints,” in *Proceeding of International Conference on Audio and Video Based Biometric Person Authentication*, 2005, pp. 310–319.
- [45] K. Nandakumar and A.K. Jain, “Multibiometric template security using fuzzy vault,” in *Biometrics: Theory, Applications, and Systems*, 2008, pp. 1–6.
- [46] A. Nagar, K. Nandakumar, and A.K. Jain, “Multibiometric cryptosystems based on feature-level fusion,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, 2012.
- [47] A. Kong, K.H. Cheung, D. Zhang, M.S. Kamel, and J. You, “An analysis of biohashing and its variants,” *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.
- [48] Y. Sutcu, Q. Li, and N. Memon, “Secure biometric templates from fingerprint-face features,” in *CVPR. 2007*, IEEE Computer Society.
- [49] Y. Sutcu, T.S. Husrev, and M. Nasir, “A geometric transformation to protect minutiae-based fingerprint templates,” .
- [50] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A.K. Jain, “Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 3, pp. 450–455, 2005.
- [51] R. Brunelli and D. Falavigna, “Person identification using multiple cues,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 17, no. 10, pp. 955–966, Oct. 1995.
- [52] K.A. Toh, “Fingerprint and speaker verification decisions fusion,” in *CIAP*, 2003, pp. 626–631.
- [53] K.A. Toh and W.Y. Yau, “Fingerprint and speaker verification decisions fusion using a functional link network,” *IEEE Trans. Systems, Man and Cybernetics*, vol. 35, no. 3, pp. 357–370, Aug. 2005.

- [54] S.M. Anzar and P.S. Sathidevi, “Adaptive score level fusion of fingerprint and voice combining wavelets and separability measures,” *International Journal of Electronics and Communications*, , no. 0, pp. –, 2013.
- [55] S. Ben-Yacoub and Y. Abdeljaoued, “Fusion of face and speech data for person identity verification,” in *IEEE Transactions on Neural Networks*, 1999, vol. 10, pp. 1065–1075.
- [56] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, “On combining classifiers,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 3, pp. 226–239, Mar. 1998.
- [57] L. Hong and A.K. Jain, “Integrating faces and fingerprints for personal identification.,” in *ACCV (1)*, Roland T. Chin and Ting-Chuen Pong, Eds. 1998, vol. 1351 of *Lecture Notes in Computer Science*, pp. 16–23, Springer.
- [58] Lin Hong and Anil K. Jain, “Integrating faces and fingerprints for personal identification,” Tech. Rep. MSU-CPS-97-18, Department of Computer Science, Michigan State University, East Lansing, Michigan, June 1997.
- [59] A.A. Othman and A. Ross, “On mixing fingerprints,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260–267, 2013.
- [60] S. Li and A. C. Kot, “Fingerprint combination for privacy protection,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 350–360, 2013.
- [61] A. Ross and A.A. Othman, “Visual cryptography for biometric privacy,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70–81, 2011.
- [62] Anil K Jain, Salil Prabhakar, and Sharath Pankanti, “Can identical twins be discriminated based on fingerprints,” Tech. Rep., Technical Report MSU-CSE-00-23, Department of Computer Science, Michigan State University, East Lansing, Michigan, 2000.
- [63] Anil Jain, Lin Hong, and Ruud Bolle, “On-line fingerprint verification,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 19, no. 4, pp. 302–314, 1997.

- [64] Marius Tico and Pauli Kuosmanen, “Fingerprint matching using an orientation-based minutia descriptor,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 25, no. 8, pp. 1009–1014, 2003.
- [65] A.M. Bazen and S.H. Gerez, “Fingerprint matching by thin-plate spline modelling of elastic deformations,” *Pattern Recognition*, vol. 36, no. 8, pp. 1859–1867, 2003.
- [66] Alessandra A Paulino, Jianjiang Feng, and Anil K Jain, “Latent fingerprint matching using descriptor-based hough transform,” *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 1, pp. 31–45, 2013.
- [67] George Wolberg, “CUBIC SPLINE INTERPOLATION: A REVIEW,” Tech. Rep. CUCS-389-88, University of Columbia, 1988.
- [68] F. L. Bookstein, “Principal wraps: Thin-plate splines and the decomposition of deformations,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 11, no. 6, pp. 567–585, June 1989.
- [69] Arun Ross, Sarat C. Dass, and Anil K. Jain, “Estimating fingerprint deformation,” in *Biometric Authentication, First International Conference, ICBA 2004, Hong Kong, China, July 15-17, 2004, Proceedings*, David Zhang and Anil K. Jain, Eds. 2004, vol. 3072 of *Lecture Notes in Computer Science*, pp. 249–255, Springer.
- [70] N.K. Ratha, K. Karu, S. Chen, and Anil K. Jain, “A real-time matching system for large fingerprint databases,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 18, no. 8, pp. 799–813, 1996.
- [71] A.K. Jain., L. Hong, S. Pankanti, and R. Bolle, “An identity authentication system using fingerprints,” *Proceedings of the IEEE*, vol. 85, pp. 1365–1388, Sep. 1997.
- [72] N. Ratha, S. Chen, and A.K. Jain., “Adaptive flow orientation based feature extraction in fingerprint images,” *Pattern Recognition*, vol. 28, pp. 1657–1672, 1995.
- [73] M. Tico and P. Kuosmanen, “An algorithm for fingerprint image post-processing,” in *Proceedings of the 34'th Asilomar Conference on Signals, Systems and Computers*, Nov. 2000, vol. 2, pp. 1735–1739.
- [74] J. Feng and Anil K. Jain, “Fingerprint reconstruction: From minutiae to phase,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 33, no. 2, pp. 209–223, Feb 2011.

-
- [75] Lawrence Rabiner and Biing-Hwang Juang, *Fundamentals of Speech Recognition*, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1993.
- [76] H. Hermansky, “Perceptual linear predictive (plp) analysis of speech,” *J Acoust Soc Am*, vol. 87, no. 4, pp. 1738–1752, 1990.
- [77] Andreas Stolcke, Luciana Ferrer, Sachin Kajarekar, Elizabeth Shriberg, and Anand Venkataraman, “Mllr transforms as features in speaker recognition,” in *Proceedings of the 9th European Conference on Speech Communication and Technology*, 2005, pp. 2425–2428.
- [78] H. Beigi, *Fundamentals of Speaker Recognition*, SpringerLink : Bücher. Springer, 2011.
- [79] A. Kanak, Y. Bicil, M.U. Dogan, and H. Palaz, “Tren-si: A dcom-based speaker identification software,” in *Signal Processing and Communications Applications, 2006 IEEE 14th*, April 2006, pp. 1–4.
- [80] Arun Ross, Jidnya Shah, and Anil K. Jain, “From template to image: Reconstructing fingerprints from minutiae points,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 544–560, 2007.
- [81] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
- [82] A. Kholmatov and B. Yanikoglu, “Realization of correlation attack against fuzzy vault scheme,” in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, Mar. 2008, vol. 6819 of *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*.