ROMA
TRE
UNIVERSITÀ DEGLI STUDI

Scuola Dottorale di Ingegneria
Sezione di Ingegneria dell'Elettronica Biomedica,
dell'Elettromagnetismo e delle Telecomunicazioni

TESI DI DOTTORATO

PROTEZIONE DEI TEMPLATE BIOMETRICI PER SISTEMI DI AUTENTICAZIONE BASATI SU FIRMA

BIOMETRIC TEMPLATE PROTECTION FOR SIGNATURE BASED AUTHENTICATION SYSTEMS

Candidato
Emanuele Maiorana

Docente guida
Prof. Alessandro Neri

Roma, 1 marzo 2009

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Biometric Template Protection for Signature based Authentication Systems

by

Emanuele Maiorana

A Dissertation submitted to

University “Roma Tre”, Rome, Italy
Department of Applied Electronics

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Rome, 2009

Department:	Department of Applied Electronics, University “Roma Tre” of Rome, Italy
PhD Thesis:	Biometric Template Protection for Signature based Authentication Systems
Author:	**Emanuele Maiorana**
Supervisor:	Prof. **Alessandro Neri** (University “Roma Tre” of Rome, Italy)
Advisor:	Prof. **Patrizio Campisi** (University “Roma Tre” of Rome, Italy)
Year:	2009
Reviewers:	Prof. **Michael Fairhurst** (University of Kent, Canterbury, United Kingdom)
	Prof. **Sonia Garcia-Salicetti** (Institut TELECOM & Management Sud Paris, Paris, France)
Committee:	Prof. **Francesco Beltrame** (University of Genoa, Italy)
	Prof. **Roberto Cusani** (University “La Sapienza” of Rome, Italy)
	Prof. **Alessandro Toscano** (University “Roma Tre” of Rome, Italy)
	Expert Member: Prof. **Javier Ortega-Garcia** (“Universidad Autonoma de Madrid”, Madrid, Spain)

ROMA TRE
UNIVERSITÀ DEGLI STUDI

DIGITAL SIGNAL PROCESSING
MULTIMEDIA & OPTICAL COMMUNICATIONS

This Thesis describes the research carried out within the COMLAB Laboratory of the University “Roma Tre” of Rome, Italy, from 2006 to 2008.

Abstract

Biometric Template Protection for Signature based Authentication Systems

by

Emanuele Maiorana

One of the most emerging technologies for automatic people recognition is biometrics. In contrast with traditional approaches, based on what a person knows (password) or what a person has (ID card, tokens), biometric based authentication relies on who a person is or what a person does. Biometric based recognition systems are then typically able to provide improved comfort and security for their users, when compared to traditional authentication methods.

Unfortunately, the use of biometric data in an automatic recognition system also involves various risks not affecting other methods: if biometric data are somehow stolen or copied, they can be hardly replaced. Moreover, biometric data can contain relevant information regarding personality and health, which can be used in an unauthorized manner for malicious or undesired intents. It is also worth pointing out that, when a cross-matching among different biometric databases is performed, an unauthorized user tracking of the enrolled subjects can be done by means of users' biometric traits. This would unavoidably lead to users' privacy loss. Therefore, when designing a biometric based recognition system, the issues deriving from security and privacy concerns have to be carefully considered. Moreover, the adopted countermeasures should enhance biometric data resilience against attacks, while guaranteeing acceptable recognition performance.

This Thesis is focused on the protection of the biometric templates employed in a signature based authentication system. Signature biometrics is usually characterized by a high intra-user variability and a small forgeries inter-user variability, thus representing a challenging field of application for template protection techniques.

The literature regarding biometric template protection and on-line signature based recognition is first reviewed. Then, we take into account both parametric and functional features based on-line signature verification approaches, and describe, for each of them, how to provide protection to the employed biometric templates.

Specifically, we propose the use of cryptographic techniques and error correcting codes to secure global parametric features extracted from an on-line signature. Together with protection, also template cancelability and renewability are guaranteed. Moreover, the proposed authentication scheme is tailored to the signature variability of each user, thus obtaining a user adaptive system with enhanced performances with respect of a non-adaptive one.

We then propose how to provide security to the templates employed in a functional feature based signature authentication system, by means of a feature transformation protection approach. Specifically, we introduce a set of non-invertible transforms, which can be applied to any sequence based biometric template to generate multiple transformed version of it. Retrieving the original data from the transformed one is computationally as hard as random guessing. The effectiveness of the proposed approach is tested by considering both a regional signature functions analysis (employing Hidden Markov Models) and a local signature functions analysis (employing Dynamic Time Warping). Moreover, the performances achievable with the fusion of these two approaches are also discussed.

Eventually, we also propose the use of watermarking techniques to protect a set of dynamic signature features, by embedding it into a static representation of the signature itself. User authentication can be performed either by means of the only signature static image, or by using it together with the dynamic features embedded in the enrollment stage, by using a fusion approach. A multi-level authentication system, which is capable to provide two different levels of security, is then obtained. The proposed watermarking techniques are based on the properties of the Radon transform, being thus tailored to images, like those of a signature, with sharp edges. A procedure for the selection of the dynamic features which allow to guarantee the best recognition performances, as well as a novel approach which defines the minimum number of bits which should be employed to binarize a given feature without affecting the recognition performances, is proposed.

The effectiveness of the proposed approaches is tested by employing the public MCYT on-line signature corpus, with signatures taken from 100 different subjects, as experimental database.

Abstract

Protezione dei template biometrici per sistemi di autenticazione basati su firma

di

Emanuele Maiorana

Una tra le tecnologie maggiormente innovative impiegate per il riconoscimento automatico di persone la *biometria.* In contrasto con gli approcci tradizionali, basati su ciò che una persona conosce (password), o su quello che una persona possiede (carta d'identità, tessere), l'autenticazione basata su dati biometrici utilizza ciò che una persona *è*, o ciò che una persona *fa.* I sistemi di riconoscimento biometrico sono pertanto in grado di garantire ai propri utenti, rispetto ai sistemi tradizionali di autenticazione, un comfort maggiore e una sicurezza superiore.

Purtroppo, l'uso di dati biometrici in un sistema di riconoscimento automatico comporta anche vari rischi, nei quali non si incorre utilizzando invece altri approcci: se i dati biometrici impiegati vengono rubati o in qualche modo copiati, difficilmente possono essere sostituiti. Inoltre, i dati biometrici possono contenere informazioni riguardanti la personalità e la salute di una persona, e pertanto possono essere utilizzati per scopi non autorizzati, dannosi, o indesiderati dagli utenti. Vale anche la pena di sottolineare che, se viene effettuato un confronto tra differenti database di dati biometrici, i soggetti memorizzati nelle basi dati possono essere monitorati sulla base delle loro caratteristiche uniche. Ciò porta inevitabilmente ad una rilevante compromissione della privacy. Pertanto, nella progettazione di un sistema di riconoscimento biometrico, i problemi relativi alla sicurezza ed alla tutela della privacy devono essere attentamente valutati. Inoltre, le contromisure adottate dovrebbero migliorare la resistenza contro eventuali atttacchi ai dati biometrici, garantendo però delle prestazioni di riconoscimento accettabili.

Questa Tesi è focalizzata sulla protezione dei template biometrici impiegati in sistemi di autenticazione basati su firma. La firma viene comunemente impiegata come dato biometrico, ed è generalmente caratterizzata da un elevata variabilità intra-utente e una piccola variabilità inter-utente, rappresentando pertanto un campo di applicazione sfidante per la definizione di tecniche di protezione.

Nella presente Tesi viene inizialmente rivista la letteratura scientifica in materia di protezione dei template biometrici e di riconoscimento di firma dinamica. Dopodiché, si prendono in considerazione gli approcci basati su template parametrici e funzionali di firma, proponendo per ciasuno di essi un possibile schema di protezione dei template.

In particolare, si propone l'uso di tecniche crittografiche per garantire protezione a caratteristiche parametriche estratte dalle firme. Tale sistema impiega codici a correzione d'errore, la cui capacità correttiva può essere determinata sulla base delle caratteristiche dell'utente.

Si propone poi un metodo per garantire la sicurezza di template funzionali rappresentanti firme dinamiche, basato sulla definizione di trasformazioni non invertibili. L'efficacia del metodo proposto viene valuatata impiegando classificatori basati su Hidden Markov Models, o su tecniche di Dynamic Time Warping. Anche la fusione tra questi approcci viene considerata.

Infine, si propone l'uso di tecniche di watermarking per proteggere una serie di caratteristiche dinamiche della firma, inserendole all'interno di una rappresentazione statica della firma stessa. L'autenticazione degli utenti può essere effettuata tramite la sola firma statica, o utilizzando insieme ad essa le caratteristiche dinamiche inserite in fase di registrazione dell'utente. La tecnica di watermarking proposta si basa sulle proprietà della trasformata Radon, essendo quest'ultima particolarmente adatta a trattare immagini con bordi evidenti, quali sono le immagini delle firme.

L'efficacia dei metodi proposti viene valutata utilizzando il database pubblico di firme dinamiche MCYT, il quale contiene firme acquuisite da 100 soggetti diversi.

To my mother and my father, for having always supported me.

To Valentina, for having stayed close to me.

A mia madre e mio padre, per avermi sempre supportato.

A Valentina, per essermi stata vicina.

Acknowledgments

Choosing to focus all my energies on this Ph.D. has not been an easy decision four years ago. Leaving a secure job to dedicate myself to a project without specific guarantees, with the only exceptions of my dedication and the pleasure I feel in engaging myself in research and teaching, would not have been possible without the people I've been lucky to have at my side.

First of all, I wish to thank my parents for all the support and the love they gave me during my life, and especially during these last three years. I also thank my grandparents, who have always reminded me the simple things which are really important in life.

I thank Prof. Campisi, who always showed me an example hardly improvable of motivation and application, and has guided me throughout these years in my research, as well as Professor Neri, who gave me the opportunity to follow this path, and from which I've could benefit for his vision. I also thank Prof. Ortega-Garcia of the "Universidad Autonoma de Madrid", for giving me the opportunity to spend the most significant period of my Ph.D. at the ATVS research group in Spain. I've learned a lot during that time, both from a professional and human point of view, I'll always carry bright memories of those days and of Madrid. I'm also grateful to Professor Ortega-Garcia for having accepted to participate as an expert member during the discussion of my Ph.D. dissertation, as well as deeply grateful to Prof. Fairhurst and Prof. Garcia-Salicetti for their valuable comments and suggestions, which have greatly enhanced this thesis. I thank all the mates and comrades I've met during this period, both at "Roma Tre" as well as at the "Universidad Autonoma de Madrid". These years would have deserved to be spent even only for the possibility of having met each of them. I want also to thank all the friends that I know since the early years of university (and even before), for having had the possibility of share doubts, concerns, vents, joys, achievements, laughs and more with them.

Last, but not least, I wish to thank Valentina for having stayed close to me, for having supported me and made me happy during these years, and for having let me imagine how I'd like my future to be.

Ringraziamenti

Decidere di focalizzare tutte le mie energie su un dottorato di ricerca non è stata una scelta facile quattro anni fa. Lasciare un lavoro sicuro, per dedicarsi ad un progetto senza particolari garanzie, eccezion fatta per la mia dedizione ed il piacere che provo nell'impegnarmi nella ricerca e nella didattica, non sarebbe stato possibile senza le persone che ho avuto la fortuna di avere vicino.

Prima di tutto, desidero pertanto ringraziare i miei genitori, per tutto il supporto ed il bene che mi hanno dato nel corso della mia vita, ed in modo speciale durante questi ultimi tre anni. Ringrazio anche i miei nonni che mi hanno sempre ricordato quali sono le cose semplici ma realmente importanti nella vita di una persona.

Ringrazio il Prof. Campisi, che mi ha mostrato un esempio difficilmente migliorabile di motivazione ed applicazione, e mi ha guidato durante questi anni nelle mia ricerca, ed il Prof. Neri, che mi ha dato la possibilità di seguire questa strada, e del quale ho potuto beneficiare per la sua visione. Ringrazio inoltre il Prof. Ortega-Garcia della "Universidad Autonoma de Madrid", per avermi dato l'opportunità di trascorrere il periodo più significativo del mio dottorato presso il suo gruppo di ricerca ATVS in Spagna. Ho appreso molto durante quel periodo, professionalmente ed umanamente, e porterò sempre un ricordo luminoso di quei giorni e di Madrid. Al Prof. Ortega-Garcia sono inoltre riconoscente per aver accettato di partecipare come membro esperto di commissione per la discussione della mia tesi di dottorato, così come ringrazio profondamente il Prof. Fairhurst e la Prof. Garcia-Salicetti per i loro preziosi commenti e suggerimenti, che hanno contribuito a migliorare significativamente questa tesi. Ringrazio tutti i ragazzi e i compagni che ho avuto modo di conoscere durante questo periodo, tutti i ragazzi di "Roma Tre" come quelli della "Universidad Autonoma de Madrid". Questi anni avrebbero meritato di essere spesi anche solo per la possibilità di aver conosciuto ciascuno di loro. Voglio ringraziare anche tutti gli amici che conosco dai primi anni di Università (ed anche da prima), per aver potuto condividere con loro dubbi, perplessità, sfoghi, gioie, successi, risate e tanto altro.

Per ultima, non certo per importanza, desidero ringraziare Valentina per essermi stata vicina, per avermi rallegrato e sostenuto durante questi anni, e per avermi fatto immaginare come vorrei fosse il mio futuro.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The field of *information security* [1] has evolved rapidly and significantly during recent years. One of the main factors which have driven its development can be found in the widespread use of electronic data processing, an example of which is represented by the electronic business conducted through the Internet. Also the numerous occurrences of international terrorism emergencies have contributed in generating a huge need of better methods for protecting computers, along with the information they store, process and transmit.

Information security deals with the protection of any kind of information from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. It is often used interchangeably with the term *computer security*, although information security has a broader connotation: in fact, it is not concerned with the form the considered data may take, which can be electronic, print, or others.

The core principles of information security rely on the concepts of *confidentiality*, *integrity* and *availability*:

- confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. It is typically enforced by employing cryptographic techniques, by limiting the places where the information can appear, and by restricting the access to the places where the information is stored;

- integrity means that data cannot be modified without authorization;

- availability means that, in any information system, the information must be available when it is needed. Thus, the computing systems used to store and process the information, the security controls used to protect it, as well as the communication channels used to access it, always have to function correctly.

In addition to confidentiality, integrity and availability, also *authenticity* and *non-repudiation* are often considered. The authenticity requirement concerns with the necessity to ensure that data, transactions, communications or documents are genuine. Non-repudiation implies that the parties involved in a transaction can not deny having performed it.

Many disciplines can be considered under the “umbrella” of information security. Among them, *identity management* represents a fundamental issue, which has recently received an increasing interest by the research community. In fact, both governments and private companies are usually involved with the development of identity management systems, in order to provide access control to places and services, such as bank accounts or countries at international border crossings, buildings or computer applications, and so on.

The identity management process deals with the identity life cycles of the considered entities, which can be subjects or objects. It is then responsible for:

- the creation of an identity, and the establishment of a link between the identity and the considered entity;
- the maintenance of an identity, which can consists in the assignment of attributes to the entities;
- the destruction of an identity.

Specifically, when the considered entities are individuals, the problem of establishing (which can mean determining or verifying) the identity of a person is indicated as *people recognition* or *authentication*, and it is a critical task in any identity management system. The employed identities can be generated by employing two different kinds of identifiers: social or biological. Creating a social identity requires an authority to certify that the concerned person is effectively the individual he says to be. This check is usually performed employing already available identifiers: for instance, it happens when parents register the birth of their children, which is certified by appropriate medical records. When the identity of a subject has been confirmed, the considered authority can release physical (e.g., ID cards, tokens) or logical (e.g., personal identification numbers, passwords) identifiers. Thus, such identifiers can be employed to establish the identity of a person, using “something known” in the case of logical identifiers, of “something possessed” in the case of physical identifiers.

However, the use of identifiers such as passwords or ID cards in an identity management system has several drawbacks. Specifically, the major connected risk consists in the possibility of *identity theft*, that is the possibility, for an unauthorized user, of employing a legitimate user’s identifier to gain access to a given resource. In fact, passwords can be easily guessed employing social engineering [2] or dictionary attacks [3]. Moreover, they often do not provide the expected security due to their limited length: the National Institute of Standards and Technology (NIST) have estimated that the average length of commonly employed passwords is 8 ASCII characters, which can guarantee an approximate value of 18 bits of entropy [4], much less than the expected minimum of 56 bits for a provably secure system. Recent Internet threats, such as the so called “phishing”, have also demonstrated that the most of people do not pay enough attention to the disclosure of their passwords to untrusted parties. Serial numbers are more difficult to guess by an attacker than passwords, and usually longer; however, their use is typically less comfortable and immediate Moreover, they are often employed in conjunction with storage device such as magnetic cards, being in this case considered as a sort of physical identifiers. Also ID cards, or tokens in general, are subjected to thefts, which even not require specialized attacks as in the case of passwords. It is also worth pointing out that logical identifiers can be forgotten, as well as physical identifiers can be lost. Re-issuing new identifiers for a given identity always has a cost for an identity management system, which increases with the probability of a user to forget or loose its identifier. Moreover, passwords and ID cards cannot provide non-repudiation: the users of the considered system can easily deny the use of a service, by simply claiming that their passwords have been stolen or guessed. Individuals can also conceal their true identity by presenting forged or duplicate identifiers, which can not be verified instantaneously by security attendants, due to possible difficulties in contacting the considered certifying authority.

Therefore, it is becoming increasingly evident that knowledge-based and possessionbased approaches, by themselves, can not represent efficient solutions for reliable identity recognition processes. For this reason, the most recent developments in identity management have led to solutions where individuals' social and biological identifiers are joined together, to provide greater certainty about the authenticity of a queried identity, and thus implementing strong and secure authentication schemes. The use of biological identifiers or, more generally, the use of "something you are" for people recognition purposes, is commonly indicated as *biometrics* [5].

1.1 Biometric Systems

The term biometrics derives from two Greek words, *bios* and *metron*, which respectively mean "life" and "measure". Specifically, in the context of identity management, the term biometrics is commonly employed with two different meanings: it is usually employed to indicate the process of measuring and analyzing any *physical* or *behavioral* human characteristics, performed in order to automatically recognize individuals [6, 7]. Moreover, it can also be used to indicate the characteristic itself, depending on the context.

The use of specific traits for people recognition is the method most commonly employed for thousands of years by humans to recognize each others. However, the first practical people recognition system has been implemented only in the mid 19th century by Alphonse Bertillon . Bertillon, who was the chief of the criminal identification division of the police department in Paris, used a number of body measurements (height, weight, length of arms and legs, and so on) to identify criminals. In late 19th century, the use of these measurements has been overtaken by a far more significant and distinctive measurement of human body: the fingerprints. During the last century, the use of fingerprints for criminals identification has been adopted by the most of law enforcement departments in the whole world, and the number of fingerprints stored in the employed databases has given risen to an unavoidable need for automatic fingerprint identification systems (AFIS). Although biometrics emerged from its extensive use in law enforcement and forensic applications, it is currently the most promising technology for automatic people recognition in civilian applications. Examples of physical traits which have been employed in biometric based recognition systems include face [8], fingerprint [9], iris [10], retina [11], palmprint [12], hand geometry [13], ear shape

[14], thermogram [15], DNA [16], body odor [17], vein patterns [18], and also electrocardiogram [19] or brain waves [20]. Between the considered behavioral characteristics, the most employed so far are signature [21], handwriting [22], gait [23], keystroke [24] or lip motion [25]. Voice [26] is usually considered as a biometrics related to both physical and behavioral attributes, due to the fact that it is determined by characteristics such as pitch or nasality, connected to the shape of the vocal tract, and also by peculiarities such as pronunciation, dialect, or identifiable use of specific words.

Since many of the cited characteristics are unique to an individual, biometrics can be properly used as individuals' identifiers, thus providing a mean of authentication much more reliable than ID cards, keys, passwords, or other traditional systems. Moreover, biometric traits are more difficult to be forgotten, lost, stolen, copied or forged than traditional data, thus representing a much more robust solution than traditional approaches, when considering the threat of identity theft. In addition, since biometric systems usually require the user to be present when the recognition process is performed, they can also be employed for applications requiring non-repudiation.

However, it is worth pointing out that each biometrics has its own advantages and limitations, and that no single trait can effectively meet the requirements of all possible applications. Specifically, a given biometric characteristic can be described according to the following parameters [27]:

- *universality*: each person should have the considered biometrics;
- *distinctiveness*: it should be possible to distinguish two persons, selected according to any rule, on the basis of the considered biometrics;
- *permanence*: a biometric trait, or at least the information which can be extracted from it, should be sufficiently invariant over a period of time;
- *collectability*: the biometrics can be measured quantitatively, with the less possible effort of both the individual and the system.

Moreover, the capability of a given biometrics in being used for a specific application is typically measured according to the following requirements:

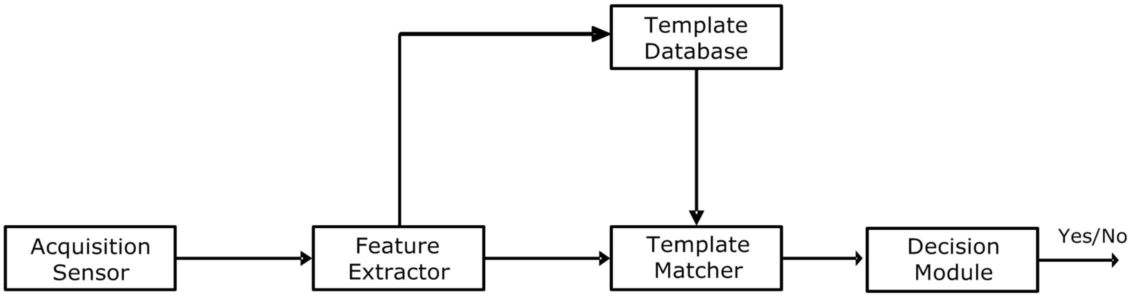


Figure 1.1: Framework of a biometric recognition system.

- *performance*: both the time needed to process the biometrics, and the recognition accuracy which can be achieved employing it, should satisfy the requirements given by the operational and environmental factors of the considered application;
- *acceptability*: this requirements refers to the willing of individuals to accept their biometrics to be the used for a specific application;
- *circumvention*: the considered biometrics should be difficult to copy, forge or steal, thus making the application difficult to be fooled by fraudulent methods.

1.1.1 Framework of a Biometric Recognition Systems

Loosely speaking, biometric systems are essentially pattern recognition applications, where the considered patterns are given by the users' physiological or behavioral characteristics. As in the classical framework of a pattern recognition system, a generic biometric system can be represented as a cascade of five main modules [6], as depicted in Figure 1.1:

- the acquisition sensor;
- the feature extractor;
- the template database;
- the template matcher;
- the decision module.

Specifically, the acquisition sensor captures the biometrics of the system's users. In practical applications, this module should first evaluate, according to a given algorithm, the quality of the acquired biometrics: if the acquisition quality is poor, the biometrics should be re-acquired from the user. For instance, if the considered biometrics is acquired through an image acquisition device, as it happens for iris, an estimation of the image blurring can be evaluated: if this value is too high, a new acquisition has to be performed.

The feature extraction module then process the acquired data, in order to extract a set of salient and discriminatory *features* from it. For example, when fingerprints are considered as the given biometrics, the feature extraction module derive the position and orientation of minutiae points (local ridge and valley singularities) in the acquired fingerprint image. The generated feature set is commonly indicated as the *biometric template*, which is considered as a new representation of the given characteristic. The employed template should consists of all the relevant information contained in the original biometrics, in order to make it available for recognition purposes. It is also worth noticing that the templates extracted from the biometrics of a given user, for different acquisitions, should show a very low variability (small intra-user variability). Moreover, they should be enough different from the templates extracted by other users, being thus possible to consider them unique for a single subject (small inter-user similarity).

The templates extracted from a user can then be stored in the template database, or sent to the template matcher. In this latter case, they are compared with those templates which have been previously stored in the database, in order to evaluate a degree of similarity between them. The obtained measure, usually indicated as *similarity score*, is then fed to the decision module, which decides whether or not the considered templates are generated from the same person.

The templates generated by the feature extraction module are stored or sent to the template matching module, depending on which phase the system is performing. The possible phases which are implemented in a biometric recognition system are detailed in Section 1.1.2.

1.1.2 Phases of a Biometric Recognition Systems

Biometric authentication systems always consist of two phases: the *enrollment* and the *authentication* ones. During the enrollment phase, biometric data are captured from a subject, and checked for their quality. Then, relevant information is extracted, and eventually stored in a database. As for authentication (which is commonly indicated also as recognition), two modalities can be implemented:

- *verification*: the subject who claims an identity presents some form of identifier (an ID card, a username) and a biometric characteristic. The system extracts some features from the acquired data, and compares the features corresponding to the provided ID, which are stored in the system database, with the provided ones. Identity verification is typically used for the so called *positive recognition*, where the aim is to prevent multiple people from using the same identity [28]. It is worth pointing out that, in this modality, the presented biometric trait is compared only with the one, stored in the centralized/distributed database, corresponding to the declared identity, which implies one or few *one to one* biometric comparisons. The verification problem can be formally stated as follows: given a query biometric representation F_Q, and a claimed identity I, it should be determined if F_Q has been extracted from a biometrics taken by the claimed identity I. This is done by comparing F_Q with the biometric template F_T, stored in the database during the enrollment of the identity I. If the score obtained as output of the template matching module, indicated as $s(F_Q, F_T)$, is higher than a pre-defined *threshold* t (where it is assumed that the higher the score, the more similar are the feature sets F_Q and F_T), then the feature set F_Q is considered to be taken from the claimed identity I. Otherwise, if $s(F_Q, F_T) < t$, the query sample is considered to be taken from an impostor, which is then rejected by the system. It is worth pointing out that many template matching modules produce *dissimilarity distances* as output, instead of scores. In this cases, the more two feature sets F_Q and F_T are similar, the less their distance $d(F_Q, F_T)$ will be. Thus, a user is recognized as the claimes identity when $d(F_Q, F_T) \leq t_d$, or rejected by the system if $d(F_Q, F_T) > t_d$, being t_d the threshold employed to perform a decision;

- *identification*: the system acquires the biometric sample from the subject, extracts some features from the raw measurements, and searches for matches the entire database, using the extracted biometric features. When the authentication system operates in the identification modality, *one to many* biometric comparisons are realized. Performing many template comparison can require a large amount of processing time. In order to limit the time needed to identify an individual, *scalable systems* are usually employed. In such systems, the database where the search has to be performed is typically first analyzed by employing individuals' ancillary attributes, like those employed in the first biometric system of Bertillon. Information regarding gender, age, scars, tattoo, and so on, have also been proposed in practical biometric based recognition system [29]. These attributes do not provide enough distinctiveness to precisely determine the identity of individuals, and are therefore indicated as *soft biometrics*. However, they can be employed to rapidly isolate limited sub-sets of identities, over which the identification process can be performed with reduced processing time. Differently from verification, an identification process is usually performed in *negative recognition* applications, where the system has to establish whether the individual is who he denies to be. The purpose of negative recognition is therefore to prevent a single person from using multiple identities [28]. However, an identification process can also be performed in the context of a positive recognition, for example when this approach can be convenient for the enrolled users, which are not requested to claim their identity when they want to be recognized. It is worth pointing out that, while traditional methods employing passwords or tokens can perform positive recognition, negative recognition can only be established through biometrics.

1.1.3 Performance Evaluation

Al already stated, the quality of a biometric recognition systems can be evaluated on the basis of the acceptability, the circumvention and the performance guaranteed by the employed biometric characteristic. In fact, the system should be able to manage the *exceptions* which can occur when a user does not want to use the biometric system, does not have the biometrics, or when it is not possible, for some transitory conditions, to acquire the biometrics. Moreover, in a scenario where biometrics can be used to grant physical or logical access, *security* issues regarding the whole biometric system become of paramount importance, in order to not allow any form of circumvention or unauthorized use of the system. In addition, design parameters like the *computational speed*, which is related to the time necessary to the system to take a decision, have to be taken into account, and should be arranged in order to make the system perform at its best.

However, when considering an automatic verification system, first of all it obviously has to be *accurate*, in the sense that it should recognize the maximum number of authorized users, whereas it must minimize the number of non-authorized subjects which are accepted by the system. It is worth pointing out that, for any biometrics, for the observed features of an individual there is always an unavoidable intra-user variability over time. In fact, also for those traits which do not change over time, like for example iris, the generation of a template is subordinate to an interaction between the biometric trait and the acquisition module. This interaction is necessarily different when performed in two different instants, due for example to changes in the users physiological or behavioral characteristics, or to the ambient conditions, thus introducing an element of variability even where the biometrics itself do not change over time.

A biometric verification system can make two distinct types of errors:

- error of Type I: mistaking biometric measurements from two different persons as being taken from the same person, typically due to a significant inter-user similarity. This is commonly indicated as a *false match*, and when this happens the system commits a *false accept*;

- error of Type II: mistaking two biometric measurements from the same person as being acquired from two different persons, typically due to a large intra-user variability. This is commonly indicated as a *false non match*, and when this happens the system commits a *false reject*.

The metrics most commonly employed when defining the performances of a biometric recognition system therefore are:

- the False Rejection Rate (FRR), defined as the ratio between the estimated false reject, and the total number of attempts made by authorized individuals to gain access to the system, by claiming their identity;

- the False Acceptance Rate (FAR), defined as the ratio between the estimated false

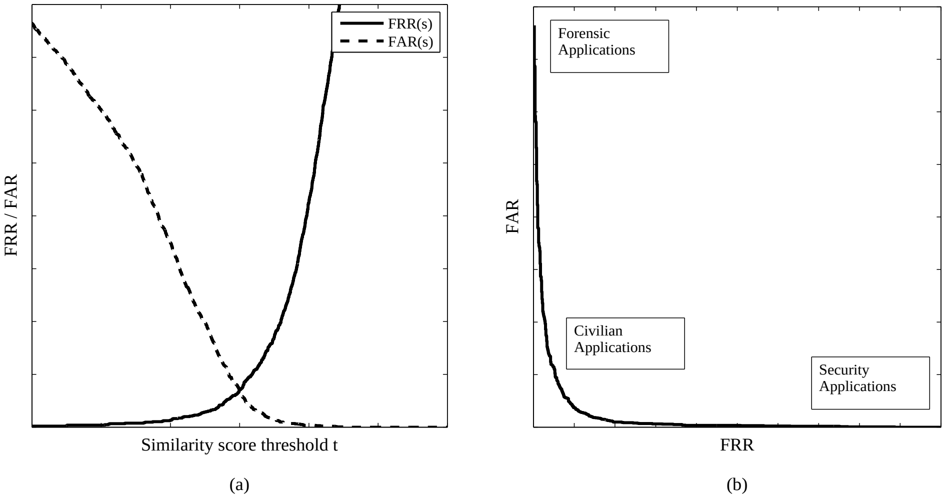


Figure 1.2: Performance descriptors for biometric systems. (a): FRR and FAR with respect of the similarity score s; (b): ROC curve.

accepts, and the total number of attempts made by impostors to gain access to the system, by claiming identities of authorized users.

Obviously, there is a tradeoff between FRR and FAR. In fact, both FRR and FAR can be expressed as functions of the system threshold t, introduced in Section 1.1.2: if the threshold t decreases, the system will be more tolerant to input variations and noise, thus producing a worsening of the performances in terms of FAR, although an improvement in terms of FRR will also be introduced. On the other hand, if the threshold t increases, then the FAR will decrease, while the performances in terms of FRR will get worse. Figure 1.2(a) shows the typical behavior of the FRR and the FAR for various values of the threshold t. However, the system performances at all the operating points (thresholds) are usually depicted employing a single function, which displays the FAR against the FRR for various threshold values. This function represents the Receiver Operating Characteristic (ROC) curve of the considered system, and an example is given in Figure 1.2(b). It is possible to determine, for a given biometric system, typical operating points using its performance representation in terms of a ROC curve. Specifically, high security application, where the primary objective is deterring impostors, typically require low values of FAR. On the other hand, forensic application such as criminal identification are more interested in low FRRs:

it is more desirable to miss the identification of a criminal, than to manually examine a large number of incorrect matches. The most of civilian applications usually employ operating points which lie in between these two extremes, where both FRR and FAR need to be considered. The point at which the FRR and the FAR assume the same value is referred to as the Equal Error Rate (EER). Setting the system threshold at the operating point where the EER is met, the proportion of false accepts is equal to the proportion of false rejects. This operating point is commonly considered as the most representative quality measure of a biometric system: the lower the EER value, the higher the accuracy of the biometric system.

Besides the above error rates, the Failure To Capture (FTC) rate, together with the Failure To Enroll (FTE) rate, are also used to describe the accuracy of a biometric system. The FTC rate is only applicable when the biometric device has an automatic capture functionality implemented in it, and denotes the percentage of times the biometric device fails to capture a presented biometric characteristic. This kind of error typically occurs when the device is not able to locate a biometric signal of sufficient quality. The FTE rate, on the other hand, denotes the percentage of users which are not able to be enrolled in the recognition system. FTE errors typically occur when the system rejects poor quality inputs during enrollment. Consequently, there is usually a correlation between the FTE and the system accuracy measures (FRR and FAR): if only good quality templates can be stored in the system, the resulting system accuracy obviously improves. All these metrics, namely the FRR, the FAR, the FTE, and the FTC, constitute important specifications in a biometric system, and should be reported during performance evaluation.

1.1.4 Applications and Issues

Biometric recognition systems are nowadays employed in many applications, with the aim of performing automatic people verification or identification. Specifically, the applications in which biometrics can be involved are typically divided into three main groups:

- *commercial applications* such as remote access on Internet or other computer applications, electronic data security, physical access control to buildings or places, medical records management, distance learning;

- *government applications* such as national ID card, drivers license, social security, border and passport control;
- *forensic applications* such as terrorist identification, corpse identification, criminal investigation, parenthood determination, and missing children.

However, in spite of the great interest risen about biometrics, the practical applications based in biometrics which have been deployed are still few, in comparison to the potential which could be expressed. This is due to the fact that biometric recognition is not yet a fully solved problem, and then the interested companies still have various perplexities about employing biometric data in their identity management systems. As already stated, the principal aspect of a biometric system about which discussions are taken is its accuracy. However, many other aspects of a biometric system have to be considered, like for example its *scalability*, which is connected to the size of the system database. Specifically, the issue of scalability is not critical for verification systems, which perform authentication by matching a query biometrics with a single stored template. However, it becomes an issue of paramount importance when dealing with identification systems, where the input biometrics has to be compared sequentially with all the templates enrolled in the system. The processing time needed to perform such operation increases linearly with the size of the database, and rapidly becomes unaffordable when the population size is in the order of millions of enrolled subjects, as it can easily happen for government or forensic application. It has been already described how this issue can be managed by employing processes such as filtering or indexing, where the database is first pruned on the basis of ancillary information related to the subject (like the already introduced soft biometrics), or considering high level information directly related to the considered biometrics (like the fingerprint pattern class, for a fingerprint based recognition system). The search is thus restricted to a database whose size is smaller than the original one.

Another challenge which has to be considered when deploying biometric recognition systems is the currently lack of a widely accepted standardization. Actually, many non-homogeneous solutions have been already proposed by researcher and companies for terminologies, technical interfaces, data formats, and so on. Recently, many efforts have been spent by the NIST and the American National Standards Institute (ANSI) to provide a commonly accepted standardization of biometrics related definitions and procedures. Specifically, the most of these tasks are carried out by the *ISO/IEC Joint Technical Committee* 1 *(JTC* 1*) Subcommittee* 37 *(SC* 37*) Biometrics*, established in June 2002.

However, what probably seems to be the most important issue which have to be solved for the deployment of practical biometric recognition systems regards their usability. Specifically, the usability of a biometric recognition system is determined by the ease of use, for an individual, of the system itself, and is strictly connected with the serious security and privacy concerns which have to be considered when dealing with biometric data. In fact, the most of people which are reluctant to use their biometric data in an automatic system fear the possibility of an identity theft: differently from what happens using password or tokens, which can be re-issued if lost or forged, biometric data are permanent, and if compromised they can not be used anymore.

The security and privacy issues, regarding the use of biometric data for automatic people authentication systems, are the main topic of this Thesis. Specifically, after having discussed in detail which security implications should be considered when dealing with biometric characteristics, different solutions will be provided as possible countermeasures to improve the security of a biometric recognition system.

1.2 Summary

The most emerging technology for identity management applications is biometrics. It can be defined as the analysis of physiological or behavioral people characteristics for automatic people recognition. Biometric authentication relies on who a person is or what a person does, in contrast with traditional approaches, based on what a person knows, such as password or personal identification numbers (PIN), or what a person has, like ID cards, keys, or tokens. Biometric authentication is based on strictly personal traits, which are much more difficult to be forgotten, lost, stolen, copied or forged than traditional data, and represent irrefutable evidences linking a person to his identity. Biometric recognition systems offer a number of functionalities such as verification or identification.

However, there are still a number of open issues which have to be solved in order to make biometric system widely deployed and accepted. Among them, the issues regarding the security and privacy of the employed biometric data greatly affect the usability of the system itself: when there is the possibility that these characteristics can be stolen or forged, the possible system's users are typically unwilling to employ their biometric trait.

1.3 Thesis Contribution and Outline

This Thesis is focused on the security issues related to biometric templates, with specific reference to on-line signature based authentication systems.

In Chapter 2 the main privacy and security issues which affect biometric recognition systems are briefly summarized, and the approaches already proposed for the protection of biometric templates are discussed.

Since this contribution is presented within the context of signature biometrics, Chapter 3 is related to the state of the art on signature recognition.

Chapters from 4 to 6 are dedicated to the proposed approaches for the implementation of signature recognition systems which provides protection to the employed templates. Specifically, the approaches presented in this Thesis have been defined to cover all the possible aspects which can be investigated in order to protect signature templates, as it will be discussed in more detailed in Chapter 3.

A biometric cryptosystem whose parameters are tuned to the variability of each user's biometrics is proposed in Chapter 4, where an application to on-line signature based authentication is considered.

A template protection scheme for sequence based biometrics, which employs a set of non-invertible transforms, is described in Chapter 5 and applied to an on-line signature recognition system.

In Chapter 6 a different perspective is taken: data hiding techniques, already proposed for the protection of biometric templates, as illustrated in Chapter 2, are employed to design a security scalable authentication system base on signature.

Eventually, the conclusions and the possible future works are discussed in Chapter 7.

Chapter 2

Privacy Issues and Countermeasures for Biometric Recognition

As discussed in Chapter 1, biometric recognition systems represent an alternative to traditional approaches, able to guarantee improved security and comfort for their users. However, the use of biometric data arises many *privacy* and *security issues* [30, 31, 32], not affecting other methods employed for automatic people recognition. In a scenario where biometrics can be used to grant physical or logical access to places or resources, security issues regarding the whole biometric system become of paramount importance.

As outlined in [30], when an individual gives out his biometrics, either willingly or unwillingly, he discloses unique information about his identity. This implies that his biometrics can be easily replicated and misused. Moreover, biometrics cannot be renewed or reissued since users have a limited number of observable features, which is in contrast with the use of passwords and tokens, which can be easily reissued. It has also been demonstrated that biometric data can contain relevant information regarding people personality and health [33, 34]. This information can be used, for example, to discriminate people for hiring, or to deny insurances to people with latent health problems or lifestyle preferences. In addition, as highlighted in [30], to some extent the *loss of anonymity* can be directly perceived by the users as a *loss of autonomy*. In a scenario where a governmental agency can collect huge databases of citizens, it could monitor their behavior and actions. *Function creep*, that is a situation where the data, collected for some specific purposes, are used for different ones, is likely to happen in the long run. The use of biometrics can also rise cultural, religious as well as physical concerns, either real or unmotivated, on the invasiveness of the acquisition process.

Therefore, the need to protect the privacy both from a procedural point of view, as well as from a technological point of view, necessarily arises.

In this Chapter, the main privacy concerns related to the deployment of biometric based authentication systems are discussed. In Section 2.1, the main threats which can be affect a biometric recognition system are presented. In Section 2.2 an operational definition of privacy is given, and its implications when dealing with biometric data are outlined. Eventually, in Section 2.4 the state of the art regarding Privacy Enhancing Technologies (PETs) is described. Eventually, a brief review of the standardization activities involving privacy and biometrics, as well as the description of some initiatives which are currently in progress and regards bioethical implications of biometric identification technologies, are provided in Section 2.5.

2.1 Biometric Systems Vulnerabilities

The main security concerns related to a biometric based authentication system are pointed out in [35]:

- can biometrics be stolen?
- can biometrics be acquired without the user authorization?
- can biometrics be repudiated?
- which kind of side information biometrics can reveal about an individual?
- is it possible to understand when a system becomes insecure?
- how can we prevent administrator misuse?

- can an operator track, identify and then steel the identity of an individual?

More specifically, in [36, 37, 38, 39] the main treats to a biometric system have been identified as:

- *repudiation*, when a legitimate user denies to have accessed the system;
- *collusion*, when a super-user grants access to an unauthorized user, in order to fool the system;
- *circumvention*, when an illegitimate user gains access to the system;
- *denial of service*, when massive attacks on the system cause the system failure;
- *coercion*, when an impostor forces a legitimate user to grant him access to the system;
- *covert acquisition*, when biometric traits are covertly taken from the legitimate user.

As can be seen, these threats can be due both to an intrinsic system failure, consequence of incorrect decisions made by the system, as well as to a failure due an intentional attacker's action [40].

As outlined in Chapter 1, a biometric authentication system can be sketched as the cascade of the sensor for the acquisition, the feature extractor module, and the module that performs matching between the output of the feature extractor and the templates stored in the database. Eventually, a decision regarding the identity of the queried subject is performed.

As discussed in [41], and also illustrated in Figure 2.1, eight possible vulnerable points can be identified within this general framework. Specifically, the potential attacks toward a biometric system can be perpetrated at the sensor level, where fake biometrics can be presented, at the feature extractor level that could be forced by an attacker to produce pre-selected features, at the matcher level, which can be attacked to produce fake scores, and at the database level that can be somehow altered. Moreover, the channels interconnecting the different parts of a biometric system, like the channel between the sensor and the feature extractor, between the feature extractor and the matcher, between the database and the

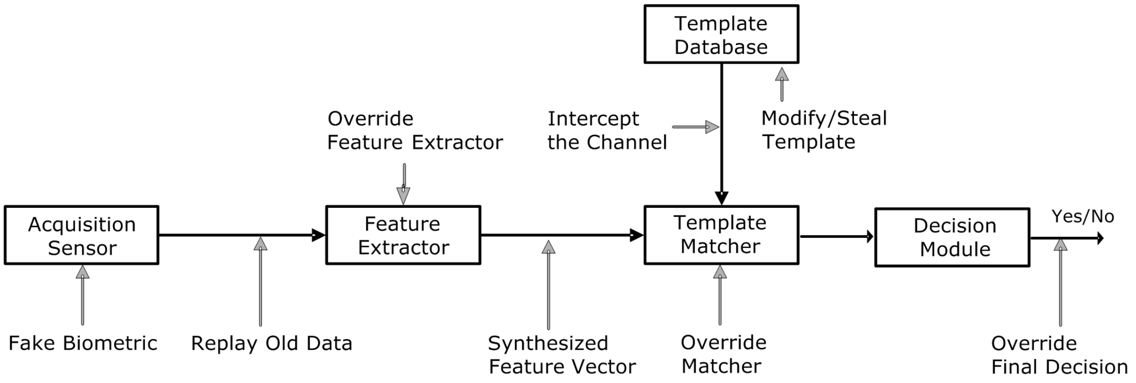


Figure 2.1: Points of attack in a generic biometric system (adapted from [41]).

matcher, and between the matcher and the application device, can be intercepted and controlled by unauthorized people.

Among the attacks which can be perpetrated at the sensor level, we can cite the *spoofing attack* and the *mimicry attack*, which are related to physiological and behavioral biometrics, respectively. These attacks consist in copying, by means of different strategies, the biometric feature of the enrolled user, and to transfer it to an impostor in order to fool the system. The *reply attack*, which consists in capturing first and in replying at a later time the stolen biometrics, in order to get unauthorized access to the system, is of primary concern. Although it was commonly believed that it is not possible to reconstruct the original biometric data starting from the corresponding extracted template, some concrete counter examples, which contradicts this assumption, have been provided for faces in [42], where a *Hill Climbing* attack is used to regenerate a face from face templates. In [37], a synthetic fingerprints template generator is devised using the *Hill Climbing* attack. A general *Hill Climbing* attack based on Bayesian adaption is described in [43] with application to signature verification. In [44], fingerprints are regenerated from the orientation map of the minutia template.

2.2 Biometric Systems: privacy and security concerns

The successful deployment of any biometric system in real life applications depends on user acceptance, for which privacy represents a critical issue. Specifically, the very fundamental question a system designer has to answer is whether biometric authentication is perceived as a privacy invasive measure, instead of a privacy protective one.

The word *privacy* is a general term which encompasses both different areas of study and real life situations. It is commonly accepted [45, 46] that the general term privacy can assume slightly different connotations. Specifically, we can talk about:

- *decisional privacy* when we refer to the right of the individual to make decisions regarding his life without any undue interferences;
- *spatial privacy* when we refer to the right of the individual to have his own personal physical spaces which cannot be violated without his explicit consent;
- *intentional privacy* when we refer to the right of the individual to forbid/prevent further communication of observable events (e.g., conversations held in public) or exposed features (e.g. publishing photos);
- *informational privacy* when we refer to the right of the individual to limit access to personal information which represents any information that could be used in any way to identify an individual. It is worth pointing out that some data which do not appear to be personal information could be used in the future to identify an individual.

According to the application, a particular privacy conceptualization may be chosen as prevalent, still being the other aspects worth to be considered in the privacy assessment. Specifically, when dealing with biometrics, a combination of decisional, spatial, intentional, and informational privacy aspects could be taken into account. In fact, as pointed out in [45], a biometric trait can be either:

- covertly acquired, thus impairing the user's right to decisional privacy;
- acquired in the user's physical spaces, thus compromising the spatial privacy;
- acquired when exposed to the public, in which case the intentional privacy is compromised;
- used to identify the individual, thus impairing the user's right to informational privacy.

However, within the outlined framework, informational privacy is commonly considered as the predominant aspect when discussing privacy protection assessments for biometrics.

It is well known that the privacy assessment of an information technology system has to be done at the earliest stages of its design, in order to embed into the system the answers to the privacy concerns which have been identified, and to limit the potential costs deriving from negligent information management. In order to properly illustrate the main concerns which have to be addressed by a privacy assessment related to the use of biometrics, it is worth pointing out clearly that, as well established in literature, biometric data are not secret.

In fact, features such as voice, face, fingerprints and many others, can be covertly acquired or stolen by an attacker, and then misused. This will directly lead to identity theft. Moreover, biometrics cannot be revoked, canceled, or reissued if compromised, since they are user's intrinsic characteristics, and they are in limited number. Therefore, if a biometrics is compromised, all the applications making use of that biometrics are compromised, and being biometrics permanent, an issue is raised when it is needed to change it.

The following concerns have therefore to be considered when deploying a biometric based application:

- biometrics can be collected or shared without specific user's permission, adequate knowledge, or without specific purpose;

- biometrics, which has been collected for some specific purposes, can be later used for another unintended or unauthorized purpose (function creep). This possibility can have dramatic consequence, since it brings to the destruction of the public trust in a given system.

- biometrics use can violate the "principle of proportionality" [47], which states that biometric data may only be used if adequate, relevant and not excessive with respect to the system's goal. If this principle is violated, the users may feel that the benefit coming from donating their biometrics is much less than what they get in exchange. As an example, it is very likely that a retinal scan authentication system used at a Point-of-Sale makes the user uncomfortable, whereas the use of dynamic signature biometrics is more accepted by users.

- biometrics can be used to reveal gender and ethnicity. Moreover, details on the medical history of the individual can be elicited. Medical conditions can be deduced by comparing biometrics acquired at the time of the enrolment and biometrics acquired later for authentication. Biometrics can also give directly information on health conditions: as a consequence, biometrics can be used to profile people according to their health status.

- biometrics can be used to pinpoint or track individuals. Being biometric data considered unique, they have the potential to locate and track people physically as they try to access some facilities, or their biometric traits are recorder by some surveillance system. Also associating people's biometrics to their identifiers, such as name, address, passport number, can represent a risk, being then possible to access, gather and compare a wide range of information starting from a single biometric trait. Moreover the use of biometrics as universal identifier can allow user tracking across different databases. All this can lead to covert surveillance, profiling, and social control.

- biometric use can be associated by the individual to forensic purposes. Therefore, the use of biometric traits such as fingerprints, which are associated for historical reasons to forensic activities, can have a low acceptability rate.

- biometric technology can be harmful to the user.

- biometrics can be improperly stored and/or transmitted. This would expose biometrics to external attacks. Moreover, biometrics is also exposed to administrator or operator abuses, since they could misuse their privileges for accessing the biometric database.

In addition to the aforementioned general concerns, an estimate of the real privacy invasiveness, as discussed in [48], should be evaluated by considering both the final application, as well as the employed biometric trait. Among the possible considerations, it has been noticed that:

- biometric overt applications are less privacy invasive than covert ones;

- mandatory biometric based authentication systems bears more privacy risks than optional ones;
- the privacy risks increases when the biometric data are stored for an unlimited amount of time. In fact, if the system deployment is indefinite in time, threats such as function creep may arise;
- biometric systems which retain identifiable biometrics, such as faces, voice patterns, and so on, are more prone to privacy risks than those which store templates;
- if the biometric data are stored in a centralized database, serious privacy concerns arise since data are stored out of user's control, whereas if the user can maintain the ownership of the biometric data, less privacy risks can occur since the user can control the collection and the usage of his biometric information.

2.3 Data Protection

To answer the need of deploying privacy protective systems, the issues discussed in Section 2.2 have to be carefully addressed. The International Biometric Group, in the framework of the IBG BioPrivacy Initiative [48], has proposed a set of guidelines for privacy aware deployments. Specifically, four categories of Best Practices have been defined, namely:

- Scope and Capabilities;
- Data Protection;
- User Control of Personal Data;
- Disclosure, Auditing, Accountability and Oversight.

The proposed Best Practices usually regard the modalities in which a biometric recognition system should work in order to not be privacy-invasive, as well as the kinds of data which should be managed. However, when discussing the proposals for data protection, a technological perspective is taken into account, specifying that biometric data must be protected through the different stages of a biometric based authentication system (sensors, aliveness detection, quality checker, features generator, matcher, and decision module).

Among the proposed suggestions, it is pointed out that the data management, such as access to the biometric database, should be limited to a restricted and well defined number of operators, in such a way to limit potential misuse of the stored data. More in detail, the need of implementing PETs, that is, methods which protect from unauthorized access or modification the biometric templates employed by the system, is extensively stressed out as a fundamental requirement for a properly designed biometric authentication systems.

2.4 Privacy Enhancing Technologies

As evident from the previous discussion, template protection is one of the key issues to face when designing a biometric based authentication system. In fact, it is highly desirable to keep secret a template, to revoke, to cancel, or to renew a template when compromised, and also to obtain from the same biometrics different keys to access different locations, either physical or logical, in order to avoid unauthorized tracking.

PETs commonly consists in the application of different kinds of signal processing techniques to the templates extracted from the considered biometrics. The use of PETs should allow the generation of biometric templates accordingly to the following properties [40]:

- *renewability*: it should be possible to revoke a compromised template and reissue a new one based on the same biometric data (also referred to as *revocability* property). Moreover, each template generated from a biometrics should not match with the others previously generated from the same data (also referred to as *diversity* property). This property is absolutely needed to ensure the user's privacy;

- *security*: it must be impossible or computationally hard to obtain the original biometric template from the stored and secure one. This property is needed to prevent an adversary from creating fake biometric traits from stolen templates: in fact, although it was commonly believed that it is not possible to reconstruct the original biometric characteristics from the corresponding extracted template, some concrete counter examples, which contradict this assumption, have been provided in the recent literature, as in [42] or [49]. It is worth pointing out that this property should be satisfied both in the case an attacker is able to acquire one single template, as well as in the case the adversary is able to collect more than a single template, and use them together to recover the original biometric information (this is commonly referred to as the *record multiplicity attack*).

- *performance*: the recognition performance, in terms of False Rejection Rate (FRR) or False Acceptance Rate (FAR), should not degrade significantly with the introduction of a template protection scheme, with respect of an unprotected system. Moreover, it is worth pointing out that the recognition performances should not be sensitive to the employed modifications: applying different processings to the same biometric data, the recognition performances should show very low variance.

The design of a template protection scheme able to properly satisfy each of the aforementioned properties is not a trivial task, mainly due to the unavoidable intra-user variability shown by every biometric trait. In this Section, we analyze the different possible solutions which have been investigated in the recent past to secure biometric templates, and to provide the desirable cancelability and renewability properties to the employed templates. Among them, we discuss the role which *classical cryptography* can play in this scenario, and describe the recently introduced techniques like *data hiding* and *cancelable biometrics.*

2.4.1 Cryptography

Cryptography [50] is a well know studied solution which allows secure transmission of data over a reliable but insecure channel. Within this framework the term security is used to mean that the privacy of the message and its integrity are ensured, and the authenticity of the sender is guaranteed. However, cryptographic systems rely on the use of keys which must be stored and released on a password based authentication protocol. Therefore, the security of a cryptographic system relies on how robust is the password storage system to brute force attacks. Moreover, the use of cryptographic techniques in a biometric based authentication system, where templates are stored after encryption, does not solve the template security issues. In fact, at the authentication stage, when a genuine biometrics is presented to the system, the match can be performed either in the encrypted domain or in the template domain. However, because of the intrinsic noisy nature of biometric data, the match in the encrypted domain would inevitably bring to a failure, because small differences between data would bring to significant differences in the encrypted domain. Therefore, in order to overcome these problems, it would be necessary to perform the match after decryption, which however implies that there is no more security on the biometric templates. Recently, some activity is flourishing to properly define signal processing operations in the encrypted domain [51, 52], which could allow for example to perform operations on encrypted biometric templates on not trusted machines. However, this activity is still in its infancy and does not provide yet tools for our purposes.

2.4.2 Data Hiding

As already outlined, encryption can be applied to ensure the privacy, to protect the integrity, and to authenticate a biometric template. However, among the possible drawbacks, encryption does not provide any protection once the content is decrypted.

On the other hand, *data hiding* techniques [53, 54] can be used to insert additional information, namely the watermark, into a digital object, which can be used for a variety of applications ranging from copy protection, to fingerprinting, broadcast monitoring, data authentication, multimedia indexing, content based retrieval applications, medical imaging applications, and many others. Within this respect, data hiding techniques complements encryption, since the message can remain in the host data even when decryption has been done. However, it is worth pointing out that some security requirements, in a different sense with respect to cryptography, are also needed when dealing with data hiding techniques. In fact, according to the application, we should be able to face *unauthorized embedding*, *unauthorized extraction*, and *unauthorized removal* of the watermark. Two different approaches can be taken when dealing with data hiding techniques: either the information to hide is of primary concern, while the host is not relevant to the final user, in which case we refer to *steganography*, or the host data is of primary concern, and the mark is used to authenticate/validate the host data itself, in which case we refer to *watermarking*. In [55], both the aforementioned scenarios have been considered with applications to biometrics. Specifically, a steganographic approach has been applied to hide fingerprint minutiae, which need to be transmitted through a non secure channel, into a host signal. Moreover, in the same contribution, a watermarking approach has been employed to embed biometric features extracted from face into a fingerprint image. Some approaches for the protection and/or authentication of biometric data using data hiding have been proposed in [56], where robust data hiding techniques are used to embed codes or timestamps, in such a way that after the expiration date the template is useless. In [57], a fragile watermarking method for fingerprint verification is proposed in order to detect tampering while not lowering the verification performances. Also watermarking can be used to implement multi-modal biometric systems, as in [58], where fingerprints are watermarked with face features, in [59], where iris templates are embedded in face images, or in [60], where the voice pattern and the iris image of an individual are hidden in specific blocks of the wavelet transform of his fingerprint image. In [61], a steganographic approach is used to hide into a host image a template that is made cancelable before it is hidden. In [62, 63], the author proposes a signature based biometric system, where watermarking is applied to the signature image in order to hide and keep secret some signature features in a static representation of the signature itself.

However, data hiding techniques are not capable to address the revocability and the cross-matching issues.

It is worth noticing that, although a huge amount of literature has been produced on watermarking in the last years, no equal effort has been devoted to the integration between watermarking and cryptography. A first effort to formalize the points of contact between these two disciplines has been done in [64]. In [65], the commonly believed analogies between watermarking and cryptography are critically discussed, and a layered approach mimicking the Open System Interconnection (OSI) model, where encryption and watermarking are kept distinct, is recommended. Also application scenarios like content authentication and traitor tracing are studied. Even this research field is still in its infancy and much more research effort is needed.

2.4.3 Cancelable Biometrics

Cancelable biometrics, also known as *anonymous* or *revocable biometrics*, probably represent the most interesting approaches proposed for the protection of biometric templates. The

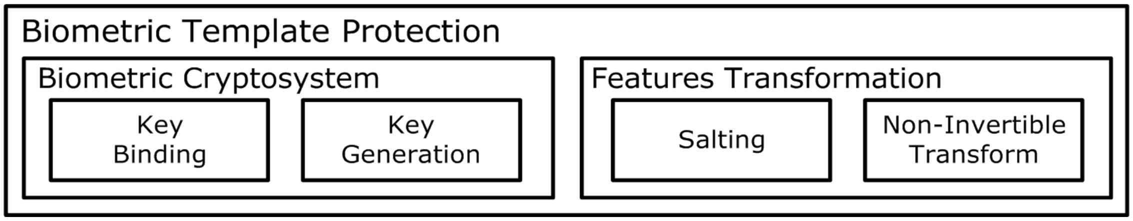


Figure 2.2: Classification of Protection Schemes (adapted from [40]).

concept of cancelable biometrics was introduced in [66], and can be roughly described as the application of an intentional and repeatable modification to the original biometric template, able to guarantee the aforementioned properties of renewability, security and performance.

Different solutions have already been proposed for the generation of secure and renewable templates. A possible classification of these methods was proposed in [40] and sketched in Figure 2.2, consisting of two macro-categories referred to as *biometric cryptosystem* and *feature transformation* approaches.

2.4.3.1 Biometric Cryptosystems

As we have already pointed out, the password management is the weakest point of a traditional cryptosystem. Many of the drawbacks risen from the use of passwords can be overcome by using biometrics. Therefore in the recent past (see [67] for a review) some efforts have been devoted to design *biometric cryptosystems* where a classical password based authentication approach is replaced by biometric based authentication, which can be used for either securing the keys obtained when using traditional cryptographic schemes, or for providing the whole authentication system. A possible classification of the operating modes of a biometric cryptosystem is given in [67] where *key release*, *key binding*, and *key generation* modes are identified. Specifically, in the *key release* mode the cryptographic key is stored together with the biometric template and the other necessary information about the user. After a successful biometric matching, the key is released. However, this approach has several drawbacks, since it requires access to the stored template and then the 1 bit output of the biometric matcher can be overridden by means of Trojan horse attacks. In the *key binding* mode, the key is bound to the biometric template in such a way that both of them are inaccessible to an attacker and the key is released when a valid biometric is presented.

It is worth pointing out that no match between the templates needs to be performed. In the *key generation* mode, the key is obtained from the biometric data and no other user intervention, besides the donation of the required biometrics, is needed.

Both the *key binding* and the *key generation* modes are more secure than the *key release* mode. However, they are more difficult to implement because of the variability of the biometric data.

Among the methods which can be classified as *key binding* based approaches (see [67, 68]) we can cite the *fuzzy commitment* scheme [69], based on the use of error correction codes and on cryptographic hashed versions of the templates, and the *fuzzy vault* scheme [70], based on polynomial based secret sharing. More in detail, the approach proposed in [69] stems from the one described in [71], where the role of error correction codes used within the framework of secure biometric authentication is investigated and provides better resilience to noisy biometrics. The approach proposed in [69] has been applied to several biometrics: acoustic ear in [72], fingerprint in [73], 2D face in [74], and 3D face in [75]. These approaches have been generalized in [76, 77], where the author defines a user adaptive error correction codes selection are used, and applies it to signature template protection. The *fuzzy vault* method [70] has also been widely used with applications to several biometrics. In [78, 79], it has been applied to fingerprints protection. A modification of the original scheme was introduced in [80] and further improved in [68]. Moreover, in [81, 82] the *fuzzy vault* scheme is described with application to signature template protection, to face protection in [83, 84], and to iris protection in [85].

Fuzzy vault security has been investigated in the recent past. In [86] the a priori chaff identification problem has been addressed. Specifically, the authors have empirically established that chaff points generated later in the process have more neighborhoods than the other ones. In [87] the record multiplicity attack, the surreptitious attack, and blended substitution attack against biometric fuzzy vault are discussed.

Key generation based cryptosystems' major design problem is related to the variability of the biometric traits. Therefore, many efforts have been devoted to obtain robust keys from noisy biometric data. In [88, 89], cryptographic keys are generated from voice and face respectively. Significant activity has been devoted to the generation of keys from signature.

As proposed in [90] and further detailed in [91], a set of parametric features is extracted from each dynamic signature and an interval matrix is used to store the upper and lower admitted thresholds for correct authentication. A similar approach was proposed in [92]. Both methods provide protection for the signature templates. However, the variability of each feature has to be made explicitly available, and the methods do not provide template renewability. In [93], biometric secrecy preservation and renewability are obtained by applying random tokens, together with multiple-bit discretization and permutation, to the function features extracted from the signatures. In [94], biometric keys are generated using a genetic selection algorithm and applied to on–line dynamic signature. In [95], two different primitives for generating cryptographic keys from biometrics are given: the *fuzzy extractor* and the *secure sketch*. This latter has been widely studied in [96], where the practical issues related to the design of a secure sketch system are analyzed with specific application to face biometrics.

2.4.3.2 Feature Transformation

In order to obtain cancelability and renewability, techniques which intentionally apply either *invertible* or *non invertible* distortions to the original biometrics have been recently proposed. The distortion can take place either in the biometric domain, that is, before features extraction, or in the feature domain. In the case an invertible transform is chosen, the security of the system relies on the key which rules the transform, whose disclosure can reveal total or partial information about the template. When non invertible transforms are used, the security of these schemes relies on the difficulty to invert the applied transformation to obtain the original data. However, a rigorous security analysis on the non invertibility of the employed functions is very hard to conduct.

An invertible transform has been applied in [97] to face images by means of convolution with a user defined convolution kernel. In [98], palmprint templates are hashed by using pseudo-random keys to obtain a unique code called palmhash. In [99], user's fingerprints are projected in the Fourier–Mellin domain thus obtaining the fingerprint features, then randomized using iterated inner products between biometric vectors and token–driven pseudo number sequences. In [100], an approach similar to the one in [99] is applied to iris features. In [101], face templates are first projected in a lower dimensionally space by using Fisher Discrimination Analysis and then projected on a subspace by using a user defined random projection matrix. This approach has been generalized in [102] for text independent speaker recognition. In [103], face templates undergo a random orthonormal transformation, performed on the base of a user defined key, thus obtaining cancelability.

In a features transformation approach, a transformation function (typically dependent on some random parameters, which can be also employed as keys for the transformation) is applied to the biometric templates, thus obtaining the desired cancelable biometrics. It is possible to distinguish between *salting* approaches, where the employed transformation functions are invertible, and where therefore the security of the templates relies in the secure storage of the function parameters, and *non-invertible transform* approaches, where a one-way function is applied to the templates, and it is computationally hard to invert the transformation even if its defining parameters are known. The use of the methods belonging to the first category typically results in low false acceptance rates, however if a user-specific key is compromised, the user template is no longer secure due to the invertibility of the transformation. Examples can be found in [101] and [97].

On the contrary, when non invertible transforms are used, even if the key is known by an adversary no significant information can be acquired on the template, thus obtaining better security than salting approach, which relies on the key security. Moreover, in contrast with cryptosystem approaches, the transformed templates can remain in the same (feature) space of the original ones, being then possible to employ the original matcher also to perform authentication in the transformed domain. This allows to guarantee performances that are similar to those of a non-protected approach. Moreover, having the possibility to resort to sophisticated matchers, a score can be obtained as the output of a recognition process, even if it has been performed in a transformed and secure domain: multi-biometrics and secure system can therefore be implemented through score-level fusion techniques [104]. Unfortunately, it seems to be difficult to design transformation functions which can satisfy both the discriminability and the non-invertibility properties simultaneously.

The concept of achieving template security through the application of non-invertible transformations was first presented in [66], where it was referred to as *cancelable biometrics* as in [105], although this expression has been later conceived in a more general sense, as we already saw. The first practical non-invertible transform approach was presented in [106], where the minutiae pattern extracted from a fingerprint undergo a key-dependent geometric transform, which basically reflects the minutiae related to a randomly selected line in the fingerprint image. However, this protection scheme introduces a significant performance degradation, and the matching score between fingerprints transformed with different keys was relatively high, thus greatly reducing the useful key space. Generalizing this approach, three different non-invertible transforms for generating cancelable fingerprint templates, namely a cartesian, a polar and a functional transform, were proposed in [107]. Applying the transformations to the minutiae pattern, each fingerprint region undergoes a random displacement, thus obtaining that two relatively large region of the input image overlap in the output. Considering a minutia relying in such a zone, it is impossible to tell to which of the two original disjoint input regions it then belongs. The recognition performances of the various protected systems were found to be are very close to those of the unprotected scheme. However, this approach provided a very limited amount of non-invertibility: using the best performing "surface folding" transform, only about 8% of the original data changes its local topology, hence it can be concluded that only a small fraction of the data is in practice non-invertible [108]. Moreover, all the approaches for template protection in [106] and [107] are vulnerable to a record multiplicity attack: having access to two or more different transformed versions of the same minutiae pattern, one can identify the original position of the considered minutiae.

In [109], non-invertible transforms are applied to face images to obtain changeable templates, which however allow human inspection. A geometric approach for fingerprint template protection has also been presented in [110], where the fingerprint minutiae are mapped on a circle centered on their centroid, and the obtained projections are organized into bins according to their position to create a fingerprint code. Some limitations of this approach are that it is not possible to use sophisticated matchers due to the employed quantization step, and the capacity of generating multiple templates from the same fingerprint is not clear.

In [111] a signature template protection scheme, where non-invertible transformations are applied to the functions representing users' signatures, has been presented by the author, and its non-invertibility discussed. The renewability property of the approach proposed in [111] is also discussed in [112], where two novel transforms, defined in order to increase the number of cancelable templates, generated from an original signature template, are also introduced.

It is worth pointing out that, when using templates distortions techniques, with either invertible or non-invertible transforms, only the distorted data are stored in the database. This implies that even if the database is compromised, the biometric data cannot be retrieved unless, when dealing with invertible transforms, user dependent keys are revealed. Moreover, different templates can be generated from the original data, simply by changing the parameters of the employed transforms.

2.5 Current Projects and Standardization Activities

Biometric standardization [113] is still underway, and the most relevant activities are carried out by the International Organization for Standardization (ISO) SubCommittee 37 (SC37) Biometrics (ISO JTC 1 SC 37). Specifically, the working group 6 (WG6) is involved with cross jurisdictional and social aspects. Among the proposed documents, the report ISO/IEC 24714-1 [114] deals with the problems related to the design of biometric based systems, with specific reference to legal requirements, privacy protection, health, safety, and legal issues associated with the capture of biometric data. In the report ISO/IEC 24714-2 [115], the health and safety, usability, acceptance, and societal, cultural and ethical issues will be discussed for a list of biometric modalities. Moreover, the SubCommittee 27 (SC 27) is carrying out the development of the standard ISO IEC 19792 [116] where, among other issues, requirements on testing of vulnerability and on privacy will be given. Within SC 27, the standard ISO IEC 24745 [117] addresses the problem of template protection with respect to confidentiality, privacy, and integrity. Moreover, techniques to bind biometric data with other user's data will be also discussed. It is worth pointing out that the two aforementioned reports are still under development and they have not been released yet.

Among the projects of the European Union which investigate the bioethical implications of biometric identification technologies, we can cite the BITE (Biometric Identification Technology Ethics) project, which ended in February 2007 [118]. The HIDE (Homeland Security, Biometric Identification & Personal Detection Ethics) project [119] will end in 2011, and is focused on the ethical and privacy issues with specific reference to those applications which require cooperation among National and International agencies is crucial. Moreover the project PRIME (Privacy and Identity Management in Europe) within the EU sixth Programme Framework, which ended in February 2008 [120], focused on solutions for privacy-enhancing identity management that supports end-users' sovereignty over their private sphere and enterprisers' privacy-compliant data processing.

2.6 Privacy Issues and Biometric Protection: Summary

In recent years we have witnessed the rapid spreading of biometric technologies for automatic people recognition, due to several advantages they offer over traditional methods employing passwords or tokens.

Unfortunately, the use of biometric data in an automatic authentication system involves various risks not affecting other methods: if biometric data are somehow stolen or copied, they can be hardly replaced. Moreover, biometric data can contain relevant information regarding personality and health, which can be used in an unauthorized manner for malicious or undesired intents. Moreover, when cross-matching among different biometric databases is performed, an unauthorized user tracking of the enrolled subjects can be done, since personal biometric traits are permanently associated with the users. This would lead to users' privacy loss. Therefore, when designing a biometric-based recognition system, the issues deriving from security and privacy concerns have to be carefully considered, trying to provide countermeasures to the possible attacks which can be perpetrated at the vulnerable points of the system. Specifically, the privacy assessment of a biometric authentication system has to be done at the earliest stages of its design, in order to embed into the system the answers to the privacy concerns which have been identified, and to limit the potential costs deriving from negligent information management.

The adopted measures should be able to enhance biometric data resilience against attacks, while allowing the matching to be performed efficiently, thus guaranteeing acceptable recognition performance. Moreover, they should allow the generation of multiple templates from the same original biometric characteristic. Among the proposed approach, the use of classical cryptography is currently the most employed solution. However, the use of cryptographic techniques in a biometric based authentication system, where templates are stored after encryption, does not fully solve the template security issues: the match of biometric templates has always to be performed after decryption, which implies that no security is provided against attacks on the matcher module.

Data hiding techniques has also been proposed to insert additional information, namely the watermark, into a digital object, which can be used for a wide variety of applications, ranging from copy protection to fingerprinting, broadcast monitoring, data authentication, multimedia indexing, content based retrieval applications, medical imaging applications, and many others.

However, what it seems to be the most promising solution to provide protection to the biometric templates probably consists in the implementation of cancelable biometrics, which can be roughly described as the application of an intentional and repeatable modification to the original biometric template.

Several projects and standardization activities regarding privacy protective guidelines and solutions are currently carried out, demonstrating that the protection of the employed biometric data, in order to guarantee the desired privacy and security for the users of biometric systems, represents a still open and challenging issue.

Chapter 3

Signature Recognition

Signature recognition is one of the most accepted biometric based authentication methods since, being signatures part of everyday life, it is perceived as a non-invasive and non-threatening process by the majority of the users [121]. Moreover, signature has a high legal value, since it has always played the role of document authentication, and it is accepted both by governmental institutions as well as for commercial transactions as a mean of identification [122]. It is also worth pointing out that, on the contrary with respect to the majority of other biometrics, signature can be reissued, in the sense that, if compromised, the user can change its own signature with a certain degree of effort. On the other end, as it can be expected from a behavioral biometrics, different signature realizations, taken from the same user, can exhibit a lot of variability, mainly due to lack of user's habit and to the different conditions of execution (seated or standing position, wide or narrow area for resting the arms, and so on) [21]. Moreover, it can be influenced by physical and emotional conditions.

Signature biometrics has also another important characteristic which distinguishes itself from the other employed biometrics, and which has to be taken into account when evaluating the performances of a signature based authentication system: it can be forged in a relatively easy way, and without the need of specialized hardware [123]. In fact, in order to produce forged samples of physical biometrics such as fingerprint, face or iris, sophisticated and costly hardware is required, in addition to the original biometrics which has to be forged [124],[125]. For this reason, when testing the recognition performances of systems employing physical biometrics, the False Acceptance Rate (FAR) is always evaluated by claiming an identity with biometrics taken from other users. The same is done when dealing with behavioral biometrics such as keystroke and gait, and even when considering speech: also in these case, the difficulty in imitating a given keystroke dynamics, or the way a specific person walks, allows to evaluate the systems' FAR by only considering, for each user, biometrics taken from other subjects.

The possibility of mistaking the biometrics of a given user as being taken from another subject can be also considered for signature based authentication system: in this case, the FAR is evaluated employing *random forgeries* which, for each user, can be taken as signatures captured from different subjects. The FAR computed for random forgeries can be indicated as FAR_{RF}. However, when considering signature based authentication systems, much more significant performances can be evaluated when taking into account *skilled forgeries*, which consist of forged samples specifically produced to imitate the signatures of a given user. In order to produce fake signatures, a forger typically possesses a set of samples taken from a given user, and uses them to train himself in imitating the considered signatures. Then, he produces the forged samples which are employed to evaluate the FAR for skilled forgeries, indicated as FAR_{SF}. For a given system similarity score threshold, the achievable FAR_{SF} is typically higher than the FAR_{RF}. This peculiarity of signature based authentication systems imposes to consider also skilled forgeries when collecting samples for a biometric database.

A review on the state of the art, far from being exhaustive due to the large amount of works published on this argument, is given in Section 3.1. In Section 3.2 we then discuss the approaches already proposed in literature to provide protection to signature templates. Eventually, the publicly available signature databases are presented in Section 3.3. A detailed description of the public MCYT signature database, which is employed throughout this Thesis to test the proposed signature recognition algorithms, is also given.

3.1 Signature based authentication systems: state of the art

Because of the wide social and economical impact of signature based authentication, a huge effort has been devoted to research in this fields in the last decades. Basically, signature based authentication can be either *static* or *dynamic*. In the static mode, also referred to as *off-line*, only the written image of the signature, typically acquired through a camera or an optical scanner, is employed. In this case, some geometric signature image characteristics can be extracted. In the dynamic mode, also called *on-line*, signatures are acquired by means of a graphic tablet or a pen-sensitive computer display, or even by means of a PDA, which can provide temporal information about the signature. These devices capture the spatio-temporal evolution of the signature thus acquiring the pressure, the velocity, the acceleration, the pen tilt signals among the others. Once the signature has been acquired, either off-line or on-line, some preprocessing is usually needed in order to normalize the signature dimensions, to localize the signature, to denoise the signature image in case of off-line data acquisition, to segment the signature and so on [126]. Since on-line signature authentication involves the acquisition of the signature dynamic behavior, which is much more difficult to forge than the static one, represented by the signature image, it is in general more suitable for personal authentication, especially in legal and commercial transactions requiring high-security.

A review of the state of the art covering the literature up to 1994 can be found in [127] and in [128]. Survey papers quoting the advances in signature recognition up to 2004 are given in [129], where also handwriting recognition is addressed, in [126], and in [122]. The most recent literature reviews can be found in [130, 131].

Signature recognition is usually performed by extracting sets of features from the acquired signatures. When dealing with on-line signatures, it is widely accepted in the current literature that two different kind of features can be considered: *parameters* and *functions* [132]. The former refers to scalar values, while the latter refers to on-line acquisitions where time functions like pressure, velocity, or acceleration can be employed.

The approaches employing parametric features, usually indicated as *global approaches*, extract static information such as the height and the width of the signatures, or dynamic information like the number of strokes, the mean signature velocity, and so on. The obtained characteristics are then employed to train a classifier [91, 133, 134]. In most comparative studies, the parameters based on dynamic information are typically more discriminative for recognition purposes than those based on static information [91]. A plethora of *parameters* have been proposed in the literature (see [126, 130] for a survey). Some of them can be obtained by applying operators like the average, the minimum, the maximum operators to time-functions, like velocity, acceleration, pressure, forces. Some other typical parameters can be obtained from on-line signature acquisitions like the number of pen-lifts, or from off-line acquired signatures, for example derived from the structural analysis of the signature like height, width, ratio between the signature length and its width, and many others. Moreover, the employed parameters can be obtained after a preliminary projection of the acquired data in a transform domain like the Fourier, Wavelet, Hadamard, Hough domain, to cite a few.

On the other hand, function based methods typically employ a signature representation consisting of various temporal sequences. Two different kinds of function based recognition approaches can be distinguished:

- *local* approaches, where time sequences extracted from different signatures are directly matched, by using elastic distance measures such as Dynamic Time Warping (DTW) [21], which represents one of the more flexible approaches to manage the signature length variability [135, 136, 137]. During the comparative studies performed for the Signature Verification Competition of 2004 (SVC 2004) [138], the on-line signature recognition algorithm proposed in [139], employing DTW matching, gave the lowest average Equal Error Rate (EER) values, when tested with skilled forgeries. In [140] a modified DTW algorithm, which is based on the stability of the components of the signature and outperforms the standard DTW, is presented;

- *regional* approaches, where the acquired signatures are analyzed by estimating some regional properties, which are then employed to train a given classifier, as it is done when modeling signatures with Hidden Markov Models (HMM) [121, 134, 141]. In [142] signatures are decomposed employing wavelet transforms, and then Discrete Cosine Transform (DCT) is applied to the resulting approximation coefficients, in order to obtain a signature representation. A Linear Programming Descriptor (LPD) classifier is then trained using the DCT coefficients. Also neural networks have been widely used for matching signature templates[143, 144].

According to the recently published results, the most promising approaches belong to the category of function based methods. However, one of the major research trend in on-line signature verification is to combine different systems, in order to build multiple classifiers based in global, local and regional approaches [145, 146].

Moreover, as outlined in [147], it is worth pointing out that not all the features have the same *consistency*, when considering both parametric and functional features. From an ideal point of view, a reliable feature should have values close enough for genuine signatures, whereas far enough when they are extracted from forged signatures. In [147], a consistency model is proposed, and the reliability of some commonly used features is analyzed.

3.2 Signature Template Protection: Related Works

As we already asserted, one of the advantage of using signature in a biometric recognition system is that a signature, when compromised, can be reissued by its owner. However, the definition of a new signature requires a certain degree of effort by the user. Moreover, if a user has to be recognized by means of a signature with which he is not used to, the produced signatures can exhibit an unacceptable variability, due to lack of user's habit with its new signature. Moreover, from a template which represents the signatures of a given user, a lot of personal information can be extracted, even regarding people personality. This possibility holds true specifically when the stored templates permit to perfectly reconstruct both the shape and the dynamics of the signatures, as it happens when employing local based recognition approaches such as DTW. The protection of the employed templates is therefore a design issue which has to be carefully considered when implementing a signature based authentication system.

Signature template protection has been first considered in [90] and [92] with a key generation approach, where a set of parametric features is extracted from the acquired dynamic signatures, and a hash function is applied to the feature binary representation, obtained exploiting some statistical properties of the enrollment signatures. Both methods provide protection for the signature templates, although the cancelability property is not considered. In [81] an adaptation of the fuzzy vault to signature protection has been proposed:

this method is based on a quantized set of maxima and minima of the temporal functions, mixed with chaff points in order to provide security. A salting approach has been proposed in [148] as an adaptation of the *BioHashing* method [101] to signature templates. Moreover, in [149] an improved version of the BioHashing approach, where the procedure is iterated many times to increase the security of the system, has also been proposed for the protection of signature templates.

Also the fuzzy commitment [69] (more specifically, its practical implementation known as Helper Data System [74]) has been employed to provide security for the features extracted from an on-line signature, as proposed in [77], [150], where a user-adaptive error correcting code selection was also introduced. The use of watermarking based techniques to provide a security scalable system was proposed by the author in [62, 63, 150, 151].

In [111] a signature template protection scheme, where non-invertible transforms are applied to a set of signature sequences, has been presented by the author, and its non-invertibility discussed. The renewability capacity of the approach in [111] as also been analyzed in [112], where additional non-invertible transforms have been introduced.

The present Thesis describes in details three different systems where the employed signature templates are protected against possible attacks. Specifically, the presented methods do not define innovative matching strategies for the comparison of signatures; instead of doing this, the proposed approaches are defined in order to make privacy-protective the already proposed procedures for signature based authentication.

Two different *cancelable biometrics* based schemes are presented in Chapter 4 and Chapter 5.

Specifically, a *global features* based approach is considered in Chapter 4, where a user-adaptive biometric cryptosystem is implemented to protect the employed signature parametric characteristics.

On the other hand, *functional features* based recognition methods are taken into account in Chapter 5, where a feature transformation protection approach, based on non-invertible transforms, is defined. The applicability of the proposed approach to both DTW and HMM based classifiers is considered.

Eventually, a system where watermarking is employed as the mean to provide protection to parametric features based signature templates is presented in Chapter 6. Instead of defining a cancelable biometrics based system, data hiding techniques are employed to hide and keep secret some relevant signature characteristics.

The approaches presented in this Thesis therefore supply a comprehensive collection of solutions which can provide protection to the signature templates employed in the most of the currently deployed signature based recognition systems.

3.3 Signature Databases

In order to test the verification capabilities of a given biometric recognition algorithm, a large number of biometric samples have to be acquired and made available for tests. The growth that the field of biometric recognition has experimented over the past two decades has led to an increasing number of biometric databases, either mono-modal [152] (one biometric feature sensed) or multi-modal [153] (two or more biometric features sensed), which have been collected and employed by the research community.

However, due to the use of data acquired with different instruments, and according to different conditions, it is usually difficult to compare recognition systems based on the same biometric trait. Even the testing and reporting modalities employed to verify the effectiveness of two methods can differ, resulting in the impossibility of establishing a common benchmark between different approaches. For all these reason, it is in generally recommendable to employ publicly available databases to test a given algorithm, in order to be able to properly compare the achieved recognition performances with those of other already proposed approaches.

Obviously, the most interesting available biometric databases are the multi-modal ones, because they contain a large amount of biometric data collected by the same individuals, and therefore allow to perform many evaluation tests for different biometric recognition approaches. Some significant examples of multimodal biometric databases, either completed and already available, or in process of completion are:

- BIOMET database [154]. This multi-modal database includes five different biometric modalities: audio, face images (2D and 3D), hand images, fingerprint (captured with both an optical and a capacitive sensor), and on-line signature. The BIOMET database has been acquired in three temporally separated sessions (8 months between the first and the last one) and comprises 91 subjects, from each of which the five aforementioned biometrics have been collected;

- MyIDEA database [155]. This database contains six different biometric modalities: face, audio, fingerprints, signature, handwriting and hand geometry. Two additional synchronized recordings were also performed: face-voice and writing-voice. The general specifications of the database are: target of 104 subjects, different quality sensors, various realistic acquisition scenarios with different levels of control, organization of the recordings to allow an open-set of experimental scenarios, and compatibility with other existing databases such as BANCA [156].

- BIOSEC database [153]. This database has been collected under the EU FP6 BioSec Integrated Project [157], and comprises four biometric modalities: fingerprint images acquired with three different sensors, frontal face images from a webcam, iris images from an iris sensor, and voice utterances (captured both with a webcam and a close-talk headset). The baseline corpus described in [153] comprises 200 subjects with 2 acquisition sessions per subject. The extended version of the BioSec database comprises 250 subjects with 4 sessions per subject (about 1 month between sessions).

- BiosecurID database [158]. This database has been collected in 6 different sites, using an office-like uncontrolled environment (in order to simulate a realistic scenario). It comprises biometric data acquired by 400 users, during 4 sessions distributed in a 4 month time span. The eight collected biometric modalities are: speech, iris, face (photographs and talking faces videos), signature and handwriting (on-line and offline), fingerprints, hand (palmprint and contour-geometry), and keystrokes. By now, it is the database comprising the higher number of different biometric modalities;

- BIOSECURE database [159]. One of the objectives of the EU FP6 Biosecure Network of Excellence has been the acquisition of a multi-modal database, with the aim of extending the efforts conducted in MyIDEA, BioSec, and BiosecurID. The BIOSECURE database considers three acquisition scenarios, namely:

  - *Internet Dataset*: voice and face (still images and talking faces) data have been captured in an unsupervised setup through the Internet;
  - *Desktop Dataset*: the acquisition setup represents an office-like scenario, and the acquisition of the following biometrics is conducted with human supervision: voice, fingerprints (two sensors), face (still images and talking faces), iris, signature (genuine and skilled forgeries) and hand;
  - *Desktop Dataset*: the acquisition of the following data is conducted using two mobile devices (a PDA and a Ultra-Mobile PC): signature (genuine and skilled forgeries), fingerprints (sweep sensor), voice, and face (images and video).

  All datasets include 2 sessions, with the biggest dataset (internet) comprising over 1000 subjects, and about 700 users the other two. Around 400 of these donors are common to the whole database. This database is therefore the one comprising the larger number of enrolled users;

- MCYT database [160]. This database include two biometric modalities: fingerprints and signatures. The data have been collected from 330 subjects in four acquisition sites;
- MBioID database database [161]. This database has been collected in order to study the use of biometric data in Identity Documents. The acquired biometric modalities are: 2D and 3D face, fingerprint, iris, signature and speech.

We can notice that all the aforementioned multi-modal databases, with the only exception of the BIOSEC database, include acquisition of on-line signatures. This fact can testify the high relevance of signature verification for the current biometric based recognition systems. In addition to the already listed database, on-line signatures have also been collected for the Smartkom multi-modal database [162], which includes fingerprint, hand, signature and speech acquisitions from 96 subjects. On-line signature have also been collected from 100 different subjects for the mono-modal database employed during the Signature Verification Competition (SVC) held at ICBA 2004 [138]. Moreover, a larger database will be made available for the BioSecure Signature Evaluation Campaign (BSEC) which will be held in 2009. This database will be used for the 2009 Online Signature Verification Competition, which will be carried out in the framework of the *International Conference on Biometrics 2009* Competitions, and comprises signatures taken from two subsets of the complete BioSecure Network of Excellence [159]: the considered signatures are acquired in a mobile scenario (on a PDA), as well as on a digitizing tablet.

It is worth reporting other two important signature databases: the Philips signature database [163], comprising on-line signatures acquired from 51 subjects, and the Caltech signature database [164], with on-line signatures acquired from 56 subjects by means of a camera with a Imagination PXC200 frame grabber.

In this Thesis, the public MCYT database with signatures taken from 100 users [165] is employed to test the effectiveness of each of the proposed approaches. The employed database is a publicy available subset of the complete MCYT corpus [160], which comprises signatures taken from 330 users. This database is, by now, probably the most employed by the research community in order to test algorithms regarding signature verification.

The on-line signatures collected in the considered database have been acquired by employing a WACOM pen tablet, model INTUOS A6 USB. The pen tablet resolution is 2.540 lines per inch (100 lines/mm), and the precision is ± 0.25 mm. The maximum detection height is 10 mm (so pen-up movements are also considered), and the capture area is 127 mm (width) $\times$ 97 mm (height). The tablet provides the following discrete-time dynamic sequences:

- position $\mathbf{x}[n]$ in x-axis,
- position $\mathbf{y}[n]$ in y-axis,
- pressure $\mathbf{p}[n]$ applied by the pen,
- azimuth angle $\boldsymbol{\gamma}[n]$ of the pen with respect to the tablet,
- altitude angle $\boldsymbol{\phi}[n]$ of the pen with respect to the tablet.

The sampling frequency is set to 100 Hz. Taking into account the Nyquist sampling criterion and the fact that the maximum frequencies of the related biomechanical sequences are always under 20-30 Hz [166], this sampling frequency leads to a precise discrete-time signature representation.

The employed signature database comprises both genuine and shape-based skilled forgeries with natural dynamics, for each of the considered 100 subjects. The forgeries were generated by contributors to the database imitating other contributors. For this task they were given the printed signature to imitate and were asked not only to imitate the shape but also to generate the imitation without artifacts such as time breaks or slowdowns. Specifically, signature data for each user include 25 samples of his/her own signature, and 25 skilled forgeries. Taking into account that the signer was concentrated in a different writing task between genuine signature sets, the variability between client signatures from different acquisition sets is higher than the variability of signatures within the same acquisition set.

It is worth pointing out that the results which will be presented in this Thesis have been carried out by dividing the considered database in two disjoint data sets: a *training set*, which comprises the genuine and forged signatures of the first 30 users, and a *test set*, which includes the genuine and forged signatures of the remaining 70 users. This has been done because each of the proposed signature recognition system, as it happens for practical authentication schemes, requires a training phase, during which some system's parameters are defined. The parameters estimated during the training phase will then be employed during the actual tests of the considered recognition system. In this Thesis, where not specified differently, the reported recognition performances are therefore evaluated employing the signatures taken from 70 users of the public MCYT database.

3.4 Summary

In this Chapter, some introductory concepts regarding on-line signature verification have been discussed. Among the various biometrics which can be employed in an automatic people verification system, signature has the advantages of being a non-invasive measurement. Moreover, signature based verification is widely accepted since it has been established as one of the most diffuse mean for personal verification in our daily life, including commerce applications, banking transactions, automatic fund transfers, and so on.

Signature verification has attracted many researchers during the past years, which are interested both to the scientific challenges and to the valuable applications of this field. In fact, there are few doubts on the importance of automatic signature verification in the set of biometric techniques for personal verification.

Signature verification can be performed either in a static way, by using only signature images, or in a dynamic way, by taking into account the time behavior of the signing act. On-line signature recognition usually allows to reach performances far better than those obtained when considering off-line signatures. The already proposed approaches are commonly distinguished as belonging to three different categories: global parametric feature approaches, local based function features approaches, and regional based function features approaches. The methods relying on a local analysis of a set of functional features are considered as those able to guarantee the best recognition rates.

The approaches proposed for the protection of signature templates, as well as the available databases comprising on-line signature data have also been illustrated.

Chapter 4

User adaptive On-line Signature based Cryptosystem

In this Chapter, a key binding biometric cryptosystem based on on-line signature, able to provide the required security and renewability for the employed on-line signature templates, is proposed. Moreover, an user adaptive approach, where the system parameters are tuned to the variability of each user's signatures, is presented.

The proposed cryptosystem provides protection to templates consisting of parametric features, which represent the information extracted from the acquired on-line signatures of each user.

4.1 Proposed Biometric Cryptosystem

The proposed cryptosystem for biometric templates protection is based on Juels' proposal of fuzzy commitment [69], which employs error correcting codes, together with helper data to generate a protected representation of the considered biometrics. The employed approach is twofold, allowing the system both to manage cancelable biometrics [66], and to handle the intra-class variability exhibited by biometric signatures. In fact, the signature variability is here handled by considering the obtained templates as noisy versions of an "ideal" template, where the noise power is related to the actual signature deviation from the noise free template. The architectures of the proposed enrollment and authentication procedures

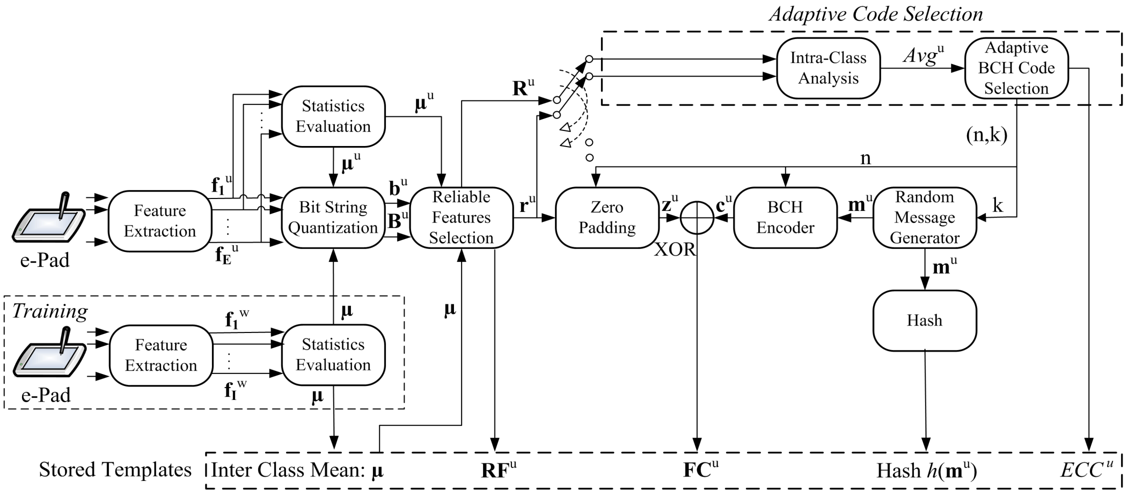


Figure 4.1: Signature-based fuzzy commitment: enrollment scheme. The acquired data are analyzed, quantized and summed to error correcting codes. The stored data are $\boldsymbol{\mu}$, $\mathbf{RF}^u$, $\mathbf{F}C^u$, ECC^u and $h(\mathbf{m}^u)$.

are illustrated in Figures 4.1 and 4.3 respectively.

In brief, during the enrollment a number E of biometrics measurements are recorded for each user u. The acquired signatures are then processed, in order to extract a set of parametric features, which supplies the employed on-line signatures representation. The mean values of the features extracted from the signatures of the user u is then estimated, and then binarized through a comparison with reference data. The data employed for the binarization process have to be computed during a training phase, which has to be performed before starting the enrollment process.

For each user, a binary string is generated by taking into account the user's most reliable features, and then bind with an error correcting codeword, through a XOR operation. The random message that originated the employed codeword is eventually stored in a hashed form, together with the binary string computed with the XOR operation. The employed error correcting code can be the same for all the enrolled users, or can be selected according to the user's characteristics, thus realizing an user adaptive code selection. The stored templates can be used to perform user authentication without revealing any information about the original data, as indicated in Section 4.1.3.

In the following, the details on the proposed cryptosystem are presented: the reliable features selection principles are outlined in Section 4.1.2.1, while both the proposed non-adaptive and the user adaptive methods are detailed respectively in Sections 4.1.2.2 and 4.1.2.3. The experimental results obtained by testing the proposed approaches are given in Section 4.3, which also includes comparisons with the performances of an unprotected system using parametric features. Moreover, our approaches are also compared with other approaches, already proposed for the protection of on-line signature parametric features.

4.1.1 Training stage

In the proposed signature based cryptosystem, a training phase is needed to evaluate the reference data which are employed for the feature binarization process. Specifically, it is assumed that signatures taken from W users, each of which has supplied I genuine signatures, are available for this phase. Having represented with $\mathbf{f}_i^w[k]$ the feature vector extracted from the i-th signature of the w-th user, the *inter-class* mean vector $\boldsymbol{\mu}[k]$ of the considered features is estimated as:

$$\boldsymbol{\mu}[k] = \frac{1}{WI} \sum_{i=1}^{I} \sum_{w=1}^{W} \mathbf{f}_i^w[k], \tag{4.1}$$

where k, with $k \in \mathcal{K} = \{1, \dots, K\}$, represents the feature index.

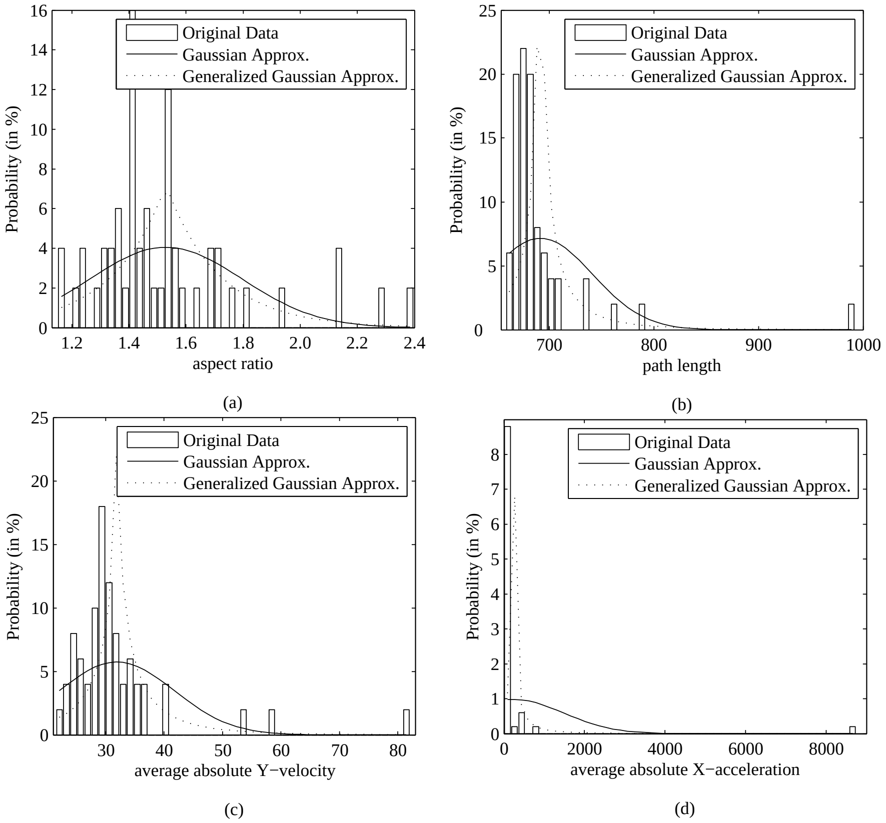
The inter-class mean vector $\boldsymbol{\mu}[k]$ is stored in the database, and employed during the enrollment and authentication phases to generate the signature binary templates.

4.1.2 Enrollment stage

The proposed enrollment scheme is sketched in Figure 4.1. For each enrolled user u, once E on-line signatures have been acquired, the feature vectors $\mathbf{f}_e^u[k]$, $e = 1, \dots, E$ and $k \in \mathcal{K}$, are evaluated. The *intra-class* mean feature vector $\boldsymbol{\mu}^u[k]$ can then be computed as:

$$\boldsymbol{\mu}^u[k] = \frac{1}{I} \sum_{e=1}^{E} \mathbf{f}_e^u[k], \tag{4.2}$$

A binary vector $\mathbf{b}^u[k]$, representative of the signatures taken from the considered user u, is then obtained by comparing the intra-class vector $\boldsymbol{\mu}^u[k]$ with the inter-class vector $\boldsymbol{\mu}[k]$,



(a)

(b)

(c)

(d)

Figure 4.2: Fitting of four common signature features distributions to Gaussian and Generalized Gaussian Model: a)aspect ratio; b)path length; c) absolute Y-velocity; d) average absolute X-acceleration.

estimated during a training phase as described in Section 4.1.1:

$$\mathbf{b}^u[k] = \begin{cases} 0 & \text{if } \boldsymbol{\mu}^u[k] \leq \boldsymbol{\mu}[k] \\ 1 & \text{if } \boldsymbol{\mu}^u[k] > \boldsymbol{\mu}[k] \end{cases}, \quad k \in \mathcal{K}. \tag{4.3}$$

4.1.2.1 Reliable Feature Selection

In the proposed scheme, a selection of the most relevant features for each enrolled user u has to be performed, in order to counteract the potential instability of the feature vector components. Specifically, the variability of each k-th feature reflects itself on the k-th component of the vector $\mathbf{b}^u[k]$, which is taken as representative of the signatures acquired from user u.

In [74], where features extracted from faces are considered, this task is accomplished

Feature	Distribution	GOF	Chi-squared	Cramer-von Mises	Anderson-Darling
Aspect Ratio	Gaussian	0.1031	0.0493	0.0463	0.1816
	Gen. Gaussian	0.0823	0.0515	0.0374	0.1543
Path Length	Gaussian	0.0683	0.1008	0.0408	0.1238
	Gen. Gaussian	0.0831	0.1084	0.0454	0.1419
Y Velocity	Gaussian	0.2824	0.2057	0.1907	0.4001
	Gen. Gaussian	0.3190	0.1514	0.1963	0.4878
X Acceleration	Gaussian	0.7829	0.2990	0.7624	2.5226
	Gen. Gaussian	0.7638	0.1039	0.7170	2.2371

Table 4.1: Test of fit of a Gaussian and Generalized Gaussian distribution to the data: Goodness-of-Fit, Chi-squared, Cramer-von Mises, and Anderson-Darling.

using a feature reliability measure, which is defined by assuming a Gaussian distribution for each considered face feature. However, the Gaussianity assumption does not properly apply to the scenario under examination, where on-line signatures are taken as the considered biometrics. In fact, extensive tests have pointed out that the majority of commonly used signature features, like mean velocity, acceleration or pressure, cannot be properly modeled according to either a Gaussian or a generalized Gaussian distribution. In Figure 4.2, the histogram of four common features (aspect ratio, path length, average absolute Y-velocity, average absolute X-acceleration) extracted from a set of signatures, is shown together with the Gaussian and the generalized Gaussian probability density functions, whose parameters are estimated from the experimental data. Testing of fit with Gaussian and generalized Gaussian distributions have also been performed. Specifically, the Goodness-of-Fit (GOF) , Chi-squared, Cramer-von Mises, and Anderson-Darling tests [167] have been used. The obtained results, collected in Table 4.1, highlight the poor match between the experimental data and the considered distributions. Therefore, in our approach we introduce a reliability measure not directly related to the signature features distribution.

In the process of defining a reliable feature user dependent selection procedure, the enrollment features vectors $\mathbf{f}_e^u[k]$ of each user u, with $e = 1, \ldots, E$, are binarized by comparing them with the inter-class mean $\boldsymbol{\mu}[k]$ and collected as row vectors in a binary matrix $\mathbf{B}^u[e, k]$, with E (signature samples) rows and K (features) columns, whose generic element $\mathbf{B}^u[e, k]$

is obtained as:

$$\mathbf{B}^u[e,k] = \begin{cases} 0 & \text{if } \mathbf{f}_e^u[k] \leq \boldsymbol{\mu}[k] \\ 1 & \text{if } \mathbf{f}_i^u[k] > \boldsymbol{\mu}[k] \end{cases}, \quad k \in \mathcal{K}. \tag{4.4}$$

Then, a reliability measure $\mathbf{Q}_1^u[k]$ of the k-th feature of user u is defined as follows:

$$\mathbf{Q}_1^u[k] = 1 - \frac{\sum_{e=1}^{E}(\mathbf{B}^u[e,k] \oplus \mathbf{b}^u[k])}{I}, \quad k \in \mathcal{K}, \tag{4.5}$$

where $\oplus$ represents the XOR operation, and $\mathbf{b}^u[k]$ is given by equation (4.3). In equation (4.5), the occurrence of the k-th binary value $\mathbf{b}^u[k]$ in the corresponding elements of the binary matrix $\mathbf{B}^u[e,k]$ is evaluated: in this way, a measure of the representativeness of the value $\mathbf{b}^u[k]$, with respect to the possible values obtainable from a new signature by the same user, is derived. According to this measure, components with a high reliability possess a high discrimination capability.

However, the use of the reliability measure $\mathbf{Q}_1^u[k]$ can lead to components with the same reliability value. Then, in order to further discriminate among them, a second level of feature screening is introduced, according to the following reliability measure:

$$\mathbf{Q}_2^u[k] = \frac{\mid \boldsymbol{\mu}[k] - \boldsymbol{\mu}^u[k] \mid}{\boldsymbol{\sigma}^u[k]}, \quad k \in \mathcal{K}, \tag{4.6}$$

being $\boldsymbol{\sigma}^u[k] = \sqrt{\frac{1}{E-1}\sum_{e=1}^{E}\left[\mathbf{f}_e^u[k] - \boldsymbol{\mu}^u[k]\right]^2}$ the standard deviation of the k-th feature of user u. A higher discriminating power is thus trusted to features with a larger difference between $\boldsymbol{\mu}^u[k]$ and $\boldsymbol{\mu}[k]$, relative to the standard deviation $\boldsymbol{\sigma}^u[k]$.

After the application of the proposed reliability metrics to $\mathbf{b}^u[k]$, the least reliable features can be discarded, thus ending up with the binary feature vector $\mathbf{r}^u[l]$, which contains the L most reliable components of $\mathbf{b}^u[k]$, being $l \in \mathcal{L} = \{1, \ldots, L\} \subseteq \mathcal{K}$. The indexes of the most reliable feature for the user u are collected in $\mathbf{RF}^u[l]$, which is stored in the database together with the inter-class vector $\boldsymbol{\mu}[k]$, being thus made available for the authentication process.

As already pointed out, in order to achieve both template protection and renewability, the generated binary biometric templates have to be bind with error correcting codewords. Specifically, the proposed implementation employed BCH codes [168], which are completely determined once the lengths of the messages to be encoded are known, together with the desired error correction capability (ECC).

ECC	n	h	ECC	n	h	ECC	n	h
1	127	120	11	127	57	21	127	29
2	127	113	12	255	163	22	255	107
3	127	106	13	127	50	23	127	11
4	127	99	14	127	43	24	1023	788
5	127	92	15	127	36	25	255	91
6	127	85	16	511	367	26	255	87
7	127	78	17	1023	858	27	127	15
8	255	191	18	255	131	28	511	277
9	127	71	19	255	123	29	255	71
10	127	64	20	511	340	30	255	63

Table 4.2: Correspondences between ECC, n and h values

The ECC of the BCH codes which are employed in the proposed scheme can be determined *a priori*, as it has been proposed in [74]: this approach is detailed in Section 4.1.2.2. However, it is also possible to define a strategy using which the ECC is selected depending on the intra-class variability of each user's signature, as detailed in Section 4.1.2.3.

4.1.2.2 A priori Selection of Error Correction Capability

After having obtained the binary feature vector $\mathbf{r}^u$, BCH codes are employed to realize the fuzzy commitment. The ECC of the employed BCH encoder, and therefore the length n of its codewords, is selected according to the desired False Acceptance Rate (FAR) or False Rejection Rate (FRR). In Table 4.2, a selection of the correspondences between the ECC and the values of n and h, respectively being the length of the codewords $\mathbf{c}$ and the length of the messages to be encoded $\mathbf{m}$, is reported.

Once the BCH encoder is chosen, a codeword $\mathbf{c}^u$ is generated from a randomly selected message $\mathbf{m}^u$. Then, the binary vector $\mathbf{r}^u$, which consists of L bits as detailed in Section 4.1.2.1, is zero padded in order to reach the same length n of the codeword $\mathbf{c}^u$, thus resulting in the vector $\mathbf{z}^u$. The pattern of zeros that is applied to $\mathbf{r}^u$, in order to generate $\mathbf{z}^u$, can be randomly selected, and also a scrambling of the feature positions in $\mathbf{r}^u$ can be performed before adding the requested number of zeros. A XOR operation between the codeword $\mathbf{c}^u$

and $\mathbf{z}^u$ is finally performed, thus obtaining the fuzzy commitment $\mathbf{FC}^u$:

$$\mathbf{FC}^u = FC(\mathbf{z}^u, \mathbf{c}^u) = \mathbf{z}^u \oplus \mathbf{c}^u. \tag{4.7}$$

A hashed version $h(\mathbf{m}^u)$ of the random message $\mathbf{m}^u$, obtained using the SHA-512 algorithm, is then stored together with $\mathbf{FC}^u$. The SHA-512 algorithm has been chosen due to its stronger resilience against attacks, with respect to the SHA-1 [169] hashing algorithm. In fact, different attacks that are able to find collisions on SHA-1, with less computational complexity than a brute force search, have already been proposed, and are therefore considered as breaks of SHA-1 [170, 171, 172]. The SHA-256 with 32-bit words, or the SHA-512 with 64-bit words, should be therefore employed in order to improve the system security for practical application of the proposed scheme. Currently, these hash functions have not yet received as much attention as SHA-1 has, and so their cryptographic security is not yet as well-established; however, it seems that no weakness have been found until now.

It is worth pointing out that, as evident from Table 4.2, no restriction is introduced for the number L of the reliable features that can be considered, given that $L < n_{min} = 127$. However, also this constraint can be removed by selecting BCH codes with a longer minimum codeword length n_{min}. Additional values of ECC can be considered, although not reported in Table 4.2, simply considering other BCH encoders.

4.1.2.3 Adaptive Selection of Error Correction Capability

The approach described in Section 4.1.2.2 allows to obtain renewable templates by changing the employed codeword $\mathbf{c}^u$, that is, the random generated message $\mathbf{m}^u$, associated to the user during enrollment. However, the variability the acquired signatures is treated in the same way for each enrolled user. An authentication method that, besides providing renewability, provides adaptability to the user signature variability, is also here proposed.

Applying the proposed user-adaptive code selection, codes with higher error correction capabilities are employed for users characterized by a high intra-class variability. Therefore, in the enrollment stage, an intra-class analysis is performed as follows: once the L reliable features are selected, as detailed in Section 4.1.2.1, the matrix $\mathbf{R}^u[e, l]$, having E rows and L columns, is obtained from $\mathbf{B}^u[e, k]$, by dropping the columns corresponding to unreliable features. Then, the Hamming distances $D^u[e]$, with $e = 1, \ldots, E$, between any rows of $\mathbf{R}^u[e, l]$ and the user representative vector $\mathbf{r}^u[l]$, are evaluated. The average A^u of the $D^u[e]$ values,

$$A^u = \frac{1}{E} \sum_{e=1}^{E} D^u[e], \tag{4.8}$$

is then used to characterize the intra-class variability of the user u.

Specifically, the BCH code whose ECC is equal to the nearest integer of $(A^u + \Delta_{ECC})$, where Δ_{ECC} is a system parameter common to all the enrolled users, is chosen. The selected error correction capability ECC^u, is then stored in the database for user u.

Once the ECC for the user u has been determined, the binary vector $\mathbf{r}^u$ is zero padded in order to reach the same length n of the selected BCH codewords, resulting in the vector $\mathbf{z}^u$ as described in Section 4.1.2.2. The fuzzy commitment $\mathbf{FC}^u$ is then generated using a codeword $\mathbf{c}^u$ obtained from the encoding of a random message $\mathbf{m}^u$:

$$\mathbf{FC}^u = FC(\mathbf{z}^u, \mathbf{c}^u) = \mathbf{z}^u \oplus \mathbf{c}^u. \tag{4.9}$$

A hashed version $h(\mathbf{m}^u)$ of $\mathbf{m}^u$, created using the SHA-256 algorithm, is eventually stored.

The proposed framework provides security, being impossible to retrieve the feature vectors $\mathbf{f}_e^u[k]$, $e = 1, \ldots, E$, from the stored templates $\boldsymbol{\mu}$, $\mathbf{RF}^u$, $\mathbf{FC}^u$, $h(\mathbf{m}^u)$, and ECC^u. In fact, in order to infer about the extracted features, or to reconstruct their binary counterparts, it is necessary to possess, among the other data, the BCH codeword $\mathbf{c}^u$ employed for data protection (see Figure 4.1). However, neither the binary word $\mathbf{m}^u$ at the input of the BCH encoder nor its output $\mathbf{c}^u$ are stored. In fact, only the hashed value of $\mathbf{m}^u$, generated by means of the hash function $h(\cdot)$, is stored, thus guaranteeing the impossibility to recover useful information from the system database. Then, as shown in [69], it can be concluded that the disclosure of the secret $\mathbf{z}^u$ is as much hard as finding a collision for the SHA-256 hash $h(\mathbf{m}^u)$, which leads to the observation that the security of the presented system is the same of the employed hash function.

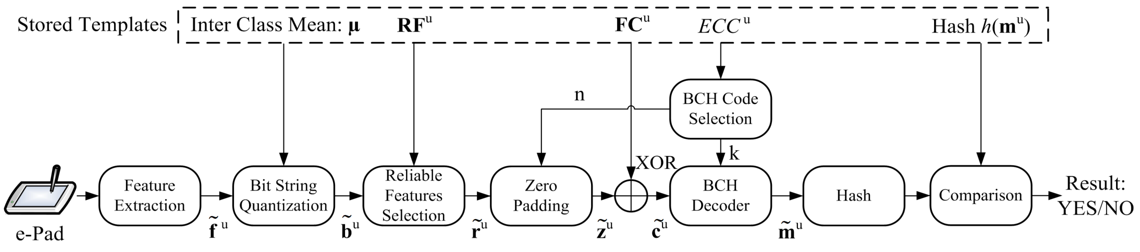


Figure 4.3: Signature-based fuzzy commitment: authentication scheme. When a subject claims his identity, a response is given using the stored data $\boldsymbol{\mu}$, $\mathbf{RF}^u$, $\mathbf{FC}^u$, ECC^u and $h(\mathbf{m}^u)$.

4.1.3 Authentication stage

The authentication phase follows the same steps as the enrollment stage (see Figure 4.3). When a subject claims his identity, he provides his signature, which is converted in the features vector $\tilde{\mathbf{f}}^u[k]$, $k \in \mathcal{K}$. Then the quantization is done using the inter-class mean $\boldsymbol{\mu}[k]$, thus obtaining $\tilde{\mathbf{b}}^u[k]$. The reliable features $\tilde{\mathbf{r}}^u[l]$, $l \in \mathcal{L} = \{1, \ldots, L\} \subseteq \mathcal{K}$, are selected using $\mathbf{RF}^u[l]$, and later extended using zero padding (employing the same zero pattern defined during enrollment), generating the binary word $\tilde{\mathbf{z}}^u$. A binary string $\tilde{\mathbf{c}}^u$, representing a possibly corrupted BCH codeword, results from the XOR operation

$$\tilde{\mathbf{c}}^u = \tilde{\mathbf{z}}^u \oplus \mathbf{FC}^u. \tag{4.10}$$

The BCH decoder is selected depending on the encoder used in enrollment, obtaining $\tilde{\mathbf{m}}^s$ from $\tilde{\mathbf{c}}^s$. Finally, the SHA-1 hashed version $h(\tilde{\mathbf{m}}^s)$ is compared to $h(\mathbf{m}^s)$: if both values are identical the subject is authenticated, otherwise he is rejected.

4.2 Signature representation: employed features

The proposed biometric cryptosystem can be employed for the protection of any biometrics which can be represented through a set of parametric features. The features employed in the system, as well as their number K, can be chosen accordingly to the interested application, in order to achieve the desired performances. Specifically, the implementation here proposed employs on-line signature as the given biometric characteristic. As remarked in Chapter 3, many sets of signature features have been proposed in the literature, and their

Index	Description	Index	Description	Index	Description
1	signature total duration T_s	34	direction histogram s_1 [174]	67	$(y_{max} - y_{min})/y_{acquisition\ range}$
2	N(pen-ups)	35	$(y_{2nd\ localmax} - y_{1st\ pen-down})/\Delta_y$	68	(1st $t(v_{x,max}))/T_w$
3	N(sign changes of dx/dt and dy/dt)	36	$(x_{max} - x_{min})/x_{acquisition\ range}$	69	(centripetal acceleration rms $a_c)/a_{max}$
4	average jerk $\overline{j}$ [173]	37	$(y_{1st\ pen-down} - x_{max})/\Delta_x$	70	spatial histogram t_1
5	standard deviation of a_y	38	$T(curvature > Threshold_{curv})/T_w$	71	θ(1st pen-down to 2nd pen-down)
6	standard deviation of v_y	39	(integrated abs. centr. acc. $a_{Ic})/a_{max}$ [174]	72	θ(1st pen-down to 2nd pen-up)
7	(standard deviation of $y)/\Delta_y$	40	$T(v_x > 0)/T_w$	73	direction histogram s_7
8	N(local maxima in x)	41	$T(v_x < 0 \vert pen - up)/T_w$	74	$t(j_{x,max})/T_w$
9	standard deviation of a_x	42	$T(v_x > 0 \vert pen - up)/T_w$	75	spatial histogram t_2
10	standard deviation of v_x	43	$(x_{3rd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	76	$j_{x,max}$
11	j_{rms}	44	$N(v_y = 0)$	77	θ(1st pen-down to last pen-up)
12	N(local maxima in y)	45	(acceleration rms $a)/a_{max}$	78	θ(1st-pen down to 1st pen-up)
13	$t(2ndpen - down)/T_s$	46	(standard deviation of $x)/\Delta_x$	79	(1st $t(x_{max}))/T_w$
14	(average velocity $\overline{v})/v_{x,max}$	47	$\frac{T((dx/dt)/(dy/dt)>0)}{T((dx/dt)/(dy/dt)<0)}$	80	$\overline{j}_x$
15	$\frac{A_{min}=(y_{max}-y_{min})(x_{max}-x_{min})}{\Delta_x=\sum_{i=1} pen-downs(x_{max\vert i}-x_{min\vert i})\Delta_y}$	48	(tangential acceleration rms $a_t)/a_{max}$	81	T(2nd pen-up)$/T_w$
16	$(x_{lastpen-up} - x_{max})/\Delta_x$	49	$(x_{2nd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	82	(1st $t(v_{max}))/T_w$
17	$(x_{1st\ pen-down} - x_{min})/\Delta_x$	50	$T(v_y < 0 \vert pen - up)/T_w$	83	$j_{y,max}$
18	$(y_{last\ pen-up} - y_{max})/\Delta_y$	51	direction histogram s_2	84	θ(2nd pen-down to 2nd pen-up)
19	$(y_{1st\ pen-down} - y_{min})/\Delta_y$	52	$t(3rd\ pen - down)/T_s$	85	j_{max}
20	$(T_w\overline{v})/(y_{max} - y_{min})$	53	(max distance between points)$/A_{min}$	86	spatial histogram t_3
21	$(T_w\overline{v})/(x_{max} - x_{min})$	54	$(y_{3rd\ local\ max} - y_{1st\ pen-down})/\Delta_y$	87	(1st $t(v_{y,min}))/T_w$
22	(pen-down duration $T_w)/T_s$	55	$(\overline{x} - x_{min})/\overline{x}$	88 – 89	(2st $t(x_{max}))/T_w$; (3rd $t(x_{max}))/T_w$
23	$\overline{v}/v_{y,max}$	56	direction histogram s_5	90	(1st $t(v_{y,max}))/T_w$
24	$(y_{last\ pen-up} - y_{max})/\Delta_y$	57	direction histogram s_3	91	$t(j_{max})/T_w$
25	$\frac{T((dy/dt)/(dx/dt)>0)}{T((dy/dt)/(dx/dt)<0)}$	58	$T(v_x < 0)/T_w$	92	$t(j_{y,max})/T_w$
26	$\overline{v}/v_{max}$	59	$T(v_y > 0)/T_w$	93	direction change histogram c_2
27	$(y_{1st\ pen-down} - y_{max})/\Delta_y$	60	$T(v_y < 0)/T_w$	94	(3rd $t(y_{max}))/T_w$
28	$(y_{last\ pen-up} - x_{min})/\Delta_x$	61	direction histogram s_8	95	direction change histogram c_4
29	(velocity rms $v)/v_{max}$	62	(1st $t(v_{x,min}))/T_w$	96	$\overline{j}_y$
30	$\frac{(x_{max}-x_{min})\Delta_y}{(y_{max}-y_{min})\Delta_x}$	63	direction histogram s_6	97	direction change histogram c_3
31	(velocity correlation $v_{x,y})/v_{max}^2$ [174]	64	T(1st pen-up)$/T_w$	98	θ(initial direction)
32	$T(v_y > 0 \vert pen - up)/T_w$	65	spatial histogram t_4	99	θ(before last pen-up)
33	N$(v_x = 0)$	66	direction histogram s_4	100	(2nd $t(y_{max}))/T_w$

Table 4.3: Features extracted from on-line signatures.

discriminatory capabilities have been evaluated employing various signature database. In order to test the effectiveness of the proposed on-line signature based cryptosystem, the 100 parametric features listed in Table 4.3, which have been used in [134], are here employed. The notations introduced in [134] to describe the considered features have been kept in Table 4.3. Specifically, T denotes time interval, t denotes time instant, N denotes number of events, while θ denotes angle. The features proposed in [134] and here employed have been defined in [173], [174] and [175].

As can be seen, the employed features are both static and dynamic, and are derived only from x and y position information. As reported in [134], the features are extracted from each signature by first performing a pre-processing, which consists of a subtraction of the center of mass, then followed by a rotation alignment, based on the average path tangent angle.

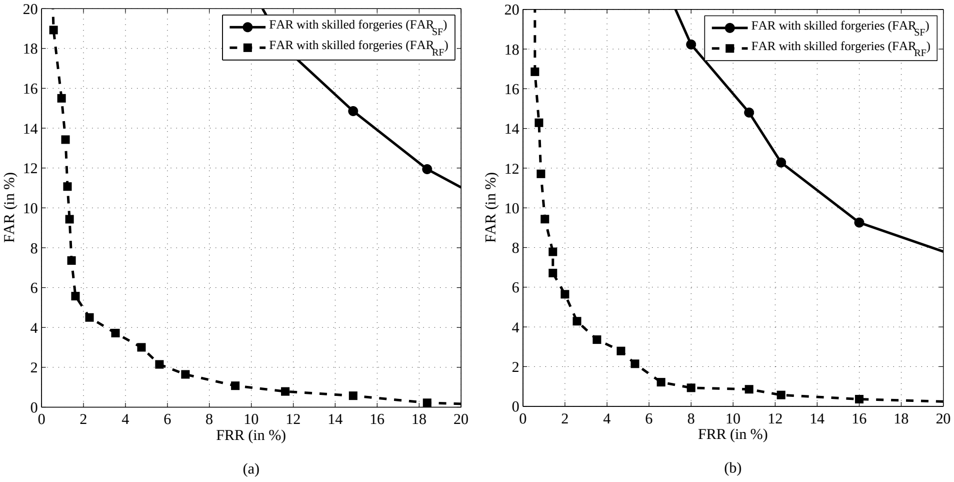
No information about pressure has been considered for our tests. Although this limitation could result in authentication performances worse than those already presented in literature for on-line signatures, it is worth pointing out that the effectiveness of the proposed approach should not be evaluated in absolute terms: the proposed system has been designed with the aim of providing protection to the feature extracted from a signature, at not trying to minimize the recognition errors given by the FRR and the FAR.

Then, in order to properly address the capabilities of the proposed system, the recognition performances achievable while providing protection have to be compared with those achievable when the employed templates are not protected. The set of features presented in [134] has been here employed to provide a specific reference to consolidated performances achievable when performing signature recognition using a parametric features based approach. The conducted analysis are presented in Section 4.3.

4.3 Signature based cryptosystem: Experimental Results

In this Section an extensive set of experimental results, concerning the performances of the proposed signature based cryptosystem, are presented. Specifically, the performances achievable employing the presented protection method are compared with those related to an unprotected system, as well as with those achievable when employing the *BioPKI* protection scheme described in [92].

As already stated in Section 3.3, the employed public MCYT Database, with signature taken from 100 users, has been divided in a training and a test data set. The training set, which comprises signatures taken from $W = 30$ users, is employed to estimate the inter-class mean vector $\boldsymbol{\mu}$ as described in Section 4.1.1. On the other hand, the remaining 70 users of the test data set are employed to evaluate the performances of the proposed



(a)

(b)

Figure 4.4: System performances without adaptive BCH code selection. (a): ROC curves obtained for $E = 5$ and $L = K = 100$; (b): ROC curves obtained for $E = 10$ and $L = K = 100$.

protected signature based cryptosystem, and to compare them with those achievable when performing recognition without providing protection, and those achievable employing the method in [92].

The first presented experiment is aimed at evaluating the system performances without the use of adaptive BCH code selection, thus employing the enrollment procedure described in Section 4.1.2.2. Several BCH codes, with different ECC, are employed to derive the system performances shown in Figure 4.4 in terms of FRR and FAR. More in detail, Figure 4.4(a) illustrates the results which can be obtained considering $E = 5$ signatures for the enrollment of each user, while Figure 4.4(b) is obtained with reference to a system where $E = 10$ signatures are acquired from each user during enrollment. The reported ROC curves are evaluated by varying the BCH ECCs employed in the system. The reported FRRs are estimated using, for each subject, the signatures not used in the enrollment stage. The FAR is both referred to conditions of random forgeries [122], indicated as FAR$_{RF}$, and to conditions of skilled forgeries, indicated as FAR$_{SF}$. For each user, the 25 signatures given from all the remaining 69 users of the test data set are used as random forgeries. The 25 skilled forgeries available for each user have been consider to determine the system FAR$_{SF}$.

The results shown in Figure 4.4 are obtained when considering $L = K = 100$, that

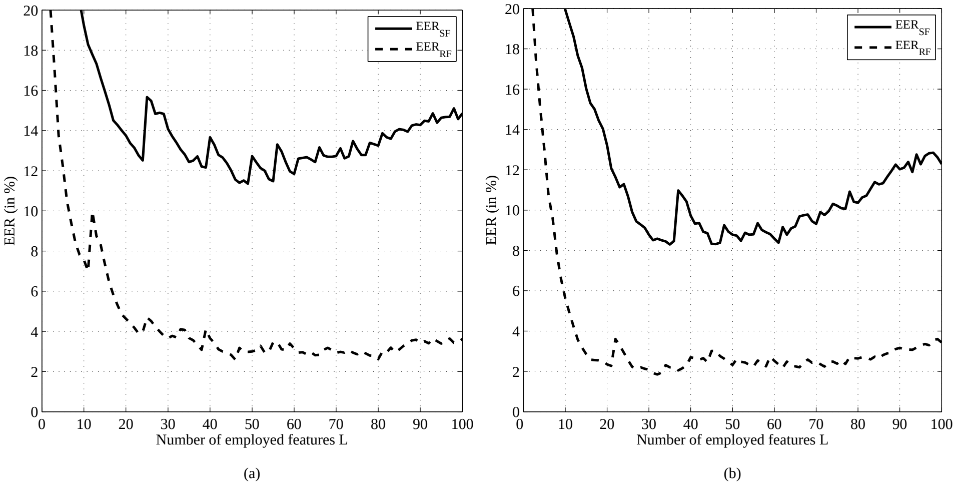
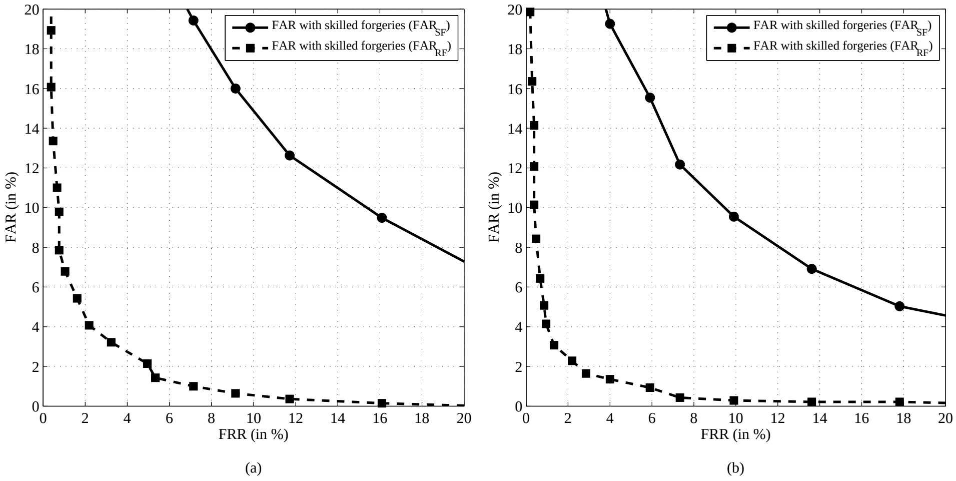


Figure 4.5: System performances without adaptive BCH code selection. (a): EERs for $E = 5$, with respect to the employed number of features L; (b): EERs for $E = 10$, with respect to the employed number of features L.

is, when the feature selection procedure described in Section 4.1.2.1 is not considered. Specifically, the equal error rate obtained for skilled forgeries (EER$_{SF}$) is 12.29% when considering $E = 10$, and 14.86% when taking $E = 5$. When random forgeries are taken into account, the obtained equal error rates (EER$_{RF}$) are equal to 3.43% for $E = 10$, and 3.62% for $E = 5$.

The effectiveness of the feature selection method of Section 4.1.2.1 is shown in Figure 4.5, where the EERs achievable for both skilled and random forgeries are displayed, with respect to the number of employed features $L \leq K$.

As can be seen, the minimum EERs are achieved, for both systems with $E = 5$ and $E = 10$, by considering even less than 50 features out of 100: as for skilled forgeries, the lowest value of EER$_{SF}$ is equal to 8.30% when $E = 10$, and is achieved representing signature templates with $L = 35$ features. When $E = 5$ signatures are acquired during enrollment, the lowest achievable EER$_{SF}$ is 11.35%, obtained for $L = 49$ features. On the other hand, when random forgeries are taken into account, the lowest value of EER$_{RF}$, when taking $E = 10$ signatures for enrollment, is equal to 1.85%, and is achieved considering $L = 32$ features, whereas taking $E = 5$ the lowest achievable EER$_{RF}$ is 2.60%, obtained for $L = 46$ features.



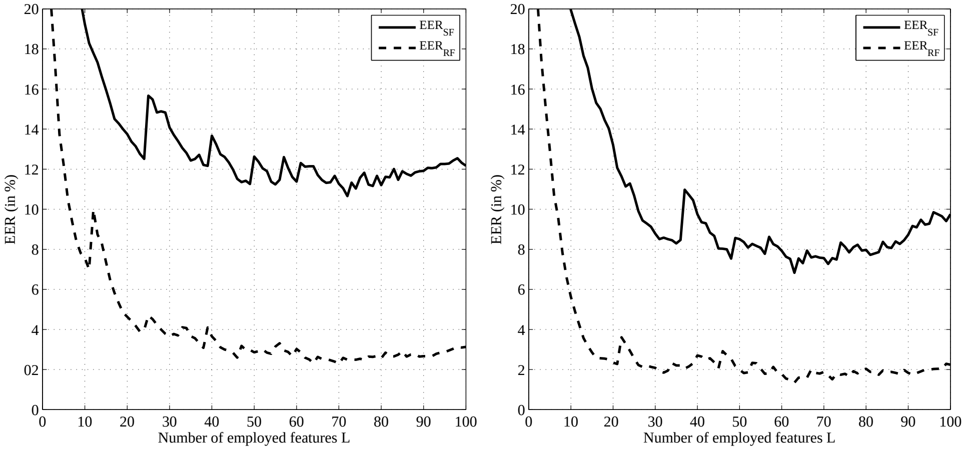
(a)

(b)

Figure 4.6: System performances with the adaptive BCH code selection. (a): ROC curves obtained for $E = 5$ and $L = K = 100$; (b): ROC curves obtained for $E = 10$ and $L = K = 100$.

The performances of a system using the proposed adaptive codes selection scheme, described in Section 4.1.2.3, are then analyzed, in order to verify if better recognition performances can be achieved employing it, with respect to the non-adaptive approach of Section 4.1.2.2. Specifically, Figure 4.6(a) illustrates the results which can be obtained by considering $E = 5$ signatures for the enrollment of each user, while Figure 4.6(b) is obtained in reference to a system where $E = 10$ signatures are acquired from each user during enrollment. The presented ROC curves are obtained by evaluating the values of FRR and FAR achievable for different values of the system parameter Δ_{ECC}, introduced in Section 4.1.2.3. As for Figure 4.4, even the results shown in Figure 4.6 are obtained by considering $L = K = 100$ selected features, that is, by not employing the feature selection procedure described in Section 4.1.2.1. The equal error rate obtained for skilled forgeries (EER_{SF}) is 9.75% when considering $E = 10$, and 12.17% when taking $E = 5$. When random forgeries are taken into account, the obtained equal error rates (EER_{RF}) are given by 2.24% for $E = 10$, and by 3.13% for $E = 5$.

The results obtained by combining the proposed feature selection approach of Section 4.1.2.1, with the adaptive ECC selection described in Section 4.1.2.3, are displayed in Figure 4.7, where the EERs achievable for both skilled and random forgeries are illustrated, with



(a)

(b)

Figure 4.7: System performances with the adaptive BCH code selection. (a): EERs for $E = 5$, with respect to the employed number of features L; (b): EERs for $E = 10$, with respect to the employed number of features L.

respect of the number of employed features.

From the presented results, it can be noticed that when employing the proposed user adaptive ECC selection procedure, the best performances are obtained when taking into account a number of features approximately comprised between 60 and 70, having available an initial set with 100 parameters: as for skilled forgeries, the lowest value of EER$_{SF}$ is equal to 6.83% for $E = 10$, and is achieved representing signature templates with $L = 63$ features. When $E = 5$ signatures are taken during enrollment, the lowest achievable EER$_{SF}$ is 10.66%, obtained employing $L = 72$ features. On the other hand, when random forgeries are taken into account, the lowest value of EER$_{RF}$, when taking $E = 10$ signatures for enrollment, is equal to 1.35%, and is achieved considering $L = 63$ features. When setting $E = 5$, the lowest achievable EER$_{RF}$ is 2.29%, obtained using $L = 70$ features.

The obtained experimental results highlight that the use of the proposed adaptive code selection procedure significantly improves the system performances. Moreover, the achievable recognition rates can be furthered improved when performing a user dependent selection of the features which have to be considered, by means of the reliability measures introduced in Section 4.1.2.1.

Finally, a performance comparison among the proposed methods, a system where no template protection is taken into account, and the protected approach proposed in [92], is here reported. Specifically, the Malahanobis distance is employed in an unprotected system to compute the dissimilarity between a given features vector $\mathbf{f}[k]$, and the intra-class mean feature vector $\boldsymbol{\mu}^u[k]$, representative of user u, as:

$$D(\mathbf{f}[k], \boldsymbol{\mu}^u[k]) = \sqrt{\sum_{k=1}^{K} \Big(\frac{\mathbf{f}[k] - \boldsymbol{\mu}^u[k]}{\boldsymbol{\sigma}^u[k]}\Big)^2} \tag{4.11}$$

where $\boldsymbol{\sigma}^u[k]$ is the feature standard deviation vector for user u, estimated during enrollment employing the available E acquisitions. If the distance $D(\mathbf{f}[k], \boldsymbol{\mu}^u[k])$ is lower than a preselected threshold T_A, the features vector $\mathbf{f}[k]$ is accepted as originating from the legitimate user u.

As for the protected approach described in [92], it consists of three stages: the shape matching, the feature coding and the private key generation. The shape matching stage examines the shape of a test sample, and filters out the random and simple forgeries. The feature coding stage finds a feature code for each of the defined features, and concatenates each feature code into a code string. Finally, the private key generation stage takes the code string as input, and generates the individuals private key. Specifically, in order to compare the method proposed in [92] with the one here presented, the feature coding and the private key generation stages is implemented, in order to protect the extracted signature features and to perform user authentication.

Three boundaries are defined for each considered feature in [92]:

- the whole boundary, which includes all possible values for a feature;
- the database boundary, which includes the values collected from all the acquired signature;
- the user boundary, which includes values for a specific user.

The user boundary ($\mathbf{UB}^u$) for each feature k is defined as $\mathbf{UB}^u[k] = \boldsymbol{\mu}[k] - b \times \boldsymbol{\sigma}[k], \boldsymbol{\mu}[k] + b \times \boldsymbol{\sigma}[k])$, where $\boldsymbol{\mu}[k]$ and $\boldsymbol{\sigma}[k]$ are respectively the estimated mean and the standard deviation of features k, for the signatures of the considered user u. The system parameter b can be adjusted according to the desired performances: a higher value corresponds to more error tolerance, and at the same time, easier barriers for forgeries.

The feature coding implies the segmentation of the whole boundary, which is divided into several segments with an assigned sequence number. The segmentation takes place by unfolding the user boundary to both ends before exceeding the database boundary. The superfluous portion at either end would be extended into the whole boundary and becomes one segment. Considering a particular feature value, the system fits it into a segment and obtains the feature code, that is, the segment sequence number. After processing all the features, the feature codes are concatenated to output a code string. The template includes the boundary definitions, without any hint on a particular segment. Finally, in order to obtain a private key from the obtained code string, a SHA1-hash is then computed, resulting in a 160-bit private key.

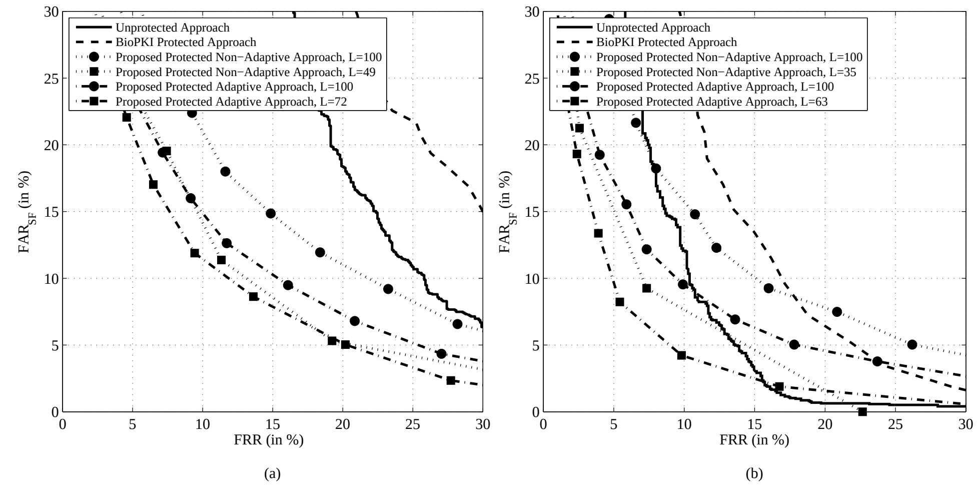
Figure 4.8 shows the ROC curves, related to the $\text{FAR}_{SF}/\text{FRR}$ behavior obtained considering skilled forgeries, which are achievable by implementing various approaches. Specifically, Figure 4.8 shows the performances obtained when considering:

- a system without any template protection, and using the Mahalanobis distance based matcher, where the threshold t is continuously varied;

- a system implementing the *BioPKI* protection approach described in [92], where the system parameter b, that acts similar to a threshold, is continuously varied;

- a system implementing the non-adaptive approach presented in this Chapter, using different ECC values and taking $L = K = 100$ features, in order to compare the achieved results with those achievable by the unprotected approach, and the *BioPKI* system proposed in [92];

- a system implementing the non-adaptive approach presented in this Chapter, using different ECC values while selecting, through the procedure described in Section 4.1.2.3, the subset of features which guarantees the best verification rates, in order to compare the achieved results with those obtained when considering the whole set of $K = 100$ features. Specifically, when $E = 10$, $L = 35$ features are selected, whereas $L = 49$ features are taken into account when $E = 5$ signature are considered for the enrollment;



(a)

(b)

Figure 4.8: Comparison between the system performances achievable by employing the proposed adaptive and non adaptive approaches, an unprotected approach based on Mahalanobis distance, and the protected approach described in [92]. (a): ROC curves obtained for $E = 5$; (b): ROC curves obtained for $E = 10$.

- a system implementing the adaptive code selection approach presented in this Chapter, using different values of Δ_{ECC} and considering $L = K = 100$ features, in order to present results comparable with those of the unprotected method, and the *BioPKI* system proposed in [92];

- a system implementing the adaptive approach presented in this Chapter, using different values of Δ_{ECC} while selecting, through the procedure described in Section 4.1.2.3, the subset of features which guarantees the best recognition rates, in order to compare the achieved results with those obtained when considering the whole set of $K = 100$ features. Specifically, when $E = 10$, $L = 63$ features are selected, whereas $L = 72$ features are taken when $E = 5$ signature are considered for the enrollment.

In order to summarize the obtained results, the EERs achievable using the unprotected approach, the method proposed in [92], as well as the proposed protected approaches, are summarized in Table 4.4, having considered tests with $E = 10$ signatures taken during enrollment for each user, and skilled forgeries for the estimation of the FAR.

As can be seen in Figure 4.8, the ROC curves obtained by employing the non-adaptive

	Non-Protected	*BioPKI*	Non-Adaptive Approach		Adaptive Approach	
	Approach	Approach in [92]	$L = K = 100$	$L = 35$	$L = K = 100$	$L = 63$
EER_{SF} (in %)	10.31	14.28	12.29	8.30	9.75	6.83

Table 4.4: EERs for the considered approaches, considering skilled forgeries and $E = 10$ signatures taken during enrollment for each user.

approach described in Section 4.1.2.2, by varying the employed ECC, move away from the behavior of the unprotected system, resulting in better performances in terms of FRR, being thus more suitable for forensic application [6] with respect of the other considered methods. Moreover, the best achievable EER, when considering the whole set of features enumerated in Table 4.3 with $L = K = 100$, is obtained using the proposed user adaptive fuzzy commitment approach. The performances achievable employing the method in [92] are worse than those obtained by an unprotected system, and even than those achievable employing the proposed protected systems. In [77] it has also been shown that the performances achievable employing the protected key generating cryptosystem described in [91], which also relies on the processing of parametric features extracted from signatures, follows approximately the same behavior offered by the method in [92]. Also the performances achievable employing the method in [91] are therefore worse than those obtained employing the proposed approaches.

Finally, it is worth pointing out that, as shown in Figure 4.8, even better performances can be obtained by using the proposed approaches when the parameters reduction procedure described in Section 4.1.2.1 is taken into account. Moreover, the proposed method is also able to provide, in addiction to template protection, the cancelability of templates, where the other considered methods in [92] and [91] cannot.

4.4 On-line Signature based Cryptosystem: Discussion

In this Chapter, a user adaptive template protection scheme applied to signature biometrics is proposed. The proposed scheme is able to provide protection to the considered signature templates, and allows to manage cancelable biometrics, being therefore possible to generate multiple templates from the same biometric data. Properly using error correcting codes, the original raw data, as well as the template derived from them, cannot be reconstructed from the stored information, thus increasing the system security against possible attacks, while allowing to perform user authentication with performances comparable to an unprotected system.

The proposed protection scheme is applied to parametric features extracted from on-line signatures. A reliability measure, independent from the features distributions, is provided. Moreover, a user adaptive intra-class variability handling is implemented, in order to customize the error correction capabilities of the employed codes for each enrolled user: in this way, the employed codes are selected depending on the characteristics of each user, thus increasing the achievable recognition performances.

Extensive experimental results are provided, showing that the proposed system is able to guarantee verification performances comparable with those achievable in an unprotected system. Comparisons with other already proposed scheme for on-line signature templates protection, employing parametric features extracted from the acquired data, are also presented.

Chapter 5

Cancelable Sequence based Biometric Templates

In this Chapter, we consider the issue of providing protection and renewability to those biometric templates which can be expressed in terms of a set of time or space dependent sequences. Specifically, a non-invertible transform based approach is employed, in order to generate transformed templates which can be stored safely in a system database, without revealing any information about the originally acquired biometric characteristic. As it will be outlined in the present Chapter, the proposed approach is independent on the biometric modality under consideration, and it could be therefore applied to different biometrics, like for example speech, signature, gait, brain activity [176], iris [177], and so on. Following the essay of the present Thesis, the effectiveness of the proposed approaches has been evaluated by applying them to an on-line signature based biometric verification system.

It is worth pointing out that, as outlined in Chapter 2, in the most of cases the methods proposed for the protection of biometric templates act on sets of parametric features, extracted from the considered biometrics. This approach is usually followed even for those biometrics which can be represented by sets of time or space dependent sequences. However, resorting to parametric features representations of biometric data unavoidably limits the kind of matching which can be performed. Employing a non-invertible transform based approach, in order to provide protection for biometric templates which can be expressed by a set of discrete sequences, the transformed templates can remain in the same (feature) space of the original ones, being then possible to employ matching schemes specifically designed for the considered biometrics. When taking on-line signature authentication systems into account, matching approaches based on elastic procedures such as Dynamic Time Warping (DTW), which represents one of the more flexible approaches to manage the signature length variability [139], or based on statistical recognition approaches such as those employing Hidden Markov Models (HMMs) [121, 141], can be employed even in the transformed domain. This possibility allows to achieve verification performances typically better than those obtained following approaches based on the extraction of parametric features, like the one proposed by the author in Chapter 4.

The organization of the present Chapter is as follows. The proposed approach for the protection of sequence based biometric templates is illustrated in Section 5.1, and its security analysis is outlined in Section 5.2. The application of the proposed protection scheme to on-line signature biometrics is then presented in Section 5.3. The experimental framework considered in order to verify the effectiveness of the proposed approaches, and the results which are obtained by testing the proposed system, are shown in Section 5.4, Section 5.5 and Section 5.6, while some final considerations on the proposed approaches are eventually drawn in Section 5.7.

5.1 Non-invertible Transforms for Sequence based Biometrics

The proposed approach for the protection of sequence based biometric templates relies on the definition of a novel set of non-invertible transforms, which extends the work presented in [111]. In the proposed biometric protection scheme, it is supposed that a set of time/space dependent discrete finite sequences are extracted from a given biometric characteristic. The obtained biometric template can then be protected by applying the transforms defined in Sections 5.1.1 and 5.1.2. The resulting transformed templates can then be further processed if the matcher is based on a sequence based modeling approach (e.g., HMM), or directly stored in the system database if the matcher works directly with sequence based descriptions (e.g., DTW).

Specifically, it is assumed that the proposed transforms can be applied to an original set of sequences $\mathcal{R}_F$, consisting of F sequences $r_{(i)}[n]$, $i = 1, \ldots, F$. The transformed template is indicated as $\mathcal{T}_F$, and consists of F sequences $f_{(i)}[n]$, $i = 1, \ldots, F$. In Section 5.1.1 a baseline sequence based template transform, specifically designed in such a way that it is not possible to retrieve the original data from the transformed ones, is proposed. Moreover, in Section 5.1.2 some alternatives for the protection of sequence based biometric templates, derived from the baseline approach of Section 5.1.1, will be detailed.

5.1.1 Protected Baseline Approach

The proposed transformations, applied to the original set of sequences $\mathcal{R}_F$ for the generation of a new set $\mathcal{T}_F$, are designed to satisfy the following properties, that are sufficient (although not necessary) to guarantee the non-invertibility and renewability properties of a properly defined cancelable biometrics, as outlined in Chapter 2:

- each transformed sequence has to be generated from the combination of at least two original time sequences (or segments of them). This requirement is needed when employing transformations expressed by means of linear dependencies on the original data. Linear combinations have been preferred in the deployment of the proposed approaches, in order to alter as less as possible (although in a non-invertible way) the characteristics of the original sequences, in both space/time and frequency domains;

- each original time sequence (or a segment of it) has to occur only in one of the combinations that generate the new sequences. This requirement is needed in order to generate transformed sequences which are independent one from the others. In such a way, even when combining different sequences belonging to the same transformed template, it will be impossible to invert the employed transforms and obtain the original sequences;

- when generating transformed sequences for two distinct systems, the sequences selected for the combinations (or the segments extracted from them) have to be different for the two distinct cases. This requirement is needed to define transforms which are robust with respect of a *record multiplicity attack*, where an attacker gains access to different transformed versions of the same original data, and tries to reveal the original biometric templates by exploiting all the gathered information.

In the baseline implementation, each transformed sequence $f_{(i)}[n]$, $i = 1, \ldots, F$, is obtained from the corresponding original sequence $r_{(i)}[n]$ of length N, $i = 1, \ldots, F$, which represents a generic original discrete time/space sequence selected among the ones available in the original template, as follows.

A number $(W-1)$ of different integer values d_j between 1 and 99 are randomly selected, ordered in an ascending way such that $d_j > d_{j-1}$, $j = 1, \ldots, W$, and arranged in a vector

$$\mathbf{d} = [d_0, \ldots, d_W]^T, \tag{5.1}$$

where d_0 and d_W are set to 0 and 100 respectively. The vector $\mathbf{d}$ represents the key of the employed transformation.

Then, the original sequence $r_{(i)}[n]$ is divided into W segments $r_{(i)j,N_j}[n]$ of length $N_j = b_j - b_{j-1}$,

$$r_{(i)j,N_j}[n] = r_{(i)}[n + b_{j-1}], \quad j = 1, \ldots, W, \tag{5.2}$$

where $b_j = \lceil \frac{d_j}{100} \cdot N \rceil$, $j = 1, \ldots, W$.

Basically, the sequence $r_{(i)}[n]$ is split into W non overlapping parts according to the randomly generated vector $\mathbf{d}$. A transformed sequence $f_{(i)}[n]$, $n = 1, \ldots, K$, is then obtained through the linear convolution of the sequences $r_{(i)j,N_j}[n]$, that is,

$$f_{(i)}[n] = r_{(i)1,N_1}[n] * \ldots * r_{(i)W,N_W}[n]. \tag{5.3}$$

Each transformed sequence $f_{(i)}[n]$ is therefore obtained through the linear convolution of parts of the corresponding original sequences $r_{(i)}[n]$, $i = 1, \ldots, F$. Moreover, each original sequence $r_{(i)}[n]$, $i = 1, \ldots, F$ undergoes the same decomposition before applying the convolutions. As can be seen, due to the convolution operation in equation (5.3), the length of the transformed sequences is equal to $K = N - W + 1$, being therefore almost the same of the original sequences. A final signal normalization, oriented to obtain zero mean and unit standard deviation transformed sequences, is then applied. Different realizations can be obtained from the same original sequences, simply varying the size or the values of the

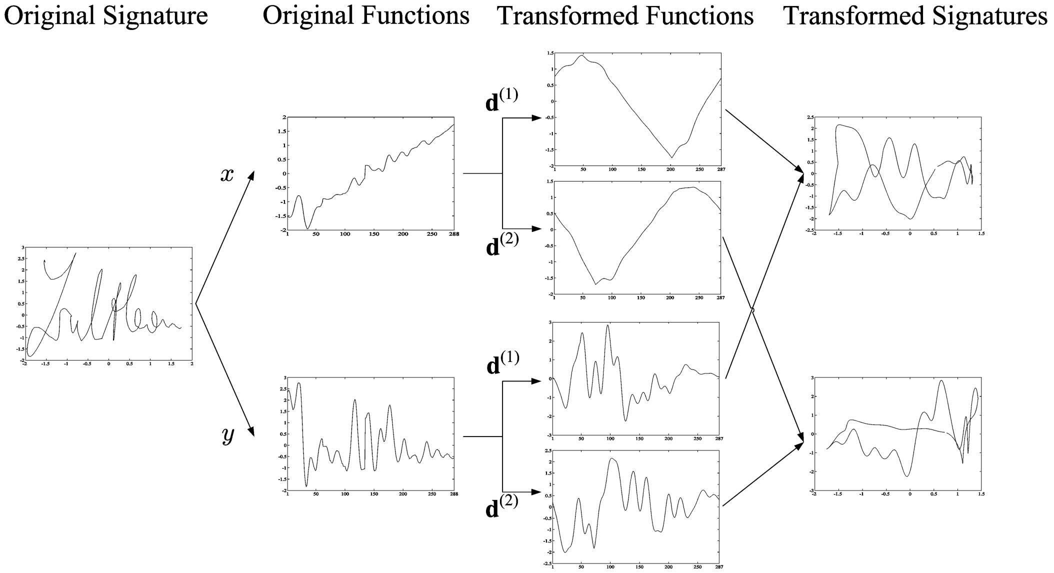


Figure 5.1: Baseline approach: two different transformations, governed by the key vectors $\mathbf{d}^{(1)} = [0\ 30\ 100]$ and $\mathbf{d}^{(2)} = [0\ 75\ 100]$, are applied to the original $x[n]$ and $y[n]$ coordinate sequences. The original and transformed signatures are also shown.

parameter key $\mathbf{d}$. The complete set of transformed sequences $f_{(i)}[n]$, $i = 1, \ldots, F$, is indicated as $\mathcal{T}_F$. As it has already been noticed, the transformed templates are yet represented as set of discrete time/space sequences, exactly like the original employed templates, being thus possible to resort to sophisticated classifiers such as HMMs or DTW in order to match them.

The effects of the employed transforms are shown in Figure 5.1 for the case with $W = 2$, where the horizontal and vertical position trajectories extracted from an original signature are transformed according to different decomposition vectors, and then recombined to reconstruct a transformed signature.

The security analysis of the proposed sequence based protection scheme is conducted in Section 5.2.

5.1.2 Non-invertible transform: extended approaches

In the previous Section it has been illustrated how to generate a transformed sequence from an original one. Two additional non-invertible sequence based transforms, stemming from the approach presented in Section 5.1.1, are proposed in the following.

5.1.2.1 Protected Mixing approach

In the baseline approach, each transformed sequence is generated by performing convolutions between segments belonging from the same original sequence. However, it is also possible to combine segments extracted from different original sequences. In order to formally define this kind of transform, a transformation key **C**, consisting of a matrix with F rows and W columns, has to be considered in this case, in addition to the decomposition key **d**. Specifically, each column of **C** is obtained as a scrambled version of the vector $[1, \ldots, F]^T$. An example of a possible matrix **C**, when considering $F = 7$ and $W = 4$, is shown in equation (5.4):

$$\mathbf{C} = \begin{bmatrix} 1 & 4 & 3 & 7 \\ 2 & 7 & 2 & 5 \\ 3 & 1 & 6 & 1 \\ 4 & 2 & 7 & 3 \\ 5 & 6 & 1 & 4 \\ 6 & 5 & 5 & 2 \\ 7 & 3 & 4 & 6 \end{bmatrix}. \tag{5.4}$$

Each i-th row of the matrix **C** is employed to define the combinations that originate the transformed sequences $f_{(i)}[n]$. Having indicated with $C[i, j]$ the element at the i-th row and at the j column of **C**, the transformed time sequences $f_{(i)}[n]$ are obtained as:

$$f_{(i)}[n] = r_{(C[i,1])1,N_1}[n] * \ldots * r_{(C[i,W])W,N_W}[n], \tag{5.5}$$

with $i = 1, \ldots, F$, and where $r_{(i),j,N_j}[n]$ is defined as in equation (5.2). Basically, each transformed sequence $f_{(i)}[n]$ is generated not only from the corresponding original sequence $r_{(i)}[n]$, but the convolutions are performed among segments extracted from different original sequences, thus also defining a kind of feature-level fusion [104] among various sequences.

5.1.2.2 Protected Shifting approach

Another variation to the approach in 5.1.1 is obtained by applying an initial shift to the original sequences $r_{(i)}[n]$, $i = 1, \ldots, F$. Specifically, a random integer value ϕ is selected in the range [0,100], and converted to the shift h as

$$h = \lceil \frac{\phi}{100} \cdot N \rceil, \tag{5.6}$$

being N the length of the original sequence, in sample units. Then, each sequence $r_{(i)}[n]$ undergoes the same circular shift governed by the parameter h, thus obtaining the sequences $c_{(i)}[n] = r_{(i)}[n-h]$, $n = 1, \ldots, N$.

The same transformation process described in Section 5.1.1, based on convolutions between segments extracted from the considered sequences, is then applied to the sequences $c_{(i)}[n]$. This modification can be also combined with the extended method presented in Section 5.1.2.1, by applying the circular shift before performing the transformations. Obviously, it is also possible to apply different initial shifts to the F sequences before performing the decompositions, in order to further increase the transformation key space. However, only the case where the same shift is applied to all the available original sequences will be considered in the following.

5.2 Transform Invertibility Analysis

As it has been reported in Chapter 2 when presenting the possible solutions proposed for the protection of a given biometric template, a properly defined cancelable biometrics should satisfy the requirements of renewability and security, and should guarantee recognition performances similar to those achievable with an unprotected approach. In order to test the renewability property, and also to evaluate the loss in recognition performances introduced by the proposed protection scheme, it is necessary to apply the proposed transformations to a specific biometric characteristic, and also to employ a specific matching algorithm for the transformed sequence based templates. These analysis will then be conducted in Section 5.5 and 5.6, after having defined in Section 5.3 the used discrete time sequences based template for on-line signatures, together with the matching strategies employed to perform on-line signature authentication in the protected domain.

On the other hand, the analysis of the invertibility, that is, the possibility of recovering the original sequences, from the ones obtained employing the proposed transformation schemes, is investigated in this Section. Specifically, this analysis does not need to be referred to a specific biometric modality, being related only to the transformations designed in Section 5.1. Furthermore, being the extended methods of Section 5.1.2 basically modifications of the principal approach described in Section 5.1.1, only the latter one is here analyzed, due to the fact that the security of the extended methods depends on the one provided by the baseline approach.

It is worth pointing out that the non-invertibility here discussed is different from the one commonly encountered in mathematics, being more focused on the computational difficulty in inverting the employed transforms. In fact, as it has been noticed in [178] when dealing the non-invertibility of the *one-way functions* employed in a public key cryptosystem, in mathematics a given function is called non-invertible when the inverse of a point of the function is not unique. On the other hand, the non-invertibility required in the context of biometric protection deals with the overwhelming difficulty which should be encountered when trying to calculate the original data from the transformed ones.

Having defined the sequence transformation as in equation (5.3), if an attacker gains access to the stored information, he has to solve a *blind deconvolution* problem [179, 180, 181] to retrieve any information regarding the original sequences. Typically, the goal of blind deconvolution is to recover a source signal given only the output of an unknown filter, or to separate different source signals from their convolutive mixtures. To solve these problems, some statistical properties of the filter, or of the considered sources, have to be assumed, or some other constraints have to be established [182]. In the considered case, the transformed template $\mathcal{T}_F$ contains only convolutions between segments extracted from the original sequences. Then, it is computationally very hard to recover, in a deterministic way, the original data from the transformed ones. In other words, the security of the proposed sequence based template protection methods relies on the difficulty to solve a blind deconvolution problem, having no *a priori* knowledge about the original sequences.

On the other hand, also considering different transformed templates based on the same original data, which is commonly referred to a *record multiplicity attack*, recovering the original sequences is as much hard as random guessing. As already discussed in Chapter 2, the possibility of performing record multiplicity attacks is one of the major problems of popular template protection schemes such as the fuzzy vault [70]. Moreover, also the already proposed non-invertible transform based methods for the protection of fingerprints, [106] and [107], are vulnerable to such an attack. In order to properly illustrate the robustness of the approach here proposed against record multiplicity attacks, we assume that the different transformed versions are derived from exactly the same original data.

It is worth pointing out that this is a worst condition case, because in real life applications the realizations of the original biometrics used in different applications, on which the multiplicity attack is based, will vary depending on the intra-user biometric variability. Moreover, when the considered biometrics is signature, this intra-user variability is specifically significant. However, under the considered assumption, it is then supposed that an attacker has acquired, from two different systems, two different transformed sets of sequences $\mathcal{T}_F^{(1)}$ and $\mathcal{T}_F^{(2)}$, generated from the same original template $\mathcal{R}_F$, by applying different transformation parameters. Considering the simplest case with $W = 2$, the attacker then possesses two transformed instances, $f_{(i)}^{(1)}[n]$ and $f_{(i)}^{(2)}[n]$, of the same original time sequences $r_{(i)}[n]$, $i = 1, \ldots, F$, obtained using the two transformation parameters $d_1^{(1)}$ and $d_1^{(2)}$ (the decomposition vectors defined in equation (5.1) contain only one random element, being $W = 2$). Given that

$$r_{(i)}[n] = r^{(1)}_{(i)1,N_1^{(1)}}[n] + r^{(1)}_{(i)2,N_2^{(1)}}[n - b_1^{(1)}] = r^{(2)}_{(i)1,N_1^{(2)}}[n] + r^{(2)}_{(i)2,N_2^{(2)}}[n - b_1^{(2)}], \tag{5.7}$$

in order to recover the sequence $r_{(i)}[n]$, the attacker should obtain the segments $r^{(1)}_{(i)1,N_1^{(1)}}[n]$ and $r^{(1)}_{(i)2,N_2^{(1)}}[n]$, where $N_1^{(1)} = b_1^{(1)}$ and $N_2^{(1)} = N - b_1^{(1)}$, or the segments $r^{(2)}_{(i)1,N_1^{(2)}}[n]$ and $r^{(2)}_{(i)2,N_2^{(2)}}[n]$, with $N_1^{(2)} = b_1^{(2)}$ and $N_2^{(2)} = N - b_1^{(2)}$, from the available transformed sequences $f_{(i)}^{(1)}[n] = r^{(1)}_{(i)1,N_1^{(1)}}[n] * r^{(1)}_{(i)2,N_2^{(1)}}[n]$ and $f_{(i)}^{(2)}[k] = r^{(2)}_{(i)1,N_1^{(2)}}[n] * r^{(2)}_{(i)2,N_2^{(2)}}[n]$.

Deconvolution problems are typically coped with in the frequency domain, being the convolutions transformed into simple multiplications. In order to properly define the Discrete Fourier Transforms (DFTs) of the considered segments of $r_{(i)}[n]$, the extended versions $\hat{r}^{(j)}_{(i)h,K}[n]$, $h, j = \{1, 2\}$, are generated by applying zero padding to the right of the segments, until reaching the length $K = N - 1$ (that is the length of the convolutions $f_{(i)}^{(1)}[n]$ and $f_{(i)}^{(2)}[n]$). Then, the sequence $\Delta_{(i)}[n]$, $n = 1, \ldots, K$, is defined as the difference between $\hat{r}^{(1)}_{(i)1,K}[n]$ and $\hat{r}^{(2)}_{(i)1,K}[n]$, which share a common part that is exactly $r^{(2)}_{(i)1,K}[n]$, having assumed that $b_1^{(1)} > b_1^{(2)}$:

$$\Delta_{(i)}[n] = \hat{r}^{(1)}_{(i)1,K}[n] - \hat{r}^{(2)}_{(i)1,K}[n], \quad n = 1, \ldots, K. \tag{5.8}$$

The following relations can then be derived for the considered finite sequences:

$$\begin{cases} \hat{r}^{(1)}_{(i)1,K}[n] = \hat{r}^{(2)}_{(i)1,K}[n] + \Delta_{(i)}[n] \\ \hat{r}^{(1)}_{(i)2,K}[n - b_1^{(1)}] = \hat{r}^{(2)}_{(i)2,K}[n - b_1^{(2)}] - \Delta_{(i)}[n] \end{cases} \tag{5.9}$$

where all the considered shifts are circular shifts. Then, applying the DFT to the *a priori* known sequences $f^{(1)}_{(i)}$ and $f^{(2)}_{(i)}$, and considering the relations between the DFT and the linear convolution of two discrete sequences, it results:

$$\begin{cases} \text{DFT}\{f^{(1)}_{(i)}[n]\} = \text{DFT}\{\hat{r}^{(1)}_{(i)1,K}[n]\} \cdot \text{DFT}\{\hat{r}^{(1)}_{(i)2,K}[n]\} = \\ \quad \text{DFT}\{\hat{r}^{(1)}_{(i)1,K}[n]\} \cdot \text{DFT}\{\hat{r}^{(1)}_{(i)2,K}[n - b_1^{(1)}]\} \cdot e^{j2\pi(l/K)b_1^{(1)}} \\ \text{DFT}\{f^{(2)}_{(i)}[n]\} = \text{DFT}\{\hat{r}^{(2)}_{(i)1,K}[n]\} \cdot \text{DFT}\{\hat{r}^{(2)}_{(i)2,K}[n]\} \end{cases} \tag{5.10}$$

where the DFT coefficients are indexed with k. Using the relations in equation (5.9), the first equation of (5.10) can be written as:

$$\begin{aligned} \text{DFT}\{f^{(1)}_{(i)}[n]\} = &\left[\text{DFT}\{\hat{r}^{(2)}_{(i)1,K}[n]\} + \text{DFT}\{\Delta_{(i)}[n]\}\right] \cdot \\ &\left[\text{DFT}\{\hat{r}^{(2)}_{(i)2,K}[n - b_1^{(2)}]\} - \text{DFT}\{\Delta_{(i)}[n]\}\right] \cdot e^{j2\pi(l/K)b_1^{(1)}} \end{aligned} \tag{5.11}$$

and therefore:

$$\begin{cases} \text{DFT}\{f^{(1)}_{(i)}[n]\} = e^{j2\pi(l/K)b_1^{(1)}} \cdot \Big[\text{DFT}\{\hat{r}^{(2)}_{(i)1,K}[n]\} \cdot \text{DFT}\{\hat{r}^{(2)}_{(i)2,K}[n]\} \cdot e^{-j2\pi(l/K)b_1^{(2)}} - \\ \quad \text{DFT}\{\Delta_{(i)}[n]\} \cdot \text{DFT}\{\hat{r}^{(2)}_{(i)1,K}[n]\} + \text{DFT}\{\Delta_{(i)}[n]\} \cdot \text{DFT}\{\hat{r}^{(2)}_{(i)2,K}[n]\} \cdot e^{-j2\pi(l/K)b_1^{(2)}} - \\ \quad \text{DFT}^2\{\Delta_{(i)}[n]\}\Big] \\ \text{DFT}\{f^{(2)}_{(i)}[n]\} = \text{DFT}\{\hat{r}^{(2)}_{(i)1,K}[n]\} \cdot \text{DFT}\{\hat{r}^{(2)}_{(i)2,K}[n]\} \end{cases} \tag{5.12}$$

As can be seen, the resulting system of equations admits inf^1 possible solutions, which implies that recovering the original segments $r^{(2)}_{(i)1,K}[n]$ and $\hat{r}^{(2)}_{(i)2,K}[n]$ is as much hard as random guessing. Although with such demonstration is not possible to state that the proposed transforms are non-invertible, independently from the approach which is employed when trying to invert them, the difficulty in reaching a solution for the original sequence observed in the proposed formulation (which is the most natural, being based on spectral techniques for solving the blind deconvolution problem), corroborates the difficulty in succeeding in a record multiplicity attack.

5.3 Application to an On-line Signature Verification System

The effectiveness of the proposed protection scheme for sequence based biometrics is applied in this Thesis to the protection of on-line signature templates. In Section 5.3.1 it is discussed how to extract a sequence based template $\mathcal{R}_F$ from an acquired signature, while the matching strategies employed to compare transformed templates obtained from different signatures, are described in Section 5.3.2.

5.3.1 Feature extraction stage

As already pointed out, the proposed non-invertible transform based approaches aim at securing finite sequences such as those acquired by touch screens or digitizing tablets when writing signatures on them.

During the employed feature extraction stage, the horizontal $x[n]$ and vertical $y[n]$ position trajectories, together with the pressure signal $p[n]$, are acquired from each on-line signature through a digitizing tablet. A geometric normalization, consisting of position normalization followed by rotation alignment, is applied to the pen-position sequences $x[n]$ and $y[n]$. Other four discrete time sequences are derived from the basic set, and used as an additional extended set of sequences, namely the path-tangent angle $\theta[n]$, the path velocity magnitude $v[n]$, the log curvature radius $\rho[n]$, and the total acceleration magnitude $a[n]$. Specifically, the set of sequences which are considered for the experiments described in Sections 5.5 and 5.6 is:

$$\mathcal{R}_{14} = \Big\{x[n], y[n], p[n], \theta[n], v[n], \rho[n], a[n], \dot{x}[n], \dot{y[n]}, \dot{p[n]}, \dot{\theta}[n], \dot{v}[n], \dot{\rho}[n], \dot{a}[n]\Big\} \qquad (5.13)$$

where the upper dot notation denotes the first order derivative. $F = 14$ sequences are therefore employed to represent the considered on-line signatures.

It is worth pointing out that, when generating the derivative sequences of the extended set as described in [121], it is not possible to derive any sequence of the basic set from the sequences of the extended one. Being then impossible to express any considered sequence by means of linear dependencies between other sequences, the security of the templates obtained by applying the non-invertible transform of Section 5.1.1 to each sequence does not depend on the relations between the sequences considered in the employed sets.

5.3.2 Signature Template Matching

In this Section, the matching strategies employed to compare transformed templates obtained from different signatures, are described. Specifically, three different approaches have been employed to compare the sequence based templates which are derived by transforming the original signature representations $\mathcal{R}_F$:

- a stochastic modelization based on HMMs is applied to the transformed signature templates. HMMs represent a tool for stochastic signal modeling which have been used in a wide range of pattern recognition applications, allowing to characterize signals in terms of parametric models. The HMMs represents a doubly embedded stochastic process, composed by an underlying Markov chain whose states are not observable, and by a set of stochastic processes which produce a sequence of available observations. Basically, it is assumed that, at a discrete time instant n, the Markov process is in one of its states, which generates an observation symbol according to a probability distribution associated with the current state. The model is defined "hidden" in the sense that the underlying state, which generates each symbol, cannot be deduced from simple symbol observation. The HMM represents one of the most employed approaches for matching templates extracted from on-line signatures, as described in [121]. The details of the employed matching strategy based on HMM is outlined in Section 5.3.2.1;

- an elastic string matching procedures such as Dynamic Time Warping (DTW) [139] is applied to the transformed signature templates. The use of the DTW based matching strategy for the comparison of signature templates, outlined in Section 5.3.2.2, is strongly suggested by the comparative studies performed during the Signature Verification Competition of 2004 (SVC 2004) [138]. The on-line signature recognition algorithm proposed in [139], employing DTW matching, gave the lowest average Equal Error Rate (EER) values, when tested with skilled forgeries. An on-line signature based recognition system employing DTW matching has also been discussed in [21]. The recognition rates achievable using a DTW based matching strategy are compared in Sections 5.5 and 5.6 with the performance achievable when employing a HMM based matching strategy, showing that better results can be achieved in both an unprotected and a protected on-line signature recognition system;

- in addition to experimental results obtained by applying HMM and DTW based matching strategies, in Sections 5.5 and 5.6 also the performances achievable by employing in conjunction both HMM and DTW will be presented. As already pointed out, one of the greatest advantage in using a non-invertible transform based approach for the protection of biometric templates consists in the possibility of representing the transformed templates in the same feature space of the original ones, and thus having the possibility of employing the same matchers designed for the original biometric templates. Such matchers, as it happens for example when considering HMM and DTW based matching strategies, commonly generate a score as the output of the matching process, differently from what happens when providing protection through biometric cryptosystem, as the one proposed in Chapter 4. Having the possibility of manage scores as the output of two or more matchers, *score fusion techniques* [104] can be employed to produce a single final score from the already computed ones. By combining information processed from different matchers, it is usually possible to achieve recognition performances that are even better than those achievable employed the considered matchers separately. The algorithms employed in order to fuse scores obtained from different matchers are outlined in Section 5.3.2.3. In Sections 5.5 and 5.6 it will then be outlined how the proposed non-invertible transform based approach, employed to provide protection to on-line signature templates, allows to obtain authentication performances far better than those achievable by implementing biometric cryptosystems for protection of signature templates.

5.3.2.1 Hidden Markov Models

An HMM is characterized by the following elements:

- the number H of hidden states $\{S_1, S_2, \ldots, S_H\}$ of the model. The state at discrete time n is indicated as q_n;

- the state transition probability $\mathbf{A} = \{a_{i,j}\}$, where $a_{i,j} = P[q_{n+1} = S_j | q_n = S_i),\ i, j = 1, \ldots, H$.

- the observation symbol probability distributions in each state j, indicated with $\mathbf{B} = \{b_j(\mathbf{o})\},\ j = 1, \ldots, H$. The observation processes are represented using mixtures of M multivariate Gaussian distributions: $b_j(\mathbf{o}) = \sum_{m=1}^{M} \zeta_{j,m} p_{\mu_{j,m}, \Sigma_{j,m}}(\mathbf{o})$, $j = 1, \ldots, H$, where $\mu_{j,m}$ and $\Sigma_{j,m}$ indicate respectively the mean and the diagonal covariance matrix of each Gaussian component. The coefficients $\zeta_{j,m}$ are selected respecting the condition of normalization $\sum_{m=1}^{M} \zeta_{j,m} = 1$, $j = 1, \ldots, H$.

- the initial state distribution $\boldsymbol{\pi} = \{\pi_j\} = \{p[q_1 = S_j]\}$, $j = 1, \ldots, H$

Following the proposed approach, during the enrollment phase the client model $\lambda = \{\boldsymbol{\pi}, \mathbf{A}, \mathbf{B}\}$ is estimated considering E transformed templates, obtained by processing the enrollment signatures of the subject at hand. Specifically, a matrix with F rows and K columns $\mathbf{O}^{(e)} = \{\mathbf{o}^{(e)}[1], \ldots, \mathbf{o}^{(e)}[K]\}$, $e = 1, \ldots, E$, is generated from the e-th acquired signature, taking as rows the transformed sequences belonging to the set $\mathcal{T}_F^{(e)}$. The observations correspond to the K columns $\{\mathbf{o}^{(e)}[n]\}$, $n = 1, \ldots, K$ of the matrix $\mathbf{O}^{(e)}$, which represent F-dimensional symbols. The HMM λ is then estimated according to the iterative strategy presented in [121].

The obtained model λ is stored in a database, and invoked during the authentication phase, when an user claims his identity on the basis of an input signature. This signature is converted to a matrix representation $\mathbf{O}$ whose rows represent the transformed signature sequences, and a similarity score is calculated as $(1/K) \log P(\mathbf{O}|\lambda)$ using the Viterbi algorithm [183]. A decision regarding whether the signature is authentic or a forgery is made by comparing the matching score to a threshold: if the computed score is higher than

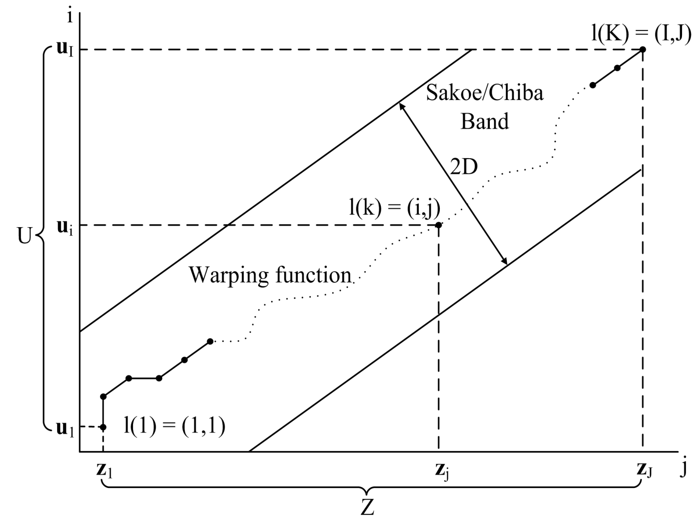


Figure 5.2: Warping function and Sakoe/Chiba band definition (adapted from [184])

.

the employed threshold, the acquired signature is considered as belonging to the claimed identity.

It is worth pointing out that when using HMMs for signature recognition, also in an unprotected approach, the client model $\lambda = \{\boldsymbol{\pi}, \mathbf{A}, \mathbf{B}\}$, instead of the original signature sequences, is stored in the database. However, if an attacker is able to acquire the client HMM, the statistical properties of the client's signatures can be derived from the model. Using the proposed protection approach, if an attacker succeeds in acquiring the stored models, he can only retrieve information about the set of transformed sequences $\mathcal{T}_F$, from which it is not possible to get any information about the original sequences $r_{(i)}[n]$, $i = 1, \ldots, F$, as discussed in Section 5.2.

5.3.2.2 Dynamic Time Warping

Following the approaches outlined in Section 5.1, a set $\mathcal{T}_F$ of F transformed sequences can be obtained from the original signature representation $\mathcal{R}_F$. Dynamic Time Warping (DTW) [139] is a well known method to compare sequences of different lengths, and it is here employed to compare different signature instances, by applying it to their transformed templates.

The DTW algorithm finds an alignment between the points in the two sequences, such that the sum of the differences between each pair of aligned points is minimal. Formally, having indicated with $U = \{\mathbf{u}_i\}$, $i = 1, \ldots, I$, and $Z = \{\mathbf{z}_j\}$, $j = 1, \ldots, J$, two sequences of feature vectors, representing respectively the biometric template employed as reference and the biometric sample to be verified, a point-to-point distance $\delta(i, j)$ between the elements $\mathbf{u}_i$ and $\mathbf{z}_j$ can be evaluated, for $i = 1, \ldots, I$ and $j = 1, \ldots, J$. Typically, $\delta(i, j)$ is computed as the Euclidean distance between the vectors $\mathbf{u}_i$ and $\mathbf{z}_j$. With reference to Figure 5.2, where the patterns U and Z are developed along in an $i - j$ plane, the DTW algorithms finds the optimal warping function $L = \{l(k)\} = \{(i(k), j(k))\}$, $k = 1, \ldots, K$, which connects the points $l(1) = (1, 1)$ and $l(K) = (I, J)$, minimizing the total distance

$$\Delta_L(U, Z) = \sum_{k=1}^{K} \delta(l(k)) = \sum_{k=1}^{K} \delta(i(k), j(k)) \tag{5.14}$$

The minimum accumulated distance $\min_{L \in \mathcal{L}}\{\Delta_L(U, Z)\}$, where $\mathcal{L}$ represents the set of all properly defined distortion paths L for U and Z, is employed to characterize the dissimilarity of the considered sequences. The paths in $\mathcal{L}$ have to satisfy the necessary monotonic and continuity requirements [184]. Moreover, only the paths which remains in the so-called Sakoe/Chiba band [184], depicted in Figure 5.2, are taken into account.

The band is defined by considering those indexes (i, j) whose distance from the diagonal which connect the point $(1, 1)$ to the point (I, J) is less than a fixed value D. More formally, each element w_k of a warping path W in $\mathcal{W}$ should respect the adjustment window condition:

$$\sqrt{i^2 + j^2} \cdot \sin(|\arctan(J/I) - \arctan(j/i)|) < D. \tag{5.15}$$

In the following, the width D of the Sakoe/Chiba band will be expressed as percentage of the minimum value $min(I, J)$ between the test and reference signature lengths. No additional slope constraint has been considered in our implementation. In order to compensate the effect of the summation of K terms in equation (5.14), a normalization has to be done on the minimum accumulated distance. When normalizing with respect to the sum of the sequence lengths $(I + J)$, a symmetric distance $\Delta_S(U, Z) = \min_{L \in \mathcal{L}}\{\Delta_L(U, Z)\}/(I + J)$ is defined. Otherwise, asymmetric distances can be defined when normalizing with respect to the length of the reference sequence U ($\Delta_R(U, Z) = \min_{L \in \mathcal{L}}\{\Delta_L(U, Z)\}/I$), or with respect to the length of the test sequence Z ($\Delta_T(U, Z) = \min_{L \in \mathcal{L}}\{\Delta_L(U, Z)\}/J$).

When employing the DTW based matching strategy in the proposed system, E signatures are acquired from each user during enrollment. From each signature, the original representation $\mathcal{R}_F^e$ is evaluated, and then the protected templates $\mathcal{T}_F^e$, $e = 1, \ldots, E$, are computed and stored in a database. During authentication, the user claims his identity providing a test signature, which is processed to generate its transformed template $\mathcal{T}_F^a$. This test sample is then compared to all the E templates in the reference set by employing the DTW algorithm. The considered output, for each comparison, is the distance $\Delta_R(\mathcal{T}_F^e, \mathcal{T}_F^a)$ between the test sample $\mathcal{T}_F^a$ and the reference sample $\mathcal{T}_F^e$. The distance normalized with respect of the reference sample is therefore taken. Eventually, the minimum of the E distances between the test sample $\mathcal{T}_F^a$ and the E reference samples $\mathcal{T}_F^e$, $e = 1, \ldots, E$, is taken as representative of the verification process. As it has been noticed in [58], and verified in the performed experiments, better recognition rates are achieved when considering the minimum value, with respect to consider the maximum or the average ones. A decision regarding whether the signature is authentic or a forgery is made by comparing the result of the matching to a threshold: if the computed distance is lower than the employed threshold, the acquired signature is considered as belonging to the claimed identity.

It is worth pointing out that, differently from what is done when using HMMs, when DTW is employed as matcher in an unprotected signature based recognition system, the stored templates permit to perfectly reconstruct both the shape and the dynamics of the signatures. This important privacy and security issue [185] then gives an also greater relevance to the proposed on-line signature template protection approach.

5.3.2.3 Combination of HMM and DTW based strategies: score fusion techniques

As already outlined, score fusion techniques can be applied in the proposed protected system, thanks to the fact that, in the employed transformed domain, it is possible to use template matchers which output a score as result of a template comparison. The aim of score fusion is to improve the authentication performances, with respect of systems employing a single matcher. The fusion of scores obtained from two or more matchers typically consists of two steps:

1. a *normalization* process, which is responsible of taking into account that the match scores generated by the individual matchers may not be homogeneous. For example, as it happens in the proposed application, one matcher may output a distance or a dissimilarity measure, where smaller distances indicates a better similarity, while the other matcher may output a similarity score, where a larger score value implies a better match between the considered templates. Furthermore, the outputs of the individual matchers may be in different numerical ranges, or may follow different distributions. All these possibilities have to be considered when defining the employed normalization technique.

2. the application of a *fusion rule*, which consists of combining the available normalized scores, according to a selected classifier rule.

As for the normalization process, *fixed score normalization* [186], which is based on the estimation of some parameters during a training phase, is employed throughout this Thesis. Following this approach, it is assumed that a set of match scores is available during the training phase of the fusion module. Analyzing these scores, a suitable statistical model, which has to fit the available data, is determined. The score normalization parameters are determined on the basis of the estimated model, and employed when performing the authentication tests, to fuse the obtained match scores.

Specifically, as already outlined for the considered scenario, the similarity scores obtained as output of the HMM based matcher have to be combined with the dissimilarity measures obtained from the DTW based classifier. The similarity scores, according to what illustrated in Section 5.3.2.1, are given by the logarithm of a probability, and are therefore negative values comprised in the range $[-\infty, 0]$. Differently, the distances which are computed by the DTW algorithm lie between 0 and ∞. In order to represent over the same range the outputs of the considered matchers, it is then necessary to change the sign of the outputs of one of the two classifiers. Specifically, in the proposed implementation the sign of the scores generated by the HMM matchers are changed. Once this is done, the following techniques can be employed to normalize the available scores: the *min-max*, the *z-score*, the *median*, the *double sigmoid*, or the *tanh-estimators* [104] normalization technique. These methods are described in detail in the following, where it is assumed that a set of training match scores is available, and having indicated with s_j^i the i-th match score produced by the j-th classifier.

- *min-max* score normalization: the min-max normalization approach maps the original scores into a common range $[0, 1]$. The method employed in this Thesis is a generalized version of the one proposed in [104], defined in order to be robust with respect of possible outliers. Specifically, considering a score s_j^i obtained as the result of an authentication process applied to the i-th query, when employing the j-th matcher, the normalized score ns_j^i is computed as:

$$ns_j^i = \frac{s_j^i - t_j}{T_j - t_j}, \tag{5.16}$$

where $t_j = g_j(1 - \alpha)$ and $T_j = G_j(1 + \alpha)$, being g_j and G_j respectively the minimum and maximum score available in the available training set, for the j-th classifier. More in detail, in order to be robust with respect of outliers, only a selection of the scores available in the training set is employed to estimate G_j: the β highest scores are discarded from the training set (typical values of β can be in the range $[0, 0.05]$, having expressed β as percentage of the total number of available scores). It is worth pointing out that, due to the fact that the considered scores are only positive (the signs of the similarity scores produced by the HMM classifiers are changed), only the highest scores can be related to outliers, and are therefore discarded. The estimated values of g_j and G_j are multiplied by $(1 - \alpha)$ and $(1 + \alpha)$, respectively, in order to consider a wider range for the possible scores: in fact, g_j and G_j are estimated over a training set, whose cardinality may not be large enough to significantly represent the score distribution of the j-th matcher. Typical values of α are in the range $[0, 0.2]$. The standard min-max normalization technique [104] is obtained when setting $\alpha = \beta = 0$;

- *z-score* score normalization: the z-score method uses the arithmetic mean μ_j and standard deviation σ_j of the training scores for normalization. When employing this approach for score fusion, the normalized scores of the j-th matcher are computed as

$$ns_j^i = \frac{s_j^i - \mu_j}{\sigma_j}. \tag{5.17}$$

As already done for the min-max approach, the arithmetic mean μ_j of the scores produced by the j-th matcher, as well as their standard deviation σ_j, is computed by limiting the highest possible score of the j-th matcher to the maximum score obtained when discarding the β highest scores in the training set, in order to not take into account possible outliers in the available training data. The standard z-score normalization technique [104] is obtained when setting $\beta = 0$;

- *median* score normalization: this approach is insensitive to outliers, and compute the normalized scores of the j-th matcher as:

$$ns_j^i = \frac{s_j^i - q_j}{Q_j}, \tag{5.18}$$

being q_j the median value of the available training scores, and Q_j their median absolute deviation (MAD), defined as $Q_j = median(|s_j^i - q_j|)$.

- *double sigmoid* score normalization: this approach has been proposed in [187], and produces normalized scores given by:

$$ns_j^i = \begin{cases} \dfrac{1}{1 + exp\big(-2\frac{s_j^i - \tau_j}{\varsigma_j^1}\big)} & if \ s_j^i < \tau_j \\ \dfrac{1}{1 + exp\big(-2\frac{s_j^i - \tau_j}{\varsigma_j^2}\big)} & \text{otherwise,} \end{cases} \tag{5.19}$$

where τ_j is the reference operating point, while ς_j^1 and ζ_j^2 denote the left and right edges of the region in which the function is linear. Generally, τ_j is chosen to be some values falling in the region of overlap between the available genuine and impostor score distributions, computed over the training set, while ς_j^1 and ς_j^2 are set in order to correspond to the extremes of the overlapping region between the two distributions. Specifically, in the employed implementations, τ_j is selected as $\chi_j(1 + \alpha)$, where χ_j represents the score corresponding to an equal value for the cumulative histogram distributions of genuine and impostor scores, and α a system parameter. Employed values of α fall in the range $[-0.2, 0.2]$. Moreover, also the values of ς_j^1 and ς_j^2 are selected employing the cumulative histogram distribution of genuine and impostor scores: ς_j^1 is selected as the score corresponding to the β percentile of the genuine distribution, while ς_j^2 is selected as the score corresponding to the $1-\beta$ percentile of the impostor distribution. It is reminded that the percentile is the value of a variable below which a certain percent of observations falls. Employed values of β are in the range $[0.01, 0.1]$;

- *tanh-estimators* score normalization: this approach has been defined in [188], and gives normalized scores obtained as:

$$ns_j^i = \frac{1}{2}\Big\{tanh\big[0.01\big(\frac{s_j^i - \mu_{GH}}{\sigma_{GH}}\big)\big] + 1\Big\}, \tag{5.20}$$

  where μ_{GH} and σ_{GH} are the mean and standard deviation estimates, respectively, of the available training score distributions, computed considering the Hampel estimators [104]. Being the considered scores only positive, the Hampel estimators is simplified and implemented, in the employed system, by setting the maximum allowable score as the highest value obtained when discarding the β highest available scores.

The fusion rule employed throughout this Thesis is the *sum rule*, which is the approach most commonly used when implementing multi-biometrics systems. As reported in [104], the sum rule is more effective than the *product rule* when the inputs tend to be noisy, thus leading to errors in the estimation of the *a posteriori* scores probability distribution. The sum rule is also known as the *mean* or *average decision rule*, because it is equivalent to assign the considered input to the class which has the maximum average a posteriori probability, over all the available matchers.

5.4 Experimental Setup

In order to evaluate the performance of the protected system, and in order to test the renewability capabilities of the proposed approaches, when applied to on-line signature verification, an extensive set of experimental results is performed using the public MCYT on-line signature corpus, which contains signatures taken from 100 users. As already outlined in Chapter 1, the employed database has been split in a training data set, comprising the first 30 users, and a test data set, comprising the remaining 70 users. The experimental results reported in the following, regarding both the authentication and the renewability performances, have been computed over the test data set with 30 users. The training data set is employed to estimate the parameters needed for the fusion of scores obtained from HMM and DTW base classifiers, according to the procedures described in Section 5.3.2.3.

In order to properly analyze the proposed non-invertible transform based template protection schemes, the following aspects are investigated:

- Performance
  - performance dependence on HMM and DTW parameters, for both unprotected and protected systems;
  - performance comparison between approaches employing HMM, DTW and fusion based classifiers, for both unprotected and protected systems;
  - performance variability with respect of the transformation defining parameters, for protected systems;
  - performance comparison between the baseline approach described in Section 5.1.1, and the extended methods described in Section 5.1.2;
- Renewability
  - evaluation of the *diversity* between two templates originated by applying two different transformations on the original data. The analysis is conducted for the baseline approach described in Section 5.1.1, as well as for the extended methods of Section 5.1.2.

The performance analysis is detailed in Section 5.5, while the renewability capabilities of the proposed protection methods is presented in Section 5.6. Both the aspects have been analyzed by employing the three matching procedures described in Section 5.3.2.

5.5 Authentication Performance Analysis

The authentication performances achievable with the proposed protected on-line signature protection methods are here discussed. The system performances are evaluated through the FRR, the FAR for skilled forgeries (FAR$_{SF}$), the FAR for random forgeries (FAR$_{RF}$), and the Equal Error Rates (EERs). These figures of merit are obtained considering, for each user in the enrollment stage, $E = 5$ signatures taken from the first acquisition set of MCYT, or $E = 10$ signatures taken from the first two acquisition sets of MCYT. The FRR is estimated on the basis of the signatures belonging to the third, fourth and fifth available acquisition sets. The FAR_{SF} is computed using the 25 skilled forgeries available for each user. The FAR_{RF} is computed taking, for each user, one signature from each of the remaining users.

5.5.1 Dependency on the HMM, DTW and Score Normalization Parameters

Within the described experimental setup, the dependency of the authentication performances on the system parameters, which are employed to define the HMM modeling and the DTW algorithm, is first discussed. Specifically, the EERs obtained by varying the HMM parameters H and M, considering skilled forgeries, are summarized in Table 5.1, for both an unprotected approach employing HMMs as matchers, and the protected baseline approach described in Section 5.1.1 with $W = \{2, 3, 4\}$. The values of$H$ reported in Table 5.1 are $H \in \{8, 16\}$, because the best recognition rates are achieved employing, for the HMM modelization, a number of states comprised between 8 and 16, as observed in [121] and [111]. When considering the proposed protected baseline approach, the key vector $\mathbf{d}$ is randomly selected for each considered user, taking the values d_j, $j = 1, \dots, W - 1$, in the range of integers $[5, 95]$. As described in [107], this reflects how the protected system should be used in a practical implementation, where different transformations have to be used for different individuals.

The same analysis is conducted for a system employing a DTW based matching strategy, where the only parameter which has to be set is the width D of the Sakoe/Chiba band, as detailed in Section 5.3.2.2. The EERs obtained when considering skilled forgeries are shown in Table 5.2.

In both Table 5.2 and 5.2, the best EER achievable for each configuration (unprotected and protected systems, for each value of E and W)) are highlighted, and are employed to select the best HMM and DTW configurations, which are considered in the following to illus-

E	H	M	Unprotected	Baseline Protected Approach		
			Approach	$W = 2$	$W = 3$	$W = 4$
5	8	1	27.43	10.13	**14.09**	**17.43**
		2	10.96	**8.68**	14.48	17.82
		4	9.14	8.96	14.91	18.22
		8	10.29	10.21	15.37	19.69
		16	10.57	12.57	19.58	21.45
		32	16.78	28.29	30.45	32.13
	16	1	9.82	9.25	14.51	17.60
		2	9.82	9.71	15.78	18.11
		4	**8.86**	10.42	16.34	19.46
		8	10.31	12.10	20.54	23.27
		16	11.43	26.31	30.70	32.22
		32	18.89	26.06	27.85	29.11
10	8	1	10.34	8.13	11.36	13.73
		2	7.43	6.39	10.50	**12.40**
		4	5.64	5.53	**10.03**	12.59
		8	4.78	**5.35**	10.50	12.98
		16	5.28	5.64	10.09	14.87
		32	7.07	6.78	16.48	18.14
	16	1	6.00	6.39	14.15	14.98
		2	4.29	5.64	12.21	12.51
		4	**3.88**	5.53	13.15	13.65
		8	3.92	5.71	15.65	16.59
		16	5.53	7.53	17.84	20.16
		32	9.47	17.71	19.90	22.16

Table 5.1: EERs$_{SF}$ (expressed in %) for different HMM configurations considering skilled forgeries, in unprotected and protected systems, taking $E = 5$ or $E = 10$ signatures during enrollment.

trate the performances of the proposed approaches. Specifically, the selected configurations are:

- unprotected approach
  - employing HMM, with $E = 5$: $H = 16$, $M = 4$ ($\text{EER}_SF = 8.86\%$);

E	D (in %)	Unprotected	Protected Approach (Baseline)		
		Approach	$W = 2$	$W = 3$	$W = 4$
5	1	7.85	8.21	9.53	12.78
	5	5.14	**6.96**	**8.13**	**10.86**
	10	**3.92**	7.43	8.39	11.07
	15	3.95	7.43	8.39	11.07
10	1	6.00	6.03	7.92	10.10
	5	3.64	**4.99**	**6.78**	**8.21**
	10	**3.17**	5.14	7.31	9.14
	15	3.20	5.14	7.31	9.14

Table 5.2: EERs$_{SF}$ (expressed in %) for different DTW algorithms considering skilled forgeries, in unprotected and protected systems, taking $E = 5$ or $E = 10$ signatures during enrollment.

  - employing DTW, with $E = 5$: $D = 10\%$ (EER$_SF$ = 3.92%);
  - employing HMM, with $E = 10$: $H = 16$, $M = 4$ (EER$_SF$ = 3.88%);
  - employing DTW, with $E = 10$: $D = 10\%$ (EER$_SF$ = 3.17%);

- baseline protected approach, with $W = 2$
  - employing HMM, with $E = 5$: $H = 8$, $M = 2$ (EER$_SF$ = 8.68%);
  - employing DTW, with $E = 5$: $D = 5\%$ (EER$_SF$ = 6.96%);
  - employing HMM, with $E = 10$: $H = 8$, $M = 8$ (EER$_SF$ = 5.35%);
  - employing DTW, with $E = 10$: $D = 5\%$ (EER$_SF$ = 4.99%);

- baseline protected approach, with $W = 4$
  - employing HMM, with $E = 5$: $H = 8$, $M = 1$ (EER$_SF$ = 14.48%);
  - employing DTW, with $E = 5$: $D = 5\%$ (EER$_SF$ = 8.13%);
  - employing HMM, with $E = 10$: $H = 8$, $M = 4$ (EER$_SF$ = 10.03%);
  - employing DTW, with $E = 10$: $D = 5\%$ (EER$_SF$ = 6.78%);

- baseline protected approach, with $W = 3$

  - employing HMM, with $E = 5$: $H = 8$, $M = 1$ ($\text{EER}_S F = 17.43\%$);
  - employing DTW, with $E = 5$: $D = 5\%$ ($\text{EER}_S F = 10.86\%$);
  - employing HMM, with $E = 10$: $H = 8$, $M = 2$ ($\text{EER}_S F = 12.40\%$);
  - employing DTW, with $E = 10$: $D = 5\%$ ($\text{EER}_S F = 8.21\%$);

As can be seen, a system using the employed DTW matching strategy performs better than a system using the employed HMM modeling. Moreover, it can be noticed that the difference in performance between the two classifiers becomes more evident when decreasing the number E of enrolled signatures: using DTW, low EERs are achieved even with $E = 5$ signatures considered during enrollment, for both unprotected and protected systems. The EERs obtained when employing HMM, for system with $E = 5$ signatures taken during enrollment, are significatively worse than those achieved with a DTW based classifier.

From the reported results, it can be also noticed that employing both the proposed classifiers, the performances obtained with a protected system with $W = 2$ are only slightly worse than those obtained with an unprotected system. Therefore, employing the proposed baseline approach of Section 5.1.1, it is possible to obtain recognition performances comparable with those of an unprotected system, while providing the desired protection for the employed signature templates.

The performance improvement which can be achieved when employing the fusion strategies described in Section 5.3.2.3 is then analyzed. Specifically, as described in Section 5.3.2.3, the employed fusion techniques performs score normalization according to a set of values estimated over a training data set. However, in order to perform such estimates, some parameters have to be set for each normalization method (for example, the parameters α and β for the double sigmoid normalization approach). In order to verify the dependency of the achievable performances on the parameters of the considered score normalization approaches, the results reported in Table 5.3 correspond to:

- the best EERs_{SF}, selected among the results obtained by varying the parameters of the considered score normalization techniques;
- the EERs_{SF} which are obtained when performing score normalization according to given fixed parameters. Specifically, the employed parameters are:

- for the min-max normalization approach: $\alpha = 0$, $\beta = 0$. This parameter selection corresponds to the implementation of the classic min-max normalization procedure, as described in [104];
- for the z-score normalization approach: $\beta = 0$. This parameter selection corresponds to the implementation of the classic z-score normalization procedure, as described in [104];
- for the sigmoid normalization approach: $\alpha = 0$, $\beta = 0.96$. Selecting $\alpha = 0$, the reference operating point τ_j in equation (5.19) is selected as the score corresponding to an equal value for the genuine and impostor cumulative histogram distributions. Selecting $\beta = 0.96$, it is supposed that the portions of genuine and impostor score distributions, which fall out of the domain in which the double sigmoid function in equation (5.19) exhibits a linear behavior, are limited to a 4% of the total;
- for the tanh-estimator normalization approach: $\beta = 0$; This parameter selection corresponds to the implementation of a tanh-estimator normalization procedure without the application of the Hampel estimators [104]. Basically, no outsider is considered to be in the available distributions;

The median normalization approach does not require the definition of any parameter for its application;

As indicated in Section 5.3.2.3, the sum rule is always employed to combine the normalized scores.

As can be seen from the results in Table 5.3, different normalization approaches produce similar values of EER$_{SF}$, which remains in the range $[3.1\%; 3.8\%]$ for an unprotected approach, and in the range $[4.1\%; 5.5\%]$ for a protected approach with $W = 2$, when considering $E = 5$ signatures for the enrollment. When $E = 10$ signatures are taken into account during enrollment, the achievable EERs$_{SF}$ are in the range $[2.3\%; 2.6\%]$ for an unprotected system, and in the range $[3.1\%; 4\%]$ employing the protected baseline approach with $W = 2$. It is worth pointing out that, with the exception of the min-max normalization, the other normalization techniques are only minimally affected by the selection of

E	Normalization	Unprotected Approach		Baseline Protected Approach, $W = 2$	
	Technique	Best EER_{SF}	EER_{SF} (given parameters)	Best EER_{SF}	EER_{SF} (given parameters)
5	min-max	**3.12**	4.09	**4.14**	5.48
	z-score	3.80	3.80	5.41	5.52
	median	-	4.27	-	5.52
	sigmoid	3.60	**3.60**	5.01	**5.23**
	tanh	3.80	3.80	5.41	5.52
10	min-max	**2.31**	2.66	**3.13**	**3.91**
	z-score	2.66	2.66	3.87	3.91
	median	-	2.66	-	3.91
	sigmoid	2.38	**2.48**	4.05	4.09
	tanh	2.66	2.66	3.87	3.91

Table 5.3: EERs_{SF} (expressed in %) for different fusion strategies considering skilled forgeries, in unprotected and protected systems, taking $E = 5$ or $E = 10$ signatures during enrollment.

their defining parameters. This result can be dependent on the fact that, especially when considering $E = 10$, the distributions of scores obtained from the HMM and DTW matchers do not present a significative amount of outliers.

In order to illustrate in a summarizing and clarifying way the obtained results, Figure 5.3 and 5.4 show the Receiver Operating Characteristic (ROC) curves which are obtained when considering unprotected systems, as well as systems employing the baseline protected approach described in Section 5.1.1, respectively for $E = 5$ and $E = 10$. The performances achievable employing HMM, DTW, and the fusion of both HMM and DTW for the comparison of different templates, are shown. Specifically, a min-max normalization approach with $\alpha = \beta = 0$ is employed to combine the scores when $E = 10$ signatures are considered during enrollment, whereas a sigmoid normalization with $\alpha = 0$ and $\beta = 0.96$ is selected to combine HMM and DTW scores when $E = 5$. These choices are kept also in the following of the Chapter.

As already noticed, the difference between the performances obtained with HMM or DTW classifiers is more relevant when $E = 5$: in this case, a protected system employing HMMs can reach recognition performances which are identical to those of an unprotected system. Moreover, for the baseline protected approach, from the sketched ROC curves

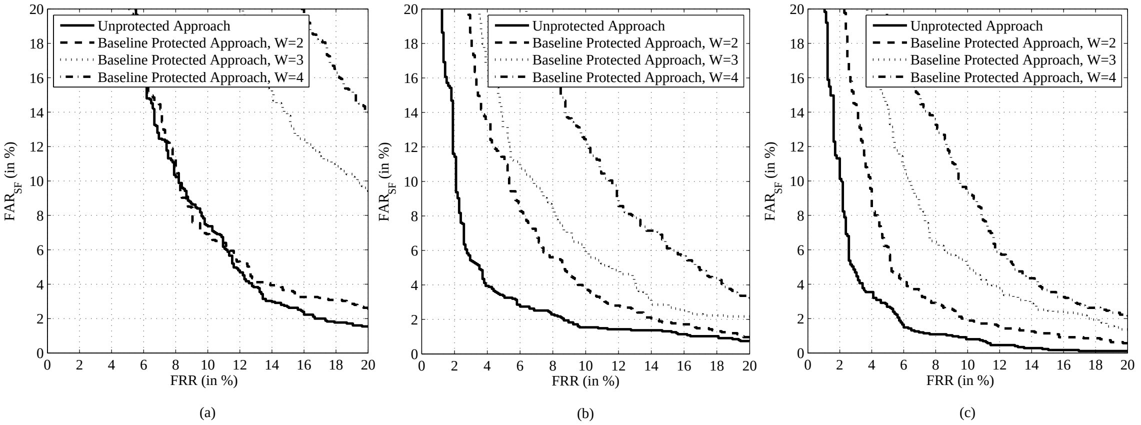


Figure 5.3: ROC curves for an unprotected system, and for protected systems with $W = 2, 3, 4$ convolved segments, considering skilled forgeries and $E = 5$ signatures during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

it can be seen that the recognition performances worsen when the system parameter W, that indicates the number of segments in which the signature sequences are divided, increases. This loss in performance can be explained as follows. The division in segments of the considered signature time sequences is accomplished using a set of fixed parameters d_j, $j = 1, \ldots, W-1$. They express, in terms of the percentage of the total sequence length, the points where the splits have to be done. However, due to the characteristics of signature biometrics, sequences extracted from different signatures, also if from the same user, typically have different lengths. Therefore, in order to align two signature sequences, a dynamic programming strategy is typically needed, whereas a simple linear correspondence strategy does not represent the best signatures alignment approach. As a consequence, the more separations are performed, the more variable will be the convolutions at the output. The best authentication results are obtained when $W = 2$, due to the fact that only one separation point has to be set in this case. However, when performing the fusion between scores obtained from HMM and DTW, the performances achievable even when decomposing the original sequences into $W = 4$ segments remain acceptable, producing an EER for skilled forgeries lower than 10% when taking $E = 5$ signatures for the enrollment, and lower than 8% when $E = 10$.

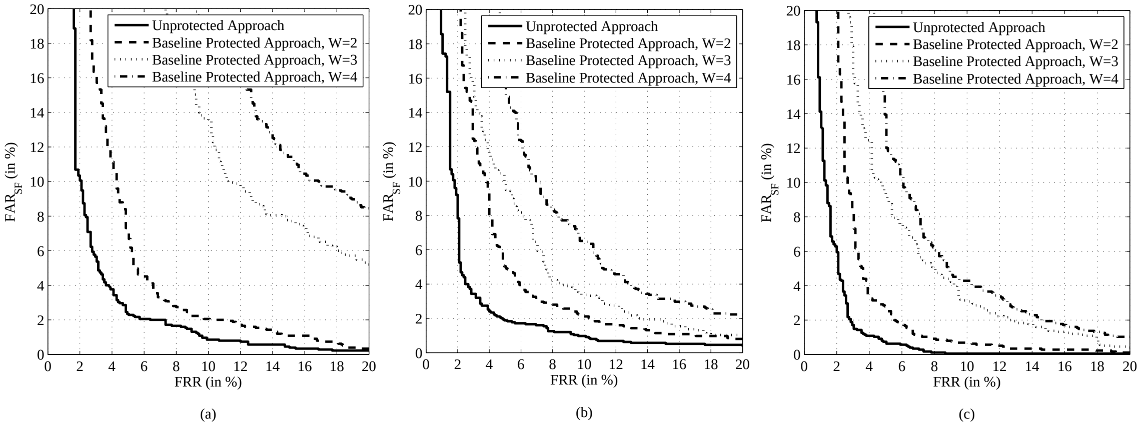
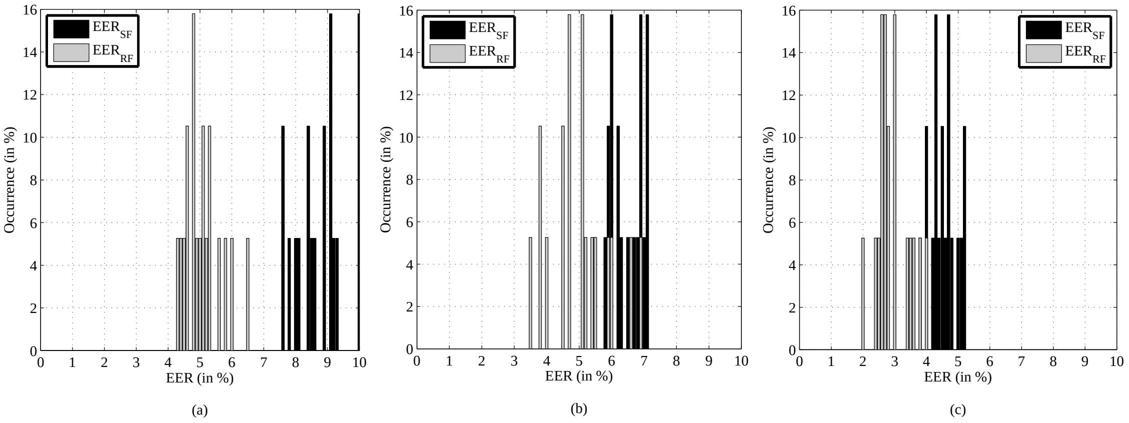


Figure 5.4: ROC curves for an unprotected system, and for protected systems with $W = 2, 3, 4$ convolved segments, considering skilled forgeries and $E = 10$ signatures during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

5.5.2 Dependency on the decomposition key vector $\boldsymbol{d}$

Considering the baseline protected approach proposed in Section 5.1.1, the dependence of the authentication performance on the key $\mathbf{d}$ is then investigated. More in detail, a protected system where the signature sequences are split into $W = 2$ segments, by means of the key $\mathbf{d}$ is considered. The performance evaluation is made performing 20 times the enrollment and authentication processes over the available test data set, varying at each iteration the transformation parameters $\mathbf{d}$ for each user. In Figure 5.5 the obtained results are shown, through the normalized histograms of the EERs for both random (EER_{RF}) and skilled forgeries (EER_{SF}), obtained when considering a protected system with $E = 5$ signatures taken from each user during enrollment. The mean and standard deviation of the obtained EERs are:

- HMM matching
  - skilled forgeries: mean $\mathrm{EER}_{SF} = 8.81\%$, with a standard deviation $\sigma_{EER_{SF}} = 0.8\%$;
  - random forgeries: mean $\mathrm{EER}_{RF} = 5.06\%$, with a standard deviation $\sigma_{EER_{RF}} = 0.6\%$.
- DTW matching



(a) (b) (c)

Figure 5.5: Normalized histograms of the EERs obtained repeating 20 times the authentication process, for a protected system with $W = 2$. $E = 5$ signatures are taken from each user during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

  - skilled forgeries: mean EER$_{SF}$ = 6.5%, with a standard deviation $\sigma_{EER_{SF}}$ = 0.46%;
  - random forgeries: mean EER$_{RF}$ = 4.94%, with a standard deviation $\sigma_{EER_{RF}}$ = 0.9%.

- Fusion of HMM and DTW matching

  - skilled forgeries: mean EER$_{SF}$ = 4.45%, with a standard deviation $\sigma_{EER_{SF}}$ = 0.4%;
  - random forgeries: mean EER$_{RF}$ = 2.93%, with a standard deviation $\sigma_{EER_{RF}}$ = 0.5%.

As requested for a properly designed non-invertible transform based method, the variations in the employed transformation parameters do not result in significant modifications of the matching performances. Moreover, it is worth pointing out that, in addition to an improvement in the achievable recognition performances, the fusion between HMM and DTW scores guarantees also a reduction of the performance variability.

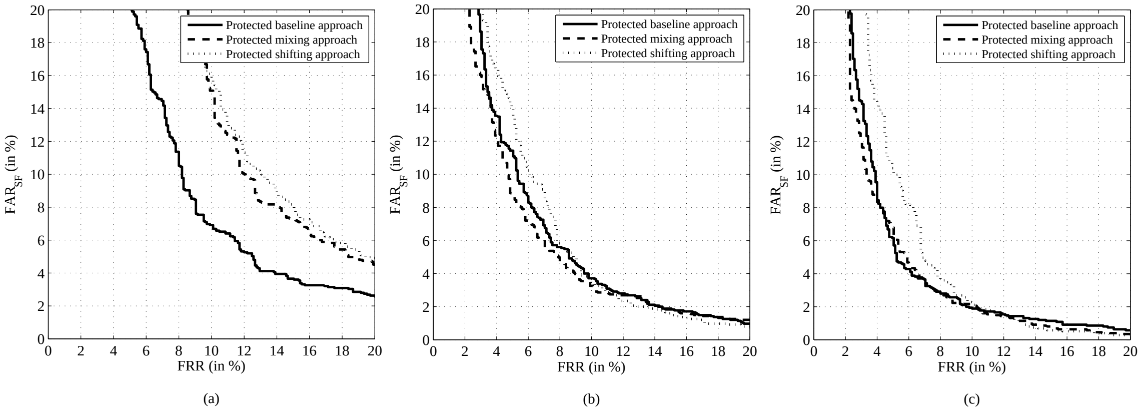


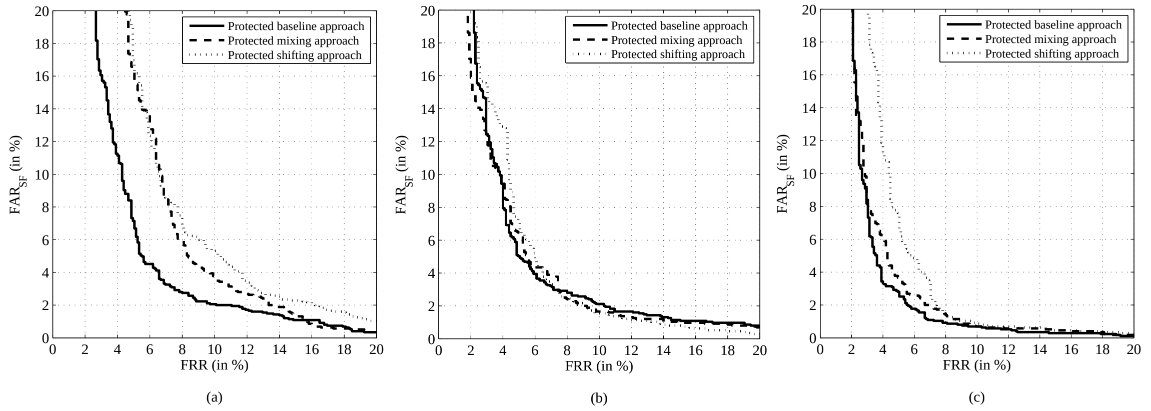
Figure 5.6: Performance comparison between the baseline protected method of Section 5.1.1, and the extended protected approaches described in Section 5.1.2, considering $E = 5$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

5.5.3 Comparison between Baseline and Extended Approaches

The proposed approaches for the protection of signature templates are also discussed by comparing the authentication performances achievable employing the extended transforms described in Section 5.1.2, with those obtained using the baseline method described in Section 5.1.1. Specifically, only the case where each sequence is split into $W = 2$ segments is considered.

In Figure 5.6 the performances obtained considering the approaches described in Section 5.1.2.1 and 5.1.2.2 respectively, when taking $E = 5$ signatures from each user during enrollment, are presented, and compared with those related to the use of the baseline protected approach. Figure 5.7 illustrates the same comparisons, referred to the case when $E = 10$ signatures are taken from each user during enrollment. For all the considered protected approaches, the aforementioned HMM and DTW configurations which give the best authentication performances for the baseline method, as well as the aforementioned selected fusion strategies, are taken into account when performing the simulations whose results are given in Figure 5.6 and Figure 5.7.

As can be seen from the reported verification results, systems using the protection methods described in Section 5.1.2 are characterized approximately by the same performances of a system using the baseline protection. Specifically, a slight difference in performance



(a)

(b)

(c)

Figure 5.7: Performance comparison between the baseline protected method of Section 5.1.1, and the extended protected approaches described in Section 5.1.2, considering $E = 10$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

can be observed when using HMMs as classifiers. However, such difference decreases when employing DTW, while the use of score fusion techniques further improve the performances of the proposed protected systems: the differences between the performances obtained employing the baseline approach, and those obtained with the approaches described in Section 5.1.2, is further reduced when combining HMM and DTW scores, with respect to the use of only one of the two proposed classifiers. Between the two extended approaches described in Section 5.1.2, the mixing approach performs slightly better than the shifting based one.

5.6 Renewability Analysis

The transformations introduced in Sections 5.1.1 and 5.1.2 are then analyzed with respect of the *diversity* property, which is a crucial requirement to implement cancelable biometrics. Specifically, it can be noticed that each of the proposed transformation approach is defined by means of a key or a set of keys, and that different transformations can be obtained by varying the employed keys. Moreover, two transformed templates, generated from the same original data, are as more different as more distant the respective transformation keys are. Being the space of possible keys finite, the number of possible instances which can be generated from the same data, and which are enough distant from each other to properly respect the diversity requirement, is necessarily limited.

The capability of the baseline approach described in Section 5.1.1 in generating multiple templates from the same original data is discussed in Section 5.6.1. Then, the renewability of the approaches introduced in Section 5.1.2 is analyzed in Sections 5.6.2 and 5.6.3.

5.6.1 Baseline Approach

Considering the baseline approach of Section 5.1.1, the key of the employed transformation is represented by the vector $\mathbf{d}$, which specifies how to decompose the originally acquired sequences into W parts, before performing the proposed transformation given by equation (5.3). In the considered experiments, for the sake of simplicity, the values which each element d_j, $j = 1, \ldots, W-1$, of a key vector $\mathbf{d}$, can assume, are restricted to the range $[5, 95]$, and taken at a distance of 5 to guarantee a minimum distance among the different signal decomposition lengths. With these constraints, the total number of allowed vectors $\mathbf{d}$ is limited to $N_D = (95-5)/5+1 = 19$, when $W = 2$ is chosen, and to $N_D = (19\times18)/2 = 171$ when $W = 3$. However, in order to be compliant with the diversity property, the actual number of transformations which can be used in different systems has to be further reduced.

In order to support this analysis with experimentations, a distance measure Ψ between two key vectors, namely $\mathbf{d}^{(1)}$ and $\mathbf{d}^{(2)}$, is introduced as follows:

$$\Psi(\mathbf{d}^{(1)}, \mathbf{d}^{(2)}) = \sum_{i=1}^{W-1} |d_i^{(1)} - d_i^{(2)}|. \tag{5.21}$$

Considering the available test data set, each user is enrolled taking into account his first E signatures, to which the baseline transformation process of Section 5.1.1 with $W = 2$ is applied. Specifically, the transformations employed during enrollment are ruled by a key vector $\mathbf{d}^{(e)}$.

The remaining signatures of each user are employed to estimate the FRR, after being transformed according to the same key vectors $\mathbf{d}^{(e)}$ employed during enrollment. Several matching statistics related to FAR are then computed, considering:

- the skilled forgeries available in the test data set, transformed according to key vectors $\mathbf{d}^{(a)}$ which are the same of those employed during enrollment ($\Psi(\mathbf{d}^{(e)}, \mathbf{d}^{(a)}) = 0$);

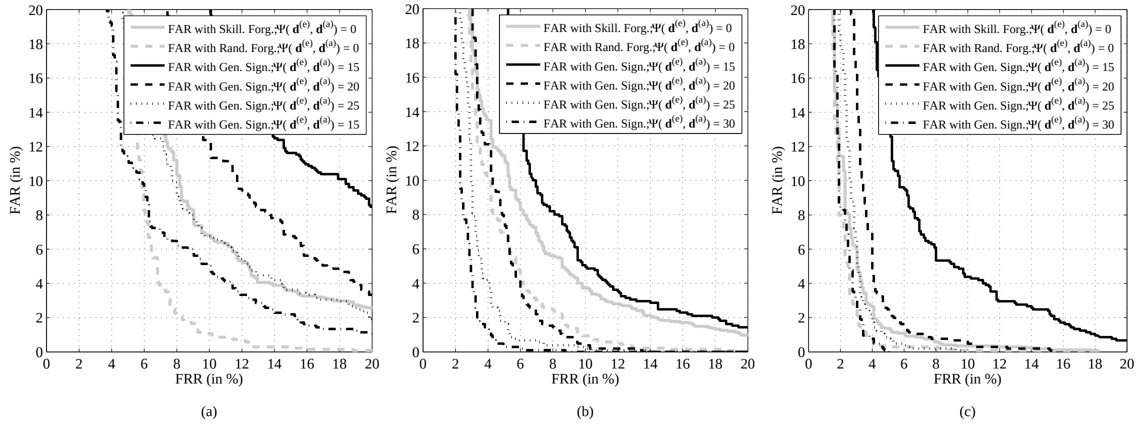


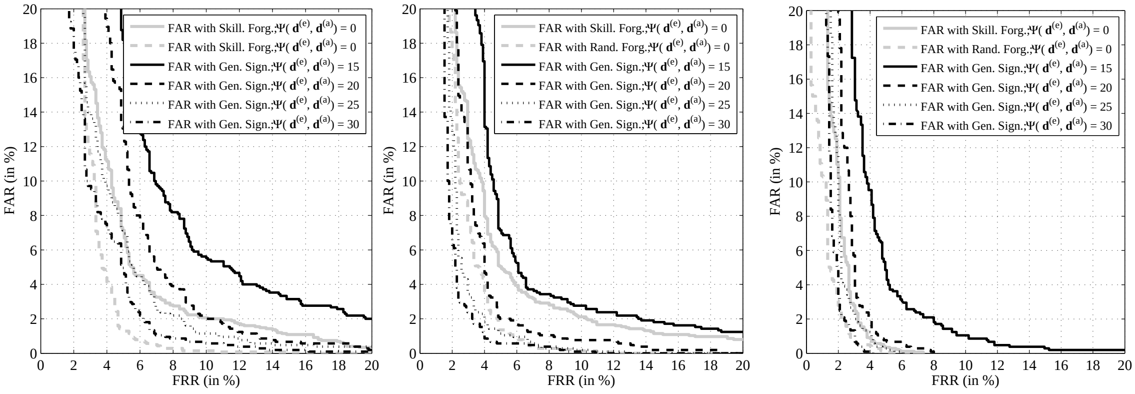
Figure 5.8: Renewability Analysis of the protected baseline approach (Section 5.1.1), having considered $E = 5$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

- the random forgeries available in the test data set, transformed according to key vectors $\mathbf{d}^{(a)}$ which are the same of those employed during enrollment ($\Psi(\mathbf{d}^{(e)}, \mathbf{d}^{(a)}) = 0$);

- the genuine signatures of each user, transformed according to key vectors $\mathbf{d}^{(a)}$ having a distance $\Psi(\mathbf{d}^{(e)}, \mathbf{d}^{(a)}) \in \{15, 20, 25, 30\}$ from the ones employed during enrollment.

The ROC curves obtained from these experiments are shown in Figure 5.8 for a system with $E = 5$, and in Figure 5.9 for a system with $E = 10$. All the three matching strategies presented in Section 5.3.2 are considered in the reported results, while $W = 2$ is kept as already said.

It is worth pointing out that, in order to properly satisfy the diversity property, different templates, generated from the same data but using different keys, should not match between themselves. This means that transformed templates generated from the same signature should behave like signatures produced by different users. The diversity requirement is then respected when the pseudo-ROC curves, obtained matching signatures transformed according to different transformations, can be compared with ROC curves obtained considering the random forgeries. Specifically, the diversity property can be properly satisfied only for key vector distances $\Psi(\mathbf{d}^{(e)}, \mathbf{d}^{(a)}) > 25$. This implies that, when keeping $25 < \Psi(\mathbf{d}^{(e)}, \mathbf{d}^{(a)}) \leq 30$, a maximum number of $\Gamma = \lfloor (95 - 5)/30 \rfloor + 1 = 4$ different key



(a) (b) (c)

Figure 5.9: Renewability Analysis of the protected baseline approach (Section 5.1.1), having considered $E = 10$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

vectors $\mathbf{d}$ can be properly considered in a template protection scheme. It can also been noticed that systems employing DTW perform better, in terms of renewability capability, than those using the employed HMM implementation. However, the obtained results show that the available key space, for a system employing the baseline protected approach described in Section 5.1.1, is very small, and therefore not practical for a signature verification system. The extended approaches presented in Section 5.1.2 provide key spaces with higher dimensionality, being thus more suitable for the system deployment in real world applications.

5.6.2 Protected Mixing Approach

In Section 5.1.2.1 it has been shown how to transform an original signature employing two transformation keys: the decomposition vector $\mathbf{d}$, used to define the decomposition points, and the scrambling matrix $\mathbf{C}$, which defines the original sequences whose selected segments generate the transformed sequences, according to equation (5.5).

In order to evaluate the renewability capacity of the approach described in Section 5.1.2.1, the maximum number of scrambling matrices which can be properly employed, in order to transform the original signature representations while keeping fixed the decomposition vector $\mathbf{d}$, will be estimated.

As defined in Section 5.1.2.1, a scrambling matrix $\mathbf{C}$ consists of F rows and W columns. The total number of matrices which can be defined is then equal to $(F!)^{(W-1)}$, which corresponds to $14! = 87178291200$ when considering $F = 14$ and $W = 2$. However, among all the possible scrambling matrices, only those which allow to respect the diversity property can be employed.

Given two matrices $\mathbf{T}^{(1)}$ and $\mathbf{T}^{(2)}$, let us define the distance

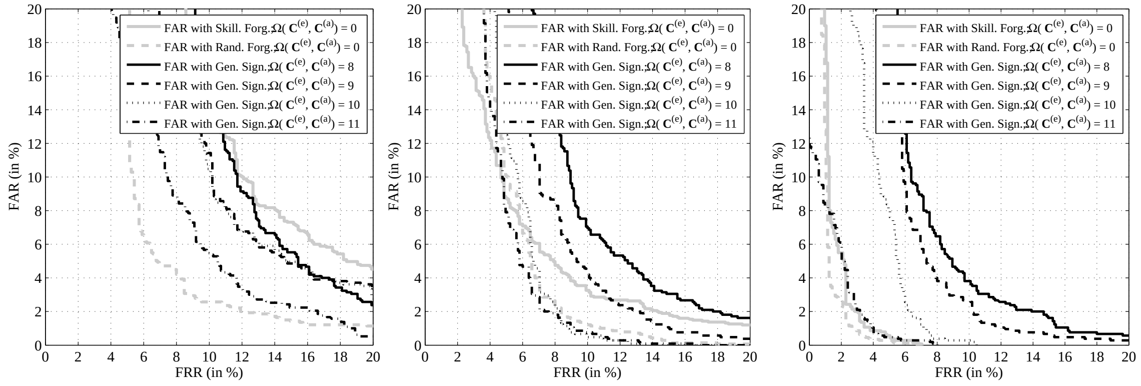
$$\Omega(\mathbf{T}^{(1)}, \mathbf{T}^{(2)}) = \text{ number of correpsonding different rows between } \mathbf{T}^{(1)} \text{ and } \mathbf{T}^{(2)} \tag{5.22}$$

as the number of corresponding different rows between the matrices $\mathbf{T}^{(1)}$ and $\mathbf{T}^{(2)}$. Following the approach illustrated in Section 5.1.2.1, two transformations obtained by using the same decomposition vector $\mathbf{d}$, while employing two distinct scrambling matrices $\mathbf{C}^{(1)}$ and $\mathbf{C}^{(2)}$, produce more distinct templates as the distance $\Omega(\mathbf{C}^{(1)}, \mathbf{C}^{(2)})$ increases. Considering the available test data set, each user is then enrolled by using his first E signatures, to which the transformation process of Section 5.1.2.1 is applied. Specifically, the transformations employed during enrollment are ruled by a decomposition vector $\mathbf{d}$ and a scrambling key matrix $\mathbf{C}^{(e)}$. The remaining signatures of each users, after being transformed using the same keys $\mathbf{d}$ and $\mathbf{C}^{(e)}$ applied during enrollment, are employed to estimate the FRR.

The matching statistics related to FAR are computed considering:

- the skilled forgeries available in the test data set, transformed according to the decomposition vector $\mathbf{d}$, and to the scrambling matrix $\mathbf{C}^{(a)} = \mathbf{C}^{(e)}$ employed during enrollment;
- the random forgeries available in the test data set, transformed according to the decomposition vector $\mathbf{d}$, and to the scrambling matrix $\mathbf{C}^{(a)} = \mathbf{C}^{(e)}$ employed during enrollment;
- the genuine signatures of each user, transformed according to the same decomposition key $\mathbf{d}$ employed during enrollment, but with different scrambling keys $\mathbf{C}^{(a)}$, characterized by distances $\Omega(\mathbf{C}^{(e)}, \mathbf{C}^{(a)}) \in \{8, 9, 10, 11\}$ from $\mathbf{C}^{(e)}$.

The renewability property of the protected mixing approach is tested by comparing the ROC curve where FAR for random forgeries is taken into account, with the pseudo-



(a)

(b)

(c)

Figure 5.10: Renewability analysis of the protected mixing approach (Section 5.1.2.1), having considered $E = 5$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

ROC curves where FAR for genuine signatures, transformed using a scrambling matrix $\mathbf{C}^{(a)} \neq \mathbf{C}^{(e)}$, is considered.

The obtained system performance are shown in Figure 5.10 for a system with $E = 5$, and in Figure 5.11 for a system with $E = 10$. All the three matching strategies presented in Section 5.3.2 are considered in the reported results.

The obtained performances show that the use of different scrambling matrices between enrollment and authentication, also when keeping fixed the decomposition keys, allows obtaining recognition rates which are similar to those associated with the use of random forgeries, but only when $\Omega(\mathbf{C}^{(e)}, \mathbf{C}^{(a)}) \geq \Xi = 11$ (over $F = 14$ considered sequences). Also in this case, systems employing DTW perform better, in terms of renewability capability, than those using the employed HMM implementation. The fusion of DTW and HMM based classifiers allows to further improve the achieved performances.

The total number of scrambling matrices which can therefore be considered, still satisfying the diversity property, that is, guaranteeing a distance $\Omega \geq \Xi = 11$ between themselves, has an upper bound equal to $\frac{F!}{(\Xi-1)!} = 24024$. Moreover, keeping in mind that, as explained in Section 5.6.1, $\Gamma = 4$ distinct decomposition vectors can be defined for each scrambling matrix $\mathbf{C}$, the total number of renewable templates which can be properly generated, following the approach of Section 5.1.2.1, is $4 \cdot 24024 = 96096$.

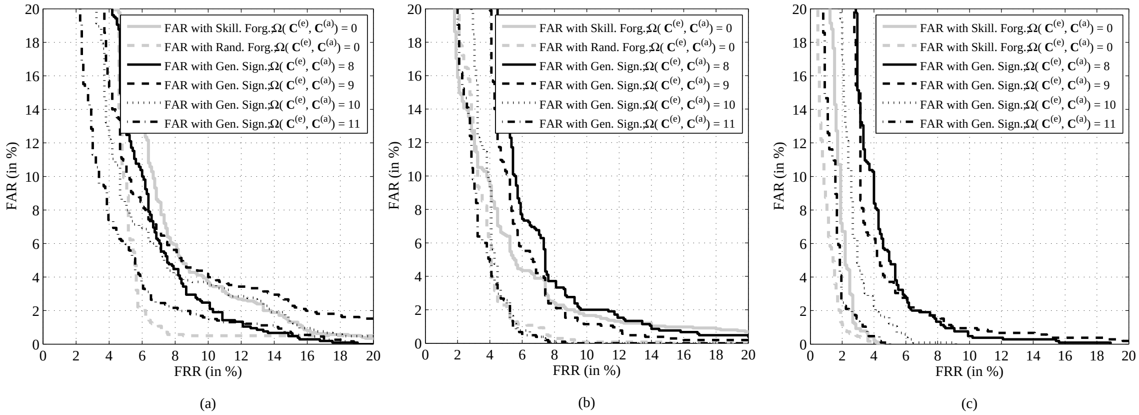


Figure 5.11: Renewability analysis of the protected mixing approach (Section 5.1.2.1), having considered $E = 10$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

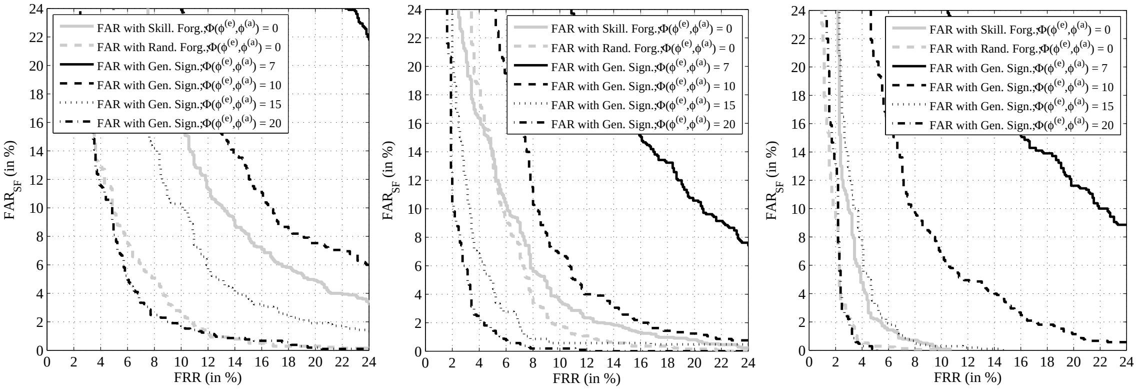
5.6.3 Protected Shifting Approach

In this Section we verify how the renewability property of the baseline approach of Section 5.1.1 is improved using the method described in Section 5.1.2.2, which employs a decomposition vector $\mathbf{d}$ and a shifting parameter ϕ as transformation keys.

Following an approach similar to the one employed in Section 5.6.1 and Section 5.6.2, each user available in the test data set is enrolled by using his first E signatures, which are then transformed according to the transformation keys $\mathbf{d}$ and $\phi^{(e)}$. Then, the remaining genuine signatures of each user are transformed using the same decomposition key $\mathbf{d}$ employed during enrollment, but with a different initial shift, indicated as $\phi^{(a)}$, to determine the FAR that is used to analyze the renewability capacity of this approach. The values of the shifts are taken in the range between 0 and 95, considering only multiples of 5: in this way, 20 different possible values are taken into account. Having defined a distance between the shifting parameters taken during enrollment and verification as:

$$\Phi(\phi^{(e)}, \phi^{(a)}) = |\phi^{(e)} - \phi^{(a)}|, \tag{5.23}$$

Figure 5.12 and Figure 5.13 show the results obtained by considering the same decomposition keys during enrollment and verification, at an increasing distance $\Phi(\phi^{(e)}, \phi^{(a)})$ between the employed shifting parameters, respectively for $E = 5$ and $E = 10$. A comparison with the recognition performances obtained considering skilled and random forgeries,



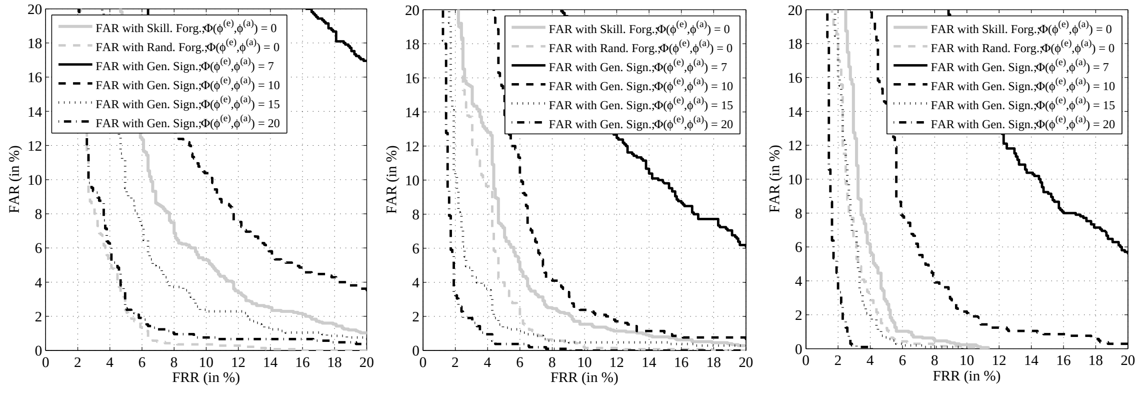
(a) (b) (c)

Figure 5.12: Renewability analysis of the protected shifting approach (Section 5.1.2.2), having considered $E = 5$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

transformed with the same transformation keys $\mathbf{d}$ and $\phi^{(e)}$ employed in enrollment, is also given. All the three matching strategies presented in Section 5.3.2 are considered in the reported results.

The obtained experimental results show that the pseudo-ROC curves, that are related to the use of different shifting parameters for the enrollment and the authentication stage, are similar to those obtained when random forgeries are taken into account, when the distance $\Phi(\phi^{(e)}, \phi^{(a)})$ is equal or greater than the 15% of the signature length N. This implies that the number of values ϕ which can be properly considered is limited to $\Upsilon = 7$. Applying the modification described in Section 5.1.2.2 to the baseline approach of Section 5.1.1, an increase of the number of templates that can be generated by a factor of $\Upsilon = 7$ can be obtained, thus reaching a number of $\Gamma \cdot \Upsilon = 4 \cdot 7 = 28$ templates. Obviously, this number is still too small for a practical application. However, if the considered modification is applied in conjunction with the method described in Section 5.1.2.1, it is possible to properly produce renewable templates with an upper limit of $\Gamma\frac{F!}{(\Xi-1)}\Upsilon = 96096 \cdot 7 = 672672$ discriminable templates.

In conclusion, although with the proposed approaches it is not possible to generate an almost infinite number of discriminable templates, still more than 600000 templates can however be generated from a single original signature, properly respecting the requirement



(a) (b) (c)

Figure 5.13: Renewability analysis of the protected shifting approach (Section 5.1.2.2), having considered $E = 10$ and $W = 2$ during enrollment. (a): HMM; (b): DTW; (c): Fusion of HMM and DTW.

of diversity. It is also worth pointing out that, having the possibility of managing more than 600000 different templates, a user could issue a new biometric templates each hour, for 60 consecutive years.

5.7 Cancelable Sequence based Biometric Templates: Discussion

In this Chapter, template protection schemes which can be applied to any biometrics based on functional features have been proposed. The basic idea of the proposed protection schemes is to transform the original sequences through non-invertible transforms based on convolutions between random sequence segments. A baseline approach, together with two extended versions of the baseline method, have been introduced.

The security of the proposed approaches, relying on the difficulty to solve a blind deconvolution problem, has been extensively carried out.

As a proof of concept, the proposed protection approaches have been applied to an on-line signature based authentication system, where HMM, DTW, and score fusion techniques have been employed for template matching. The performances of various protected configurations have been compared with those of an unprotected system, showing a very slight loss of performance in terms of EER for the protected schemes, as well as a very small dependence of the performances on the transformation parameters. Moreover, the ability of generating multiple templates from the same original data, while respecting the needed diversity property for cancelable templates, has been deeply investigated.

More in detail, from the obtained experimental results regarding both the renewability and the recognition performance of the protected on-line signature verification system, it can be noticed that:

- the baseline protection approach presented in Section 5.1.1 introduces only a slight loss of performance in terms of EER, with respect to an unprotected system. Moreover, the authentication performances achievable with the protected system present a slight dependence on the transformation parameters;

- the DTW based matching strategies performs generally better than the one employing HMMs. The better behavior is related to both the authentication performances and the renewability performances, and is enhanced when the number E of signature taken from each user during enrollment decreases;

- the recognition performances achievable following the methods described in Section 5.1.2 are basically the same of the method of Section 5.1.1.

- In order to properly guarantee the users' privacy in a protected on-line signature-based recognition application, the baseline approach presented in Section 5.1.1 cannot be used, due to its low renewability capacity. However, the methods described in Section 5.1.2 can be implemented to satisfy all the requirements of a properly defined cancelable biometrics, being possible to generate, through them, multiple templates from the same data, with a variability between them at least similar to the one found between signatures taken from different users. It is worth pointing out that, incrementing the number E of signatures taken during enrollment, the recognition performances of the proposed methods improve, and, with them, also the renewability property: the probability of match between signatures transformed according to different transformations decreases, following the behavior of the probability of matching between original and random signatures.

Eventually, it is worth stressing out that the proposed protection methods can be applied to any other biometrics for which a sequence based recognition approach can be performed. Moreover, being able to provide a score as output of the recognition process, the proposed methods can be employed in order to construct protected multi-biometrics systems, where score-level fusion is used to combine different biometric modalities, while keeping secret the original biometric data.

Chapter 6

Signature based Authentication using Watermarking

In this Chapter, we introduce a multi-level signature based authentication system, where data hiding is employed to hide and keep secret some dynamic signature features in a static representation of the signature itself. Following such approach, instead of defining a cancelable biometrics based scheme, the protection of signature templates is accomplished by means of watermarking techniques. Being a behavioral biometric, signatures are intrinsically different from other commonly used biometric data, possessing dynamic properties which can not be extracted from a single signature image. By the fact, the dynamic behavior of a signature is more difficult to forge than the static one. Therefore, the disclosure of the dynamic characteristics of an on-line signature is typically an issue more problematic than the disclosure of a static signature image. In the proposed architecture, a set of dynamic signature features is kept hidden till it is requested by a specific application.

The employed watermarking technique is tailored to images with sharpened edges, just like a signature picture. In order to obtain an embedding method which is robust to compression and additive noise, while keeping intact the original structure of the host, the mark is inserted as close as possible to the lines that constitute the signature, using the properties of the Radon transform.

The proposed system has been designed in order to realize a signature based security scalable authentication system. The marked signature images can be used for user authenti-

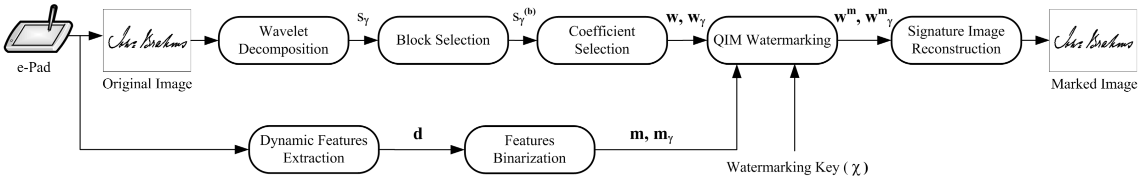

e-Pad
Original Image
Wavelet Decomposition
S_γ
Block Selection
$S_\gamma^{(b)}$
Coefficient Selection
$\mathbf{w}, \mathbf{w}_\gamma$
QIM Watermarking
$\mathbf{w}^m, \mathbf{w}^m_\gamma$
Signature Image Reconstruction
Marked Image
Dynamic Features Extraction
$\mathbf{d}$
Features Binarization
$\mathbf{m}, \mathbf{m}_\gamma$
Watermarking Key (χ)

Figure 6.1: Security-scalable signature-based authentication system using data hiding. Proposed enrollment scheme.

cation, letting their static characteristics being analyzed by automatic algorithms or security attendants. When higher security is needed, the embedded features can be extracted and used to enforce the authentication procedure.

An extensive set of experimental results, concerning both the mark extraction and the verification performances, are reported to show the effectiveness of the proposed approach.

6.1 Multi-level signature based verification system

In this Section, the proposed security scalable signature based authentication system is briefly sketched, and it will be described in detail in the following sections.

6.1.1 Enrollment Stage

The enrollment procedure of the considered system is shown in Figure 6.1. During this stage, we both extract a set of dynamic features which has to be embedded in a signature image of the considered user u, and some static features which are employed to perform a first level of user authentication. The proposed enrollment scheme can be summarized in the following steps:

- for a given user u, a set of static features is extracted from each of the E acquired signatures, and collected in the vectors $\mathbf{v}_e^u[k]$, with $e = 1, \cdots, E$ and $k = 1, \ldots, K$. Among the E signatures acquired from the user u, a representative signature is selected, and employed to to generate a synthetic signature image $s[i, j]$. In order to select the user's most representative signature, the mean and standard deviation feature vectors $\boldsymbol{\mu}^u[k]$ and $\boldsymbol{\sigma}^u[k]$ are computed from the vectors $\mathbf{v}_e^u[k]$, $e = 1, \cdots, E$. A distance measure D^u is then evaluated for each enrolled signature as:

$$D_e^u = \sqrt{\sum_k^K \left(\frac{\mathbf{v}_e^u[k] - \boldsymbol{\mu}^u[k]}{\boldsymbol{\sigma}^u[k]} \right)^2}. \tag{6.1}$$

The signature giving the lowest value D_e^u, with $e = 1, \ldots, E$, is then selected for the user u. The chosen signature represents the one whose static features are the closest to the estimated mean, and becomes the host image where to embed the selected user's dynamic features;

- the signature pressure values are considered when creating the image $s[i,j]$, which is therefore represented in a gray-scale. Linear interpolation is implemented, both for the spatial coordinate and for the pressure values, in order to obtain the signature image from the acquired data. The acquired pressure values are inserted in the signature static representation in order to obtain, during authentication, a higher discriminative capability, with respect to the simple binary signature images employed by conventional methods. Features depending ont he applied pressure are therefore considered in the feature vectors $\mathbf{v}_e^u[k]$, employed to select the representative signature of user u;

- the acquired pressure image $s[i,j]$ undergoes a two-level wavelet decomposition. The second level subbands, namely $s_{2LL}[i,j]$, $s_{2HL}[i,j]$, $s_{2LH}[i,j]$, and $s_{2HH}[i,j]$, which represent the approximation, the horizontal detail, the vertical detail, and the diagonal detail subband respectively, are selected for the embedding;

- being signature images typically sparse images, the subbands $s_\gamma[i,j]$, with $\gamma \in \Gamma = \{2LL, 2HL, 2LH, 2HH\}$, are then decomposed into blocks of $P_I \times P_J$ pixels, in order to perform a local analysis and to identify the proper areas where the watermark has to be embedded;

- a novel embedding domain is employed to hide the dynamic information in the considered signature images. The proposed domain is derived from the Radon transform [189], as detailed in Section 6.2.3, and indicated as *Radon-DCT* domain. The selected blocks are projected in the Radon-DCT domain, and the most relevant projections' coefficients are chosen as the hosts where to embed the mark. In the following, even

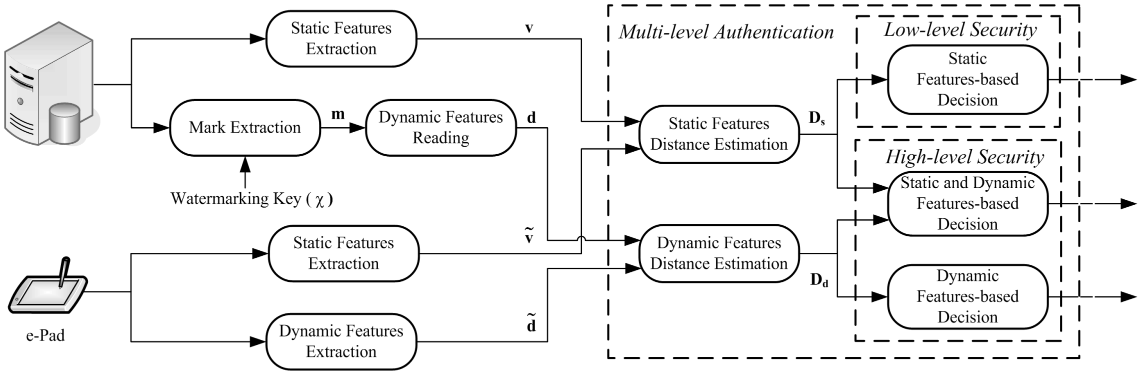

Static Features Extraction
v
Mark Extraction
m
Dynamic Features Reading
d
Watermarking Key (χ)
Static Features Extraction
ṽ
Dynamic Features Extraction
d̃
e-Pad
Multi-level Authentication
Static Features Distance Estimation
Dynamic Features Distance Estimation
Ds
Dd
Low-level Security
Static Features-based Decision
High-level Security
Static and Dynamic Features-based Decision
Dynamic Features-based Decision

Figure 6.2: Security-scalable signature-based authentication system using data hiding. Proposed authentication scheme.

the ridgelet embedding domain [190], which is also based on the Radon transform, will be outlined in Section 6.2.2. The mark extraction performances achievable with the proposed Radon-DCT embedding domain are compared in Section 6.6 with those obtained when employing the ridgelet embedding domain;

- a set of relevant dynamic features is extracted from the acquired signatures. Their mean values are then binarized, in order to be embedded into the user's synthetic signature image. The number of dynamic features which are embedded in the signature image is necessarily limited, due to the need of modifying only slightly the signature image through the mark insertion. In order to identify the most representative parameters, a feature selection procedure, introduced in Section 6.4, is employed. Moreover, in order to represent the selected features with the shortest possible binary string, a feature binarization procedure, described in Section 6.5, is also proposed;

- the dynamic features extracted from the acquired signatures are eventually embedded in the signature image, by means of quantization index modulation (QIM) watermarking [191].

6.1.2 Authentication Stage

In the authentication stage, the user is asked to provide his signature by means of an electronic pad. When a low security level is required, the authentication can be performed using only the selected static features, which also comprise pressure information. With reference to Figure 6.2, for a given user u a set of static features are computed, collected in the vector $\tilde{\mathbf{v}}^u[k]$, and compared with the static signature feature vector $\mathbf{v}^u[k]$ extracted from the provided signature image. It has to be noticed that the static features employed as reference template correspond to a single signature acquisition, that is, the one employed as representative for the user u. If a higher security level is required, dynamic features are obtained from the acquired signature, collected in the vector $\tilde{\mathbf{d}}_u[k]$, and compared with the dynamic features template $\mathbf{d}^u[k]$, extracted from the watermarked signature image.

The Mahalanobis distance is employed to compare both static and dynamic features vectors. Considering the matching of dynamic features, the dissimilarity distance is computed as:

$$D(\tilde{\mathbf{d}}^u[k], \mathbf{d}^u[k]) = \sqrt{\sum_k \left(\frac{\tilde{\mathbf{d}}^u[k] - \mathbf{d}^u[k]}{\boldsymbol{\sigma}_{\mathbf{d}^u}[k]} \right)^2}. \qquad (6.2)$$

If the distance $D(\tilde{\mathbf{d}}^u[k], \mathbf{d}^u[k])$ is less than a fixed threshold, the user is authenticated, otherwise, he is rejected. The same king of matching is performed to compare the features extracted from the static signature representation.

It is worth pointing out that the presented system can employ a *distributed storage* of the considered biometrics: for example, the marked signature images can be included in an ID Card, in order to be employed when the enrolled user wants to access a given resource or service, provided by the application. The standard deviations of the considered static and dynamic features, computed during the enrollment, and employed during the authentication phase according to equation (6.2), can be stored either in the card, or in a centralized database. In fact, the information given by the variability of the considered features is typically less sensitive than the one contained in the features' mean values. However, the security of the considered system can increase if the same features' standard deviations are employed for all the enrolled users. Specifically, for a given feature k, being it static or dynamic, a standard deviation common for each user can be computed as the mean value of the standard deviations evaluated from a set signatures, available during a training phase. In this case, less information regarding the users is stored, with respect to the use of individual variances for each enrolled user.

The comparison between the verification performances achievable when employing common or individual feature standard deviations is discussed in Section 6.6.

6.1.2.1 Fusion approach

When required by the considered application, an even higher level of security can be obtained by combining both dynamic and static features, using score fusion techniques [104]. The fusion of different kinds of signature characteristics has been proposed in [134, 143], among the others.

In Section 6.6, the performances achievable when using only either the static features or the dynamic features, and a combination of both, are presented.

The techniques employed to fuse the dissimilarity values obtained from static and dynamic information have been presented in Section 5.3.2.3. As in Chapter 5, fixed score normalization [104], which consists in using the same parameters for the normalization of the scores derived from each considered user, is employed. A training data set is needed to carefully tuning the employed parameters, in order to obtain good fusion efficiency.

6.2 Embedding Domains

Signature images are sparse images characterized by line singularities defined over a 2-D domain. Therefore, the Radon transform [189] appears to be a good tool to analyze this kind of images.

The proposed watermark embedding domain is obtained from the Radon transform, aiming at focusing the energy of each Radon projection in a limited number of coefficients. When wavelet decomposition is applied to the Radon projections, the so called ridgelet transform [190] is obtained. We propose to perform the embedding in the domain obtained by applying the discrete cosine transform (DCT) to each Radon projection, thus introducing a combined Radon-DCT (R-DCT) domain.

6.2.1 Radon Transform

The Radon Transform is used in a wide variety of applications including tomography, ultrasound, optics and geophysics, to cite only a few. The continuous Radon transform $RF_f(\theta, t)$ of an integrable bivariate function $f(\mathbf{x}) = f(x_1, x_2)$ is defined as:

$$RF_f(\theta, t) = \int\int_{\mathbb{R}^2} f(x_1, x_2)\delta(x_1 \cos\theta + x_2 \sin\theta - t)dx_1 dx_2, \tag{6.3}$$

being $(\theta, t) \in [0, 2\pi) \times \mathbb{R}$, and δ the Dirac distribution. The value $RF_f(\theta, t)$ thus represents the integral of $f(\mathbf{x})$ over a line oriented at an angle θ, and whose distance from the origin is t. Therefore, the Radon transform maps each line in the spatial domain (x_1, x_2) into a point in the (θ, t) domain. The continuous inverse Radon transform can be expressed as:

$$f(x_1, x_2) = \frac{1}{2\pi^2}\int_0^{\pi}\int_{-\infty}^{\infty} \frac{\partial RF_f(\theta, t)/\partial t}{x_1 \cos\theta + x_2 \sin\theta - t} dt d\theta. \tag{6.4}$$

Among the approaches which have been proposed in literature to implement the continuous Radon Transform in the discrete domain, the recently introduced Finite Radon Transform (FRAT) [190] is employed in this Thesis. The FRAT, defined as summations of image pixels over a certain set of “lines” in a discrete 2-D space, is both perfectly invertible and non-redundant. Specifically, having considered a real function $f[i, j]$ defined over a finite grid Z_P^2, being $Z_P = \{0, 1, \cdots, P-1\}$, its FRAT is given by:

$$\mathrm{FRAT}_f[n, p] = r[n, p] = \frac{1}{\sqrt{P}} \sum_{(i,j)\in S_{p,n}} f[i, j], \tag{6.5}$$

where $S_{p,n}$ defines the set of points that form a line on Z_P^2:

$$\begin{aligned} S_{p,n} &= \{(i, j) : j = pi + n \pmod{P}, i \in Z_P\}, \\ S_{P,n} &= \{(n, j) : j \in Z_P\}, \end{aligned} \tag{6.6}$$

being $p \in Z_{P+1}$ the line direction and n its intercept.

The FRAT can be inverted using a finite back-projection (FBP) operator, defined as the sum of Radon coefficients of all the lines that go through a given point, that is:

$$\mathrm{FBP}_r[i, j] = f[i, j] = \frac{1}{\sqrt{P}} \sum_{(p,n)\in O_{i,j}} r[p, n], \quad (i, j) \in Z_P^2, \tag{6.7}$$

where $O_{i,j}$ denotes the set of indices of all the lines that go through a point $(i,j) \in Z_P^2$, that is:

$$O_{i,j} = \{(p,n) : n = j - pi \pmod P), k \in Z_{P+1}\} \cup \{(P,i)\}. \tag{6.8}$$

The watermark embedding domains described in the following, which stem from the Radon transform domain, have been designed in order to allow an energy compaction in few representative coefficients for each Radon projection. Specifically:

- the ridgelet transform [190] applies a wavelet decomposition to the Radon projections. Watermark embedding in the ridgelet domain has already been employed in [192] and in [193];

- the Radon-DCT (R-DCT) transform applies the discrete cosine transform (DCT) to each Radon projection. This domain has been proposed by the author in [63], and here employed for the proposed multi-level authentication system.

6.2.2 Ridgelet Domain

Given an integrable bivariate function $f(\mathbf{x}) = f(x_1, x_2)$, its continuous ridgelet transform (CRT), defined in [190], can be evaluated by employing the wavelet transform in the Radon domain. Specifically, the CRT can be obtained by applying a 1-D wavelet transform to $RF_f(\theta, t)$ as follows:

$$CRT_f(a, \rho, \theta) = a^{-1/2} \int_{\mathbb{R}} \psi\left(\frac{t-\rho}{a}\right) RF_f(\theta, t) dt. \tag{6.9}$$

From equation (6.9), it can be seen that an invertible finite ridgelet transform (FRIT) [190] can be derived from the application of a 1-D discrete wavelet transform on each FRAT projection sequence $(r[p,0], r[p,1], \cdots, r[p,P-1])$, for each direction $p \in Z_{P+1}$:

$$\mathrm{FRIT}_f[p,q] = g[p,q], \quad q \in Z_P. \tag{6.10}$$

Thanks to the wavelets' properties, the FRIT is able to concentrate the energy of each Radon projection sequence in its first coefficients.

6.2.3 Radon-DCT Domain

As an alternative to wavelet analysis, the DCT can be used to obtain energy compaction. A novel embedding domain is thus defined, indicating with Radon-DCT (R-DCT) the transform derived from application of the DCT on each FRAT projection sequence ($r[p,0]$, $r[p,1], \cdots, r[p,P-1]$), $k \in Z_{P+1}$:

$$\text{R-DCT}_f[p,q] = c[p,q] = \zeta[n] \sum_{n=0}^{P-1} r[p,n] \cos\left[\frac{\pi(2n+1)q}{2P}\right] \tag{6.11}$$

with $q \in Z_P$, $\zeta[0] = \sqrt{1/P}$, and $\zeta[n] = \sqrt{2/P}$, $n \neq 0$. Coefficients R-DCT $_f[p,0] = c[p,0]$, $p \in Z_{P+1}$, represent the DC component of each projection p, and are therefore connected with the mean value of each Radon projection.

6.3 Dynamic Signature Features Embedding

As already outlined, in the proposed scheme the host pressure image $s[i,j]$ undergoes a two-level wavelet decomposition, and the second level subbands $s_\gamma[i,j]$, $\gamma \in \Gamma = \{2LL$, $2HL$, $2LH$, $2HH\}$, are then decomposed into blocks of $P_I \times P_J$ pixels, in order to identify the proper areas where the watermark has to be embedded. This task is accomplished by selecting only those blocks whose energy is greater than a fixed threshold T_E. Specifically, indicating with $s_\gamma^{(h)}[i,j]$ the generic h-th block extracted from the subband γ, this block is selected for watermark embedding if

$$\frac{1}{P_I P_J} \sum_{i=1}^{P_I} \sum_{j=1}^{P_J} \left|s_\gamma^{(h)}[i,j]\right| > T_E, \tag{6.12}$$

that is, if the block contains a meaningful fragment of the signature.

In the proposed implementation, it has been considered that $P_I = P_J = P$. Table 6.1 shows the mean, the maximum, and the minimum number of blocks H_γ which can be marked according to the criterion given in equation (6.12), for each subband of the second wavelet decomposition level, $\gamma \in \Gamma = \{2LL$, $2HL$, $2LH$, $2HH\}$. The reported values are referred to experiments evaluated on the public MCYT database with 100 users, setting $P = 10$ and $T_E = 5$. The employed signature images have dimension 720 × 1440 pixels, being thus possible to divide each of them into 10368 blocks of dimension 10 × 10.

Wavelet decomposition Subband	**Minimum number of Markable Blocks**	**Mean number of Markable Blocks**	**Maximum number of Markable Blocks**
$2LL$	70	161.13	285
$2HL$	47	129.08	250
$2LH$	13	110.85	221
$2HH$	22	106.73	204

Table 6.1: Minimum, mean, and maximum number of markable blocks for each second-level wavelet decomposition subband.

As can be seen from Table 6.1, each subband can provide a significant number of blocks where to embed the mark. Once the blocks are selected, they can be projected in the R-DCT or in the ridgelet domain to choose the watermark host coefficients, as detailed in Section 6.3.1.

6.3.1 Coefficients Selection

In order to determine the coefficients where to embed the mark, the selected H_γ blocks $s_\gamma^{(h)}[i,j]$, for each subband γ, have be projected in the R-DCT domain. Given the h-th block, $P+1$ R-DCT sequences $(c_\gamma^{(h)}[p,0], c_\gamma^{(h)}[p,1], \ldots, c_\gamma^{(h)}[p,P-1])$, related to each direction $p \in Z_{P+1}$, are then available. Only the two most energetic directions, namely p_1 and p_2, are then selected. The matrix $\mathbf{W}_\gamma^{(h)}$ is then built by extracting N coefficients from each of the selected projections:

$$\mathbf{W}_\gamma^{(h)} = \begin{pmatrix} c_\gamma^{(h)}[p_1,1] & c_\gamma^{(h)}[p_1,2] & \cdots c_\gamma^{(h)}[p_1,N] \\ c_\gamma^{(h)}[p_2,1] & c_\gamma^{(h)}[p_2,2] & \cdots c_\gamma^{(h)}[p_2,N] \end{pmatrix}. \tag{6.13}$$

It is worth pointing out that the DC coefficient $c_\gamma^{(h)}[p,0]$ of each projection p is not selected to be marked. This choice is done in order to not modify the mean value of each Radon projection after the watermarking. As can be derived from equation (6.5), and reported in [190], all the FRAT projections $\mathrm{FRAT}_f[p,n]$, $p \in Z_{P+1}$ of a function $f[i,j]$ defined over Z_P^2 should possess the same mean value, related to the mean value of $f[i,j]$. Leaving the DC coefficient unchanged after watermarking means maintaining the original mean value of the Radon sequence, that remains equal to the mean values of all the other Radon projections taken from the same block.

The procedure is iterated for all the H_γ blocks selected from the subband γ. The matrix $\mathbf{W}_\gamma$, having dimension $2H_\gamma \times N$ is then built as:

$$\mathbf{W}_\gamma = \left(\begin{array}{c} \mathbf{W}_\gamma^{(1)} \\ \mathbf{W}_\gamma^{(2)} \\ \vdots \\ \mathbf{W}_\gamma^{(H_\gamma)} \end{array} \right). \tag{6.14}$$

Performing this procedure for each subband $\gamma \in \Gamma$, four host vectors $\mathbf{w}_\gamma$ where to embed the mark are obtained by scanning the matrices $\mathbf{W}_\gamma$ column-wise.

When considering the embedding in the ridgelet domain, a similar approach can be employed. Specifically, the FRIT is applied to each block selected from subband γ, whose total number is indicated as H_γ. Given the h-th block, $P{+}1$ FRIT sequences $(g_\gamma^{(h)}[p,0], g_\gamma^{(h)}[p,1], \ldots, g_\gamma^{(h)}[p, P-1])$, related to the directions $p \in Z_{P+1}$, are then available. Only the two most energetic directions, namely p_1 and p_2, are selected, and the first N values of the sequences associated to them are extracted and employed to build the matrix $\mathbf{W}_\gamma^{(h)}$:

$$\mathbf{W}_\gamma^{(h)} = \left(\begin{array}{ccc} g_\gamma^{(h)}[p_1,0] & g_\gamma^{(h)}[p_1,1] & \cdots g_\gamma^{(h)}[p_1,N-1] \\ g_\gamma^{(h)}[p_2,0] & g_\gamma^{(h)}[p_2,1] & \cdots g_\gamma^{(h)}[p_2,N-1] \end{array} \right). \tag{6.15}$$

A matrix $\mathbf{W}_\gamma$ can then be built, as reported in equation (6.14). By iterating the process for all the H_γ selected blocks, four host vectors $\mathbf{w}_\gamma$ can be obtained by scanning the matrices $\mathbf{W}_\gamma$ column-wise, as for the R-DCT coefficient embedding. However, it is worth pointing out that, when employing the ridgelet domain embedding, the mean values of all the Radon projections taken from the a given block is altered, in contrast to what happens when the mark embedding is performed in the R-DCT domain.

6.3.2 Watermark Generation

During the enrollment stage, E on-line signatures are acquired for each considered user u, and a set of L dynamic features is extracted from each of them. A vector $\mathbf{d}^u[l]$, with $l \in \mathcal{L} = \{1, \ldots, L\}$, is then generated, where each of its component is computed as the average of the l-th dynamic feature values. Furthermore, the L elements of $\mathbf{d}^u[l]$ are binarized, in order to produce the binary string which is inserted in the selected signature image.

More in detail, the binary vector which is employed as mark has to be protected against possible errors which can be performed during mark extraction. In fact, although the proposed embedding approach is robust to modifications of the host signature images, the mark can be altered if the considered image undergoes a low quality JPEG compression, or if it is subjected to the addition of white Gaussian noise.

Therefore, in order to protect the embedded marks, an error correcting code has to be applied to the string generated from the binarization of the dynamic features. Specifically, in the proposed implementation a (127,92) BCH code, which provides an error correction capability (ECC) equal to 5 bits, is employed to protect the employed binary string.

The output of the mark generation procedure therefore consists of a binary vector $\mathbf{m}$ of 127 bits, which has to be inserted in the coefficients of the R-DCT or ridgelet domain. The host coefficient where the mark has to be embedded, as described in Section 6.3.1, are given by the four vectors $\mathbf{w}_\gamma$, $\gamma \in \Gamma$.

6.3.3 QIM Watermarking

The binary mark $\mathbf{m}$ is decomposed into three 32 bits-distinct marks $\mathbf{m}_{2LL}$, $\mathbf{m}_{2HL}$ and $\mathbf{m}_{2LH}$, and a fourth mark $\mathbf{m}_{2HH}$ with dimension equal to 31 bits. These marks are separately embedded, by means of QIM [191] watermarking, in the corresponding host vectors $\mathbf{w}_\gamma$, $\gamma \in \Gamma$. Less bits are inserted in the $2HH$ subband, with respect to the others, due to its verified less reliability in the mark extraction process, as it will be shown in Section 6.6.1.

In its simplest implementation, a QIM watermarking system associates each bit of a message $\mathbf{m}$, namely m_i, to a single host element w_i, and let m_i determine which quantizer has to be used to quantize w_i. Typically, the two codebooks $\mathcal{M}_0$ and $\mathcal{M}_1$ associated respectively to $m_i = 0$ and $m_i = 1$ are defined as:

$$\mathcal{M}_0 = \{u_{0,z} = z\xi + \chi, z \in \mathbb{Z}\}, \quad \mathcal{M}_1 = \{u_{1,z} = z\xi + \frac{\xi}{2} + \chi, z \in \mathbb{Z}\}, \tag{6.16}$$

where χ is a secret key and ξ the quantization step.

Watermark embedding is achieved by applying either the quantizer associated to $\mathcal{M}_0$ or the one associated to $\mathcal{M}_1$, depending on the bit m_i that has to be embedded, respectively:

$$\mathcal{Q}_0(w_i) = \arg \min_{u_{0,z} \in \mathcal{M}_0} |u_{0,z} - w_i|, \qquad \mathcal{Q}_1(w_i) = \arg \min_{u_{1,z} \in \mathcal{M}_1} |u_{1,z} - w_i|, \tag{6.17}$$

where $u_{0,z}$ and $u_{1,z}$, with $z \in \mathbb{Z}$, are the elements of $\mathcal{M}_0$ and $\mathcal{M}_1$ respectively. Indicating with w_i^m the marked element, we obtain:

$$w_i^m = \begin{cases} \mathcal{Q}_0(w_i), & m = 0, \\ \mathcal{Q}_1(w_i), & m = 1. \end{cases} \tag{6.18}$$

The complete marked sequence is indicated as $\mathbf{w}^m$. The watermarked signature image is then obtained by reversing the embedding procedure.

The watermark extraction is obtained by using a minimum distance decoder:

$$\tilde{m}_i = \arg \min_{m \in \{0,1\}} \min_{u_{m,z} \in \mathcal{M}_m} |u_{m,z} - \tilde{w}_i^m|, \quad z \in \mathbb{Z}, \tag{6.19}$$

being $\tilde{w}_i^m$ the i-th bit from the extracted marked sequence $\tilde{\mathbf{w}}^m$.

6.4 Feature Selection

As reported in Section 6.3.2, the marks which are embedded in the employed signature images contain the binary representation of L features mean values. Specifically, the selected dynamic features has to be represented through 92 bits-binary vectors, and then protected by employing a $(127, 92)$ BCH error correcting code.

The severe limit on the length of the considered binary strings force us to selecting only the L most representative dynamic features for the embedding. Specifically, two different approaches for the selection of the most reliable features of a given set, which therefore guarantee the best recognition performances, are provided in the following. Moreover, an algorithm which defines the minimum number of bits which should be assigned to a given feature, in order to not affect the recognition performances, will be proposed in Section 6.5.

It is worth pointing out that a procedure for the selection of the most reliable binarized features has already been proposed in Chapter 4, for the implementation of the proposed signature based cryptosystem. However, in the case here discussed, the dynamic features have to be binarized to be embedded in the signature images, but can be extracted and decoded during authentication, differently from what happens with the cryptosystem of Chapter 4. Then, it is preferable to define a feature selection procedure which tries to optimize the recognition performances of a system employing the Mahalanobis distance as matching module, and a binarization method which assign to each feature the minimum number of bits which allows to not degrade the recognition performances.

The effectiveness of the proposed approaches for feature selection and binarization will be discussed in Section 6.7.

6.4.1 Related Works

In the literature of biometrics, many efforts have been made to properly define the best set of features which should be extracted from a given characteristic. In fact, when dealing with parametric features, the proposed sets often contain features which are irrelevant or correlated with other features. This typically happens because many redundant features tend to be included in the employed sets, in order to avoid any loss of useful information. However, the use of unnecessary large sets of features can affect the recognition performances, as well as the processing time, and obviously the required space for their storage.

An algorithm for the selection of those features which offer the best representation of a speech sample has been proposed in [194], where genetic algorithms [195] are employed in conjunction with feed forward neural networks. An approach based on genetic algorithms, along with a method employing particle swarm optimization [196], has been proposed in [197] for the selection of relevant keystroke dynamics features. Moreover, a method based on mutual information and applied to the problem of human gait feature selection has been presented in [198].

As far as signature recognition is concerned, the problem of feature selection has been discussed in [199], where the selection of a unique set of features for each individual has been suggested, and in [200], where a modified version of the Fisher ratio has been employed as cost function for the selection of local and global signature parametric features. In [175], a statistical distance based on the difference between the mean values of different users' features has been defined. In [201], a cost function based on the Equal Error Rate (EER) has been employed to select a subset of signature features, while a consistency measure has been introduced in [202] to rank signature features according to their importance. An algorithm employed to rank a set of on-line signature parametric features has also been presented in [134], while the use of genetic algorithms has been proposed in [43] to select an optimal set of on-line signature features.

6.4.2 Employed Methodology

The approaches presented in this Thesis stems from the one proposed in [203], performing feature selection on the basis of the distance between genuine and forgers matching scores distributions. In fact, it is well known from pattern classification [204] that a properly defined feature selection stage should be designed using the classifier that is employed for the classification. Therefore, the presented approaches can be applied for the selection of the best parametric features extracted from any biometrics, having assumed that the matching module employed in the considered authentication system is based on the computation of the Mahalanobis distance. Instead of defining different sets of features for different users, as proposed in [199], the proposed approaches aim at the definition of a unique set of features which has to be employed for each enrolled user.

It is supposed that a training set of biometric acquisitions, taken from U different users, is available. Specifically, it is assumed that, for each user u, T genuine biometric samples are acquired, and that J forgery samples are also available. These latter samples can be biometric acquisitions taken from different users, or skilled forgeries specifically produced to emulate the biometrics of the considered user (as it can be done for behavioral biometrics such as signature or keystroke, but also for physiological biometrics which can be artificially reproduced, such as fingerprints or irises). The training data are employed to analyze the contribution of each feature in the recognition process.

For each user, K features are extracted from each of E genuine samples, selected among the T ones available in the training data set. The computed features are employed to estimate the mean and standard deviation vectors $\boldsymbol{\mu}^u[k]$ and $\boldsymbol{\sigma}^u[k]$, where $k \in \mathcal{K} = \{1, \ldots, K\}$ represents the feature index, with $K > L$, being L the number of the best features which have to be selected among the considered K. From the remaining $I = T - E$ genuine acquisitions, the feature vectors $\mathbf{g}_i^u[k]$, with $i = 1, \ldots, I$, are evaluated, whereas the feature vector extracted from the j-th forged sample of user u is indicated as $\mathbf{f}_j^u[k]$, $j = 1, \ldots, J$.

It is worth pointing out that the standard deviation $\boldsymbol{\sigma}^u[k]$ have to be computed accordingly to the approach followed during authentication: when a *common variance* approach, which has been discussed in Section 6.1.2, is employed, the standard deviation $\boldsymbol{\sigma}^u[k]$ should be taken, for each considered user, as the mean of all the variances computed during the training phase.

Employing the defined notations, an approach to determine a feature ranking, and an iterative approach which determines the best feature to add to an already given set, in order to improve its recognition capabilities, are described in Sections 6.4.3 and 6.4.4, respectively.

6.4.3 Feature Selection: Ranking Approach

The feature selection approach here proposed assigns a reliability measure to each feature, which can then be ranked accordingly: the features with the L highest reliability values are selected to efficiently represent the considered biometric. Considering a feature k, with $k \in \mathcal{K}$, the following distances are computed for each user u in the training set, $u = 1, \ldots, U$:

$$\mathbf{G}^u[i,k] = \frac{|\mathbf{g}_i^u[k] - \boldsymbol{\mu}^u[k]|}{\boldsymbol{\sigma}^u[k]}, i = 1, \ldots, I; \mathbf{F}^u[j,k] = \frac{|\mathbf{f}_j^u[k] - \boldsymbol{\mu}^u[k]|}{\boldsymbol{\sigma}^u[k]}, j = 1, \ldots, J. \tag{6.20}$$

Then, for each user u a distance $\boldsymbol{\vartheta}^u[k]$ between the distributions $\mathbf{G}^u[i,k]$ and $\mathbf{F}^u[j,k]$ is evaluated, employing one of the distances defined in Section 6.4.5. The reliability of the k-th feature is then computed by taking the median value $\boldsymbol{\lambda}[k]$ among the U values $\boldsymbol{\vartheta}^u[k]$, $u = 1, \ldots, U$. The features with the L highest values of $\boldsymbol{\lambda}[k]$ are considered to be the most representative for recognition purposes.

6.4.4 Feature Selection: Incremental Approach

The approach described in Section 6.4.3 analyzes the reliability of each considered feature, without considering any correlation between different features. However, in the most of cases the considered features are correlated, and therefore the selection of the best feature which can be added to a given set should be performed on the basis of the already selected features.

In order to take into account possible dependencies between the considered features, an incremental approach has also been implemented. Specifically, if a subset comprising the L most reliable features, out of the available K, has to be identified, the proposed procedure has to be run by iterating L times the algorithm detailed in the following.

Let us define with $\mathcal{L}_l$ the set of the selected features at step l, with $l = 1, \cdots, L$ and $\mathcal{L}_0$ defines the empty set at the initialization step. Let $\mathbf{\Delta} G_0^u[i,k]$ and $\mathbf{\Delta} F_0^u[j,k]$ the zero matrices of dimensions $I \times K$ and $J \times K$ respectively.

The generic l-th step of the proposed algorithm is defined as follows:

1. for each user u, with $u = 1, \cdots, U$, computation of $\mathbf{G}_l^u[i,k]$ and $\mathbf{F}_l^u[j,k]$, for $k \in \mathcal{K} \setminus \mathcal{L}_{l-1}$, where "\" is the difference operator, as:

$$\begin{aligned} \mathbf{G}_l^u[i,k] &= \sqrt{\left(\frac{\mathbf{g}_i^u[k] - \boldsymbol{\mu}^u[k]}{\boldsymbol{\sigma}^u[k]}\right)^2 + \mathbf{\Delta} G_{l-1}^u[i,k]},\ i = 1, \ldots, I; \\ \mathbf{F}_l^u[j,k] &= \sqrt{\left(\frac{\mathbf{f}_j^u[k] - \boldsymbol{\mu}^u[k]}{\boldsymbol{\sigma}^u[k]}\right)^2 + \mathbf{\Delta} F_{l-1}^u[j,k]},\ j = 1, \ldots, J; \end{aligned} \tag{6.21}$$

2. for each user u, with $u = 1, \cdots, U$, computation of the distances $\boldsymbol{\vartheta}_l^u[k]$ between $\mathbf{G}_l^u[i,k]$ and $\mathbf{F}_l^u[j,k]$ for $k \in \mathcal{K} \setminus \mathcal{L}_{l-1}$. The measures detailed in Section 6.4.5 are employed to evaluate the required distances;

3. for each feature $k \in \mathcal{K} \setminus \mathcal{L}_{l-1}$, evaluation of the median values $\boldsymbol{\lambda}_l[k]$ of the U values $\{\boldsymbol{\vartheta}_l^u[k]\}$;

4. selection of the feature $\tilde{k} \in \mathcal{K} \setminus \mathcal{L}_{l-1}$ which possesses the highest reliability value $\boldsymbol{\lambda}_l[\tilde{k}]$;

5. update the set of selected features as $\mathcal{L}_l = \mathcal{L}_{l-1} \bigcup \tilde{k}$;

6. for each user u, with $u = 1, \cdots, U$, update the matrices $\mathbf{\Delta} G_l^u$ and $\mathbf{\Delta} F_l^u$ as follows:

$$\begin{aligned} \mathbf{\Delta} G_l^u[i,k] &= \mathbf{\Delta} G_{l-1}^u[i,k] + \left(\frac{\mathbf{g}_i^u[\tilde{k}] - \boldsymbol{\mu}^u[\tilde{k}]}{\boldsymbol{\sigma}^u[\tilde{k}]}\right)^2 \cdot \mathbf{o}[k] \\ \mathbf{\Delta} F_l^u[j,k] &= \mathbf{\Delta} F_{l-1}^u[j,k] + \left(\frac{\mathbf{f}_j^u[\tilde{k}] - \boldsymbol{\mu}^u[\tilde{k}]}{\boldsymbol{\sigma}^u[\tilde{k}]}\right)^2 \cdot \mathbf{o}[k] \end{aligned} \tag{6.22}$$

   being $\mathbf{o}[k]$ a row vector with only ones, and "$\cdot$" the column-by-row multiplication operator, for every $k \in \mathcal{K} \setminus \mathcal{L}_l$.

7. if $l < L$ then $l = l + 1$, otherwise the iterations stop.

6.4.5 Distribution Distances

As already pointed out, both the proposed procedures for feature selection compute a distance between two distributions. In the proposed implementations, two different measures have been employed to evaluate the distance between the probability distributions B_X and B_Y of the score sets X and Y, respectively.

6.4.5.1 EER based Distance

The first employed distance $\Delta_{EER}(B_X, B_Y)$ is defined through the concept of EER. Specifically, having considered B_X as the score probability distribution obtained from the matching of authentic biometric samples, and B_Y as the score probability distribution obtained from the matching of forgeries, the resulting EER is then computed. The value of the distance $\Delta_{EER}(B_X, B_Y)$ is then set to $1 - EER$.

6.4.5.2 Kullback-Leibler based Distance

The second employed distance $\Delta_{KL}(B_X||B_Y)$ is based on the estimation of the score probability distribution B_X, obtained from the matching of authentic biometric samples, and the score probability distribution B_Y, obtained from the matching of forgeries. The Kullback-Leibler (KL) divergence between the two estimated densities is eventually computed. Specifically, the Parzen window estimator [205] with a Gaussian kernel, is employed to estimate B_X and B_Y. The distance $\Delta_{KL}(B_X||B_Y)$ is then obtained as

$$\Delta_{KL}(B_X||B_Y) = \sum_i B_X(i) \ln \frac{B_X(i)}{B_Y(i)}. \tag{6.23}$$

In Section 6.7 it will be shown that the proposed feature selection approaches lead to recognition rates, expressed in terms of EER, better than those obtained using the approach in [134].

6.5 Feature Binarization

In this Section, the method employed to determine the minimum number of bits which have to be assigned to a given feature, in order to not affect the achievable recognition performances, is detailed. As for the feature selection algorithm described in Section 6.4, it is assumed that a training set of biometric acquisitions, taken from U different users, can be analyzed. Using the notations introduced in Section 6.4.2, we first estimate the minimum and maximum value for a given feature k, $k \in \mathcal{K}$.

Specifically, the maximum and minimum allowable score values, $\mathbf{M}[k]$ and $\mathbf{m}[k]$, for the k-th feature are computed as follow. The $\alpha\%$ highest score values are discarded thus obtaining as maximum allowable value for the k-th feature $\boldsymbol{\zeta}[k]$. Then, the maximum allowable score value, $\mathbf{M}[k]$ is set as $\mathbf{M}[k] = \boldsymbol{\zeta}[k] + \eta|\boldsymbol{\zeta}[k]|$, where $\eta > 0$. Similarly, the minimum allowable score value $\mathbf{m}[k]$ for the k-th features is computed as $\mathbf{m}[k] = \boldsymbol{\varsigma}[k] - \eta|\boldsymbol{\varsigma}[k]|$, being $\boldsymbol{\varsigma}[k]$ the minimum score value obtained by discarding the $\alpha\%$ lowest scores. The parameters α and η are selected in order to limit the effects of possible outliers in the estimation of the maximum and minimum values of the given distribution. Once the allowed range for the score of the k-th feature has been determined, the following procedure is employed to verify whether a given number of bits b can be used to represent the mean value of the k-th feature, without affecting the achievable verification performances.

For each user u, the matrices $\mathbf{G}^u$ and $\mathbf{F}^u$, whose values are given in (6.20) are evaluated. The values $\boldsymbol{\mu}^u[k]$ are then binarized employing b bits for each element, taking into account that the k-th feature assumes values into the interval $[\mathbf{m}[k], \mathbf{M}[k]]$. The decoded version of the binarized k-th feature mean vector is indicated as $\boldsymbol{\nu}^u[k]$, and employed to determine the distances:

$$\mathbf{Gb}^u[i,k] = \frac{|\mathbf{g}_i^u[k] - \boldsymbol{\nu}^u[k]|}{\boldsymbol{\sigma}^u[k]}; \quad \mathbf{Fb}^u[j,k] = \frac{|\mathbf{f}_j^u[k] - \boldsymbol{\nu}^u[k]|}{\boldsymbol{\sigma}^u[k]}. \tag{6.24}$$

For each user u, a measure representing the goodness of the employed binarization is then computed as:

$$\boldsymbol{\omega}_b^u[k] = \frac{1}{I}\sum_{i=1}^{I}(\mathbf{G}^u[i,k] - \mathbf{Gb}^u[i,k]) - \frac{1}{J}\sum_{j=1}^{J}(\mathbf{F}^u[j,k] - \mathbf{Fb}^u[j,k]). \tag{6.25}$$

In fact, it can be observed that if the term $\frac{1}{I}\sum_{i=1}^{I}(\mathbf{G}^u[i,k] - \mathbf{Gb}^u[i,k])$ is positive, the binarization of the k-th feature will result in an improvement of the recognition performances. Similarly, an improvement of the recognition accuracy will be obtained if the term $\frac{1}{J}\sum_{j=1}^{J}(\mathbf{F}^u[j,k] - \mathbf{Fb}^u[j,k])$ is negative. Therefore, once the terms $\boldsymbol{\omega}_b^u[k]$ have been computed for each available user u, a quality measure for the binarization of the k-th feature with b bits can be obtained as:

$$\boldsymbol{\Omega}_b[k] = \frac{\sum_{u=1}^{U}\boldsymbol{\omega}_b^u[k]}{U}. \tag{6.26}$$

If $\mathbf{\Omega}_b[k] < 0$, the binarization of the mean values of feature k with b bits, for each enrolled user, will result in a performance degradation. When $\mathbf{\Omega}_b[k] \simeq 0$ the recognition performances are not affected by the binarization, and could be even improved if $\mathbf{\Omega}_b[k] > 0$. The minimum number of bits which can be employed in order to binarize the k-th feature is therefore obtained as the lowest value b for which steadily results $\left|\mathbf{\Omega}_b[k]\right| < \epsilon$, where ε is a predefined threshold, with $\varepsilon \simeq 0$.

6.6 Experimental Results

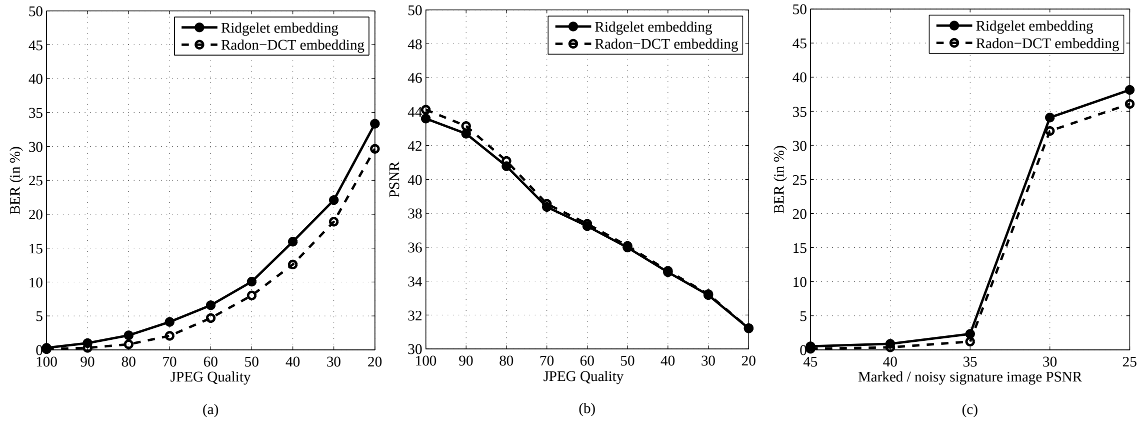
In this Section, an extensive set of experimental results, concerning the performances of the proposed watermarking based signature authentication system, are presented. Specifically, the system performances are characterized in terms of:

- the robustness of the employed Radon-DCT watermarking method, which is also compared with the capabilities of the embedding in the ridgelet domain;

- the effectiveness of the proposed feature selection approaches, which are compared with the method described in [134];

- the effectiveness of the proposed feature binarization method;

- the authentication capabilities of the proposed architecture, evaluated when considering both a system which stores individual variances for each enrolled user, as well as a system where common standard deviations for each enrolled user are employed for the extracted static and dynamic features, in order to evaluate the matching scores in equation (6.2). In this latter case, the employed common standard deviations are evaluated as the mean values od the standard deviations of the features extracted from a training set of signatures. The performances achievable using static or dynamic features separately, as well as the performances achievable by combining them, are evaluated.



(a)

(b)

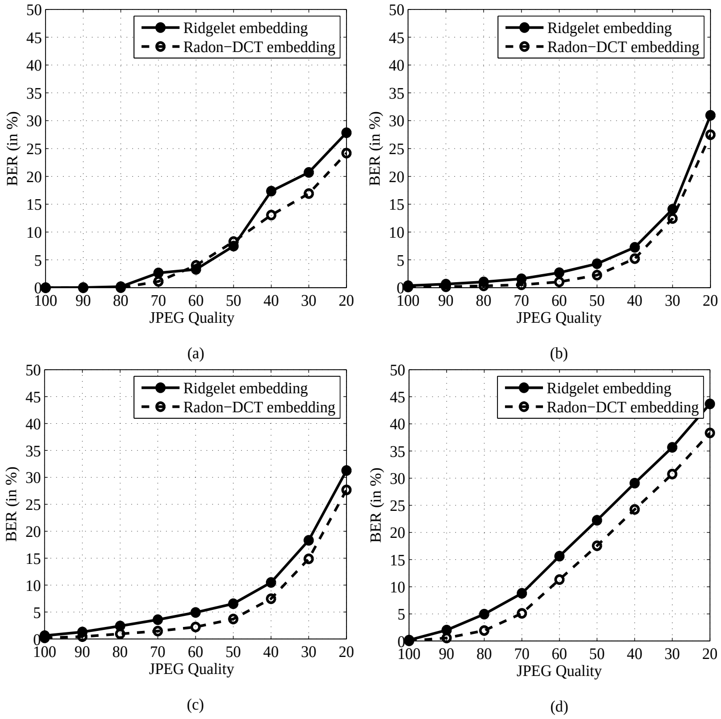
(c)

Figure 6.3: Mark extraction performances, considering $P = 10$ pixels, $T_E = 5$, $N = 6$ and $\xi = 100$. (a): BER vs. JPEG quality level; (b): BER vs. marked and noisy image PSNR; (c): PSNR vs. JPEG quality level.

6.6.1 Mark Extraction

The performances of the proposed embedding method is evaluated on the basis of the public MCYT database, which comprises 2500 genuine signatures taken from 100 different users. The embedding is performed using binary marks of 127 bits which, in our case, represent the BCH encoded dynamic features extracted from the acquired signature. Some attacks, like JPEG compression and additive random Gaussian noise, have been performed on the watermarked signature images for testing the robustness of the proposed embedding methods. Moreover, we have tested the performances of the embedding methods varying the system's parameters P and T_E, being respectively the blocks dimension and the threshold for the blocks selection. These experiments are conducted trying to keep the number of coefficients selected for the embedding constant.

Figure 6.3 shows the performances obtained when embedding marks in the proposed R-DCT domain, in terms of the Bit Error Rate (BER) noticed during mark extraction. Moreover, a comparison with the performances achievable when employing the ridgelet embedding domain is also provided. Specifically, Figure 6.3(a) shows the obtained BER as a function of the JPEG quality of the marked image. Figure 6.3(b) shows the Peak Signal-to-Noise Ratio (PSNR) between the original and the JPEG compressed marked signature: marked signatures are very similar to the original ones, and their differences are visually



(a)

(b)

(c)

(d)

Figure 6.4: BER vs. JPEG quality for the four second level subbands, considering $P = 10$ pixels, $T_E = 5$ and $N = 6$. (a): 2LL subband; (b): 2HL subband; (c): 2LH subband; (d): 2HH subband.

undetectable. Figure 6.3(c) shows the BER obtained when considering marked images with Gaussian noise added, as a function of the PSNR between the marked and the noisy signature images. As can be seen, overall better performances, both in terms of robustness and PSNR, are obtained when the mark embedding is performed in the novel R-DCT domain, with respect to an embedding performed in the ridgelet domain.

Figure 6.4 shows the BERs obtained when considering separately each second level subband. The approximation subband $2LL$ performs better than the others for JPEG quality greater than 80, and as well as the subbands $2HL$ and $2LH$ for lower JPEG qualities. As mentioned earlier, the subband $2HH$ is the less reliable embedding subband.

Moreover, Figure 6.5 shows how the mark extraction performances vary with respect to the blocks dimension P. Figure 6.5(a) presents the BER for the ridgelet and R-DCT embedding methods, when considering images compressed with a JPEG quality equal to 90. Figure 6.5(b) is related to marked images with Gaussian noise added, considering a

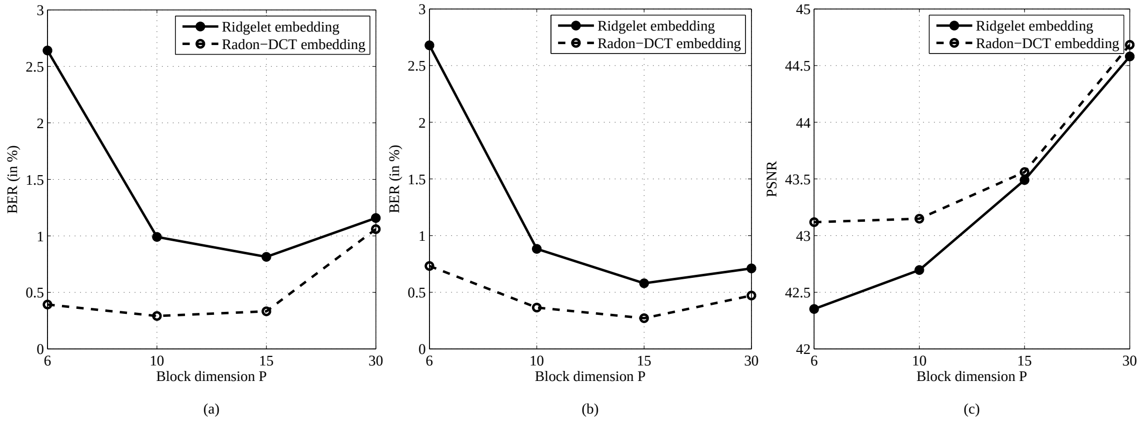
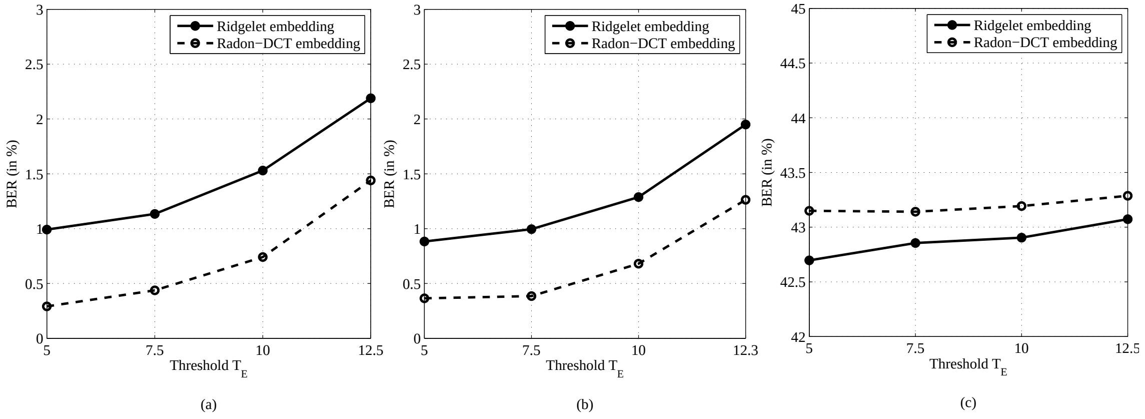


Figure 6.5: Mark extraction performances varying the blocks dimension P. (a): BER for marked signature images with JPEG quality equal to 90; (b): BER for marked signature images with Gaussian noise added, with a PSNR equal to 40 dB; (c): PSNR between the original and the marked image compressed with quality equal to 90.

PSNR equal to 40 dB. Figure 6.5(c) shows the behavior of the PSNR between the original and the marked signature image, compressed with JPEG quality equal to 90: the PSNR improves when a greater blocks dimension P is employed. However, the best performances in terms of BER are obtained when taking $P = 10$ or $P = 15$ pixels.

Finally, Figure 6.6 illustrates the system performances with respect to the threshold T_E, employed in equation (6.12) . Figure 6.6(a) refers to marked images compressed with a JPEG quality equal to 90, while Figure 6.6(b) is related to marked images with Gaussian noise added, considering a PSNR equal to 40 dB. Figure 6.6(c) shows the PSNR between the original and the marked signature image, compressed with JPEG quality equal to 90. As can be seen, the best performances are obtained with the value $T_E = 5$.

Tests on the mark extraction capability of the proposed embedding domain have also been performed considering images compressed with the JPEG2000 algorithm. However, in this case a noticeable BER (greater than 5%) can be observed only when selecting JPEG2000 compressions with extremely low qualities. It can be therefore concluded that the proposed approach is robust to the most common processing which signature images can undergo.



(a)

(b)

(c)

Figure 6.6: Mark extraction performances varying the threshold T_E for the blocks selection. (a): BER for marked signature images with JPEG Quality equal to 90; (b): BER for marked signature images with Gaussian noise added, with a PSNR equal to 40 dB; (c): PSNR between the original and the marked image compressed with quality equal to 90.

6.7 Feature Selection and Binarization

In order to test the proposed feature selection and binarization approaches, the training and test data sets, obtained from the public version of the MCYT on-line signature corpus, are considered. Specifically, the training set with 30 users is employed to select the best dynamic and static features, and also to determine the number of bits which has to be assigned for the binarization of the mean values of each selected dynamic feature. The ability of the proposed methods in providing reliable results is tested evaluating the recognition performances achievable over the signature test data set, when employing the features and the bit depths estimated over the training set.

As for the feature selection approaches, the skilled forgeries available in the training set are employed to generate the feature vectors $\mathbf{f}_j^u[k]$, $j = 1, \ldots, 25$ and $u = 1, \ldots, 30$, employed in the methods described in Section 6.4 to represent the forgeries distributions.

A feature set comprising 88 dynamic features, extracted from the set presented in Section 4.2 while discarding those related to static information, is employed to test the proposed feature selection algorithms. The list of employed dynamic features is reported in Table 6.2.

Index	Description	Index	Description	Index	Description
1	signature total duration T_s	30	N($v_x = 0$)	59	(1st $t(v_{x,max})$)$/T_w$
2	N(pen-ups)	31	direction histogram s_1 [174]	60	(centripetal acceleration rms a_c)$/a_{max}$
3	N(sign changes of dx/dt and dy/dt)	32	$(y_{2nd\ localmax} - y_{1st\ pen-down})/\Delta_y$	61	θ(1st pen-down to 2nd pen-down)
4	average jerk $\overline{j}$ [173]	33	$(y_{1st\ pen-down} - x_{max})/\Delta_x$	62	θ(1st pen-down to 2nd pen-up)
5	standard deviation of a_y	34	$T(curvature > Threshold_{curv})/T_w$	63	direction histogram s_7
6	standard deviation of v_y	35	(integrated abs. centr. acc. a_{Ic})$/a_{max}$ [174]	64	$t(j_{x,max})/T_w$
7	N(local maxima in x)	36	$T(v_x > 0)/T_w$	65	$j_{x,max}$
8	standard deviation of a_x	37	$T(v_x < 0 \vert pen - up)/T_w$	66	θ(1st pen-down to last pen-up)
9	standard deviation of v_x	38	$T(v_x > 0 \vert pen - up)/T_w$	67	θ(1st-pen down to 1st pen-up)
10	j_{rms}	39	$(x_{3rd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	68	(1st $t(x_{max})$)$/T_w$
11	N(local maxima in y)	40	$N(v_y = 0)$	69	$\overline{j}_x$
12	$t(2ndpen - down)/T_s$	41	(acceleration rms a)$/a_{max}$	70	T(2nd pen-up)$/T_w$
13	(average velocity $\overline{v}$)$/v_{x,max}$	42	$\frac{T((dx/dt)/(dy/dt)>0)}{T((dx/dt)/(dy/dt)<0)}$	71	(1st $t(v_{max})$)$/T_w$
14	$(x_{lastpen-up} - x_{max})/\Delta_x$	43	(tangential acceleration rms a_t)$/a_{max}$	72	$j_{y,max}$
15	$(x_{1st\ pen-down} - x_{min})/\Delta_x$	44	$(x_{2nd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	73	θ(2nd pen-down to 2nd pen-up)
16	$(y_{last\ pen-up} - y_{max})/\Delta_y$	45	$T(v_y < 0 \vert pen - up)/T_w$	74	j_{max}
17	$(y_{1st\ pen-down} - y_{min})/\Delta_y$	46	direction histogram s_2	75	(1st $t(v_{y,min})$)$/T_w$
18	$(T_w\overline{v})/(y_{max} - y_{min})$	47	$t(3rd\ pen - down)/T_s$	$76 - 77$	(2st $t(x_{max})$)$/T_w$; (3rd $t(x_{max})$)$/T_w$
19	$(T_w\overline{v})/(x_{max} - x_{min})$	48	$(y_{3rd\ local\ max} - y_{1st\ pen-down})/\Delta_y$	78	(1st $t(v_{y,max})$)$/T_w$
20	(pen-down duration T_w)$/T_s$	49	direction histogram s_5	79	$t(j_{max})/T_w$
21	$\overline{v}/v_{y,max}$	50	direction histogram s_3	80	$t(j_{y,max})/T_w$
22	$(y_{last\ pen-up} - y_{max})/\Delta_y$	51	$T(v_x < 0)/T_w$	81	direction change histogram c_2
23	$\frac{T((dy/dt)/(dx/dt)>0)}{T((dy/dt)/(dx/dt)<0)}$	52	$T(v_y > 0)/T_w$	82	(3rd $t(y_{max})$)$/T_w$
24	$\overline{v}/v_{max}$	53	$T(v_y < 0)/T_w$	83	direction change histogram c_4
25	$(y_{1st\ pen-down} - y_{max})/\Delta_y$	54	direction histogram s_8	84	$\overline{j}_y$
26	$(y_{last\ pen-up} - x_{min})/\Delta_x$	55	(1st $t(v_{x,min})$)$/T_w$	85	direction change histogram c_3
27	(velocity rms v)$/v_{max}$	56	direction histogram s_6	86	θ(initial direction)
28	(velocity correlation $v_{x,y}$)$/v^2_{max}$ [174]	57	T(1st pen-up)$/T_w$	87	θ(before last pen-up)
29	$T(v_y > 0 \vert pen - up)/T_w$	58	direction histogram s_4	88	(2nd $t(y_{max})$)$/T_w$

Table 6.2: Dynamic features extracted from on-line signatures.

The results obtained when considering $E = 10$ signatures for the enrollment phase are shown in Figure 6.7. Specifically, Figure 6.7(a) shows the comparison between the methods described in Section 6.4.3 and 6.4.4, employing both the distances defined in Section 6.4.5.1. The results are displayed in terms of the EER, evaluated over the test set with 70 users and considering skilled forgeries, versus the number of employed features. The obtained results illustrate how the use of the incremental procedure of Section 6.4.4 performs better than the ranking based one. This means that the employed features are highly correlated. The selection of a feature therefore cannot be made regardless of the already selected ones. Figure 6.7(b) shows the comparison between the incremental approach presented in Section

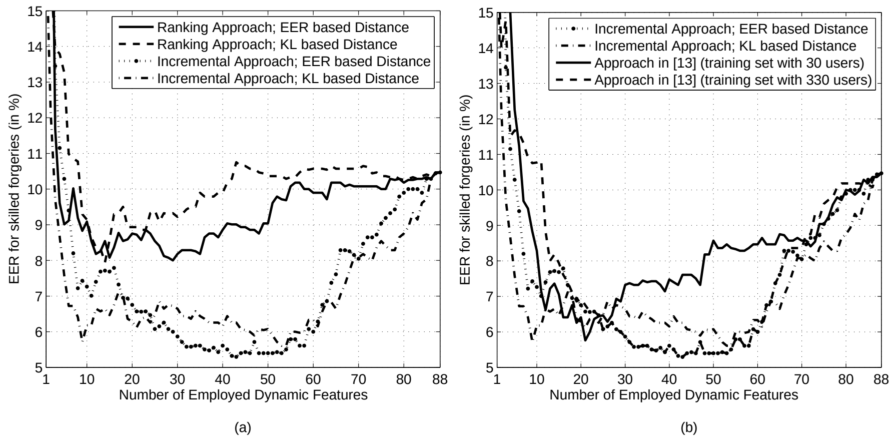


Figure 6.7: Application of the proposed feature selection approaches to dynamic signature features, for $E = 10$. (a): Comparison between the approaches in Section 6.4.3 and 6.4.4; (b): Comparison between the approaches in Section 6.4.4 and in [134].

6.4.5.2, and the feature selection method presented in [134]. Specifically, this latter approach is applied by performing its feature selection procedure over the training data set with $U = 30$ users, and then evaluating the recognition performances over the test data set. It can be seen that the proposed incremental methods performs significantly better than the one in [134]. Moreover, the proposed approach is also compared with the feature ranking presented in [134], which has been estimated employing the whole MCYT database with 330 user as training set. The incremental procedure described in Section 6.4.4 still performs better when considering the selection of few features, and allows to reach the same lowest EER which can be achieved employing the feature ranking presented in [134], that is equal to 5.4%.

The same comparisons between different feature selection methods are also carried out considering a set comprising 68 static features, which are listed in Table 6.3. These static features can be extracted from static representation of the signature, that is, from the images employed in the proposed multi-level signature based authentication system.

As can be seen, both global (the first 20) and local features (the last 48) are considered in the employed set. The local features are evaluated by dividing each signature image, of dimension 720 × 1440 pixels in the proposed implementation, in 12 equal-sized rectangular segments [91]. The statistical moments M_{rz} in Table 6.3 are defined as $M_{r,z} = \sum_{c=1}^{C} x_c^r y_c^z$,

Index	Description
1	Sample Count
2-4	Height, Width and Aspect Ratio
5-7	Minimum, Mean and Maximum X Position
8-10	Minimum, Mean and Maximum Y Position
11-12	X and Y Area
13-17	Statistical Moment $M_{1,1}$,$M_{1,2}$,$M_{2,1}$,$M_{0,3}$,$M_{3,0}$
18-20	Minimum, Mean and Maximum Pressure Value
21-32	Mean Pressure 12-segment
33-44	Sample Count 12-segment
45-68	X and Y Area 12-segment

Table 6.3: Static features extracted from each signature image.

where C is the number of samples in a signature image, and x, y are the coordinates of a signature image sample. 15 features out of 68 are related to the signature pressure, typically considered as an on-line characteristic. In fact, as reported in Section 6.1, the employed images are gray-scale, providing the signature pressure values as the hosts of the embedded watermarks.

The results obtained by applying the proposed approaches to static features, when considering $E = 10$ signatures for the enrollment phase, are illustrated in Figure 6.8, which still validates the effectiveness of the proposed approaches.

The proposed feature binarization process is then evaluated by selecting, with the proposed incremental feature selection approach of Section 6.4.4 with the distribution distance based on the KL divergence, the 17 most reliable dynamics features, out of the considered 88 ones. The feature binarization approach described in Section 6.5 is employed to represent the 17 selected dynamics features with 92 bits, as requested by the proposed watermarking based signature recognition system, and as discussed in Section 6.3.2.

The necessary bit-depths have been estimated over the training set with 30 users. The employed parameters are $\alpha = 0.01$ and $\eta = 0.2$. The behavior of the quality measure $\boldsymbol{\Omega}_b$, introduced in Section 6.5, is illustrated in Figure 6.9(a) for two selected dynamic features. According to what has been explained in Section 6.5, the mean values of the feature "stan-

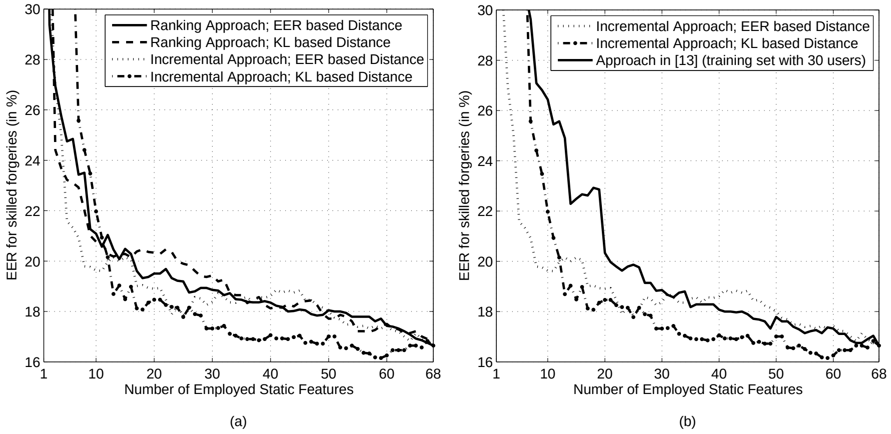


Figure 6.8: Application of the proposed feature selection approaches to static signature features, for $E = 10$. (a): Comparison between the approaches in Section 6.4.3 and 6.4.4; (b): Comparison between the approaches in Section 6.4.4 and in [134].

dard deviation of a_x" (defined in [134]) can be binarized employing 7 bits, while the mean values of the feature "$T(v_x < 0|\text{pen-up})/T_w$" (defined in [134]) can be represented employing only 4 bits. The effectiveness of the proposed binarization approach is verified by analyzing the recognition performances computed over the test data set with 70 users, while employing 17 dynamic features. Specifically, the performances obtained employing real-valued mean vectors $\boldsymbol{\mu}^u[k]$ to represent the intra-class mean are compared in Figure 6.9(b) with those achievable employing vectors $\boldsymbol{\nu}^u[k]$, generated from the binary representation of the considered dynamic features.

The reported Receiver operating Characteristic (ROC) curves, computed considering the False Acceptance Rate for skilled forgeries (FAR_{SF}), are not affected by the proposed binarization, even if the employed 17 dynamic features are represented with only 92 bits.

It is worth pointing out that the same amount of bits were employed by the author in [63] to represent only 11 dynamic features. Keeping fixed the number of employed bits (92), the number of employable bits increases by a factor of 55% by employing the proposed feature binarization procedure, with respect to the assignment used in [63].

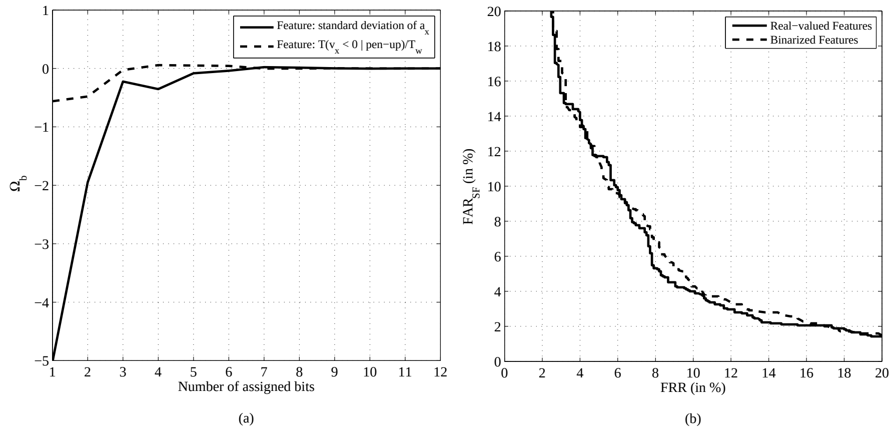


Figure 6.9: Analysis of the proposed feature binarization approach. (a): Quality measure $\mathbf{\Omega}_b$ with respect of the number of employed bits, for two considered dynamic features; (b): Effectiveness of the proposed binarization method, verified over the test data set employing 17 dynamic features.

6.7.1 Authentication System Performance

Finally, in order to test the authentication performances of the proposed security-scalable signature based authentication system, the following scenarios are considered:

- an authentication system where $E = 5$ signatures are recorded for each user during enrollment, and where individual feature variances for each user are stored in the system, and employed in the matching module based on the Mahalanobis distance;
- an authentication system where $E = 5$ signatures are recorded for each user during enrollment, and where feature variances common for all the considered users are stored in the system, and employed in the matching module based on the Mahalanobis distance;
- an authentication system where $E = 10$ signatures are recorded for each user during enrollment, and where individual feature variances for each user are stored in the system, and employed in the matching module based on the Mahalanobis distance;
- an authentication system where $E = 10$ signatures are recorded for each user during enrollment, and where feature variances common for all the considered users are

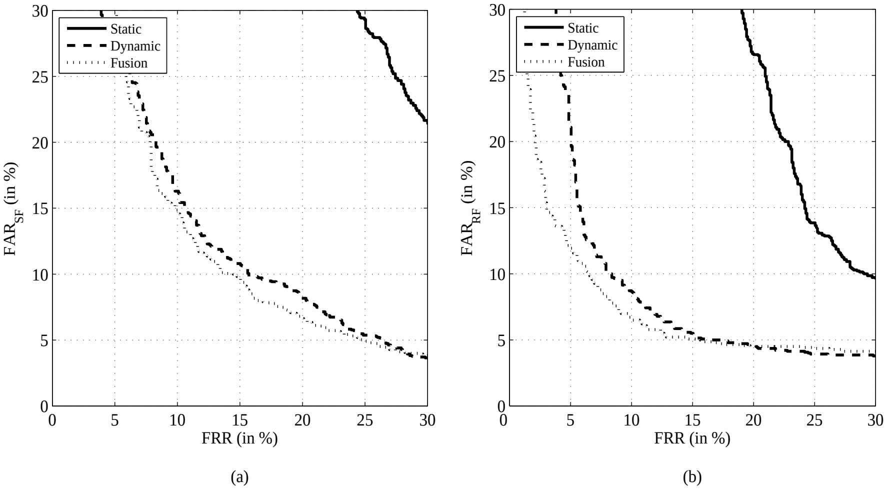


Figure 6.10: Performance of the proposed multi-level on-line based signature authentication system, using $E = 5$ signatures for the enrollment, with individual variances for each user.

stored in the system, and employed in the matching module based on the Mahalanobis distance;

Depending on the scenario taken into account, the proposed feature selection and binarization methods are accordingly implemented, in order to replicate the matcher employed during authentication. In fact, as already mentioned, a well known learning from pattern recognition states that a properly defined feature selection stage should be performed using the classifier employed for classification.

For each considered scenario, the 17 most representative dynamic features, out of the 88 listed in Table 6.2, are selected according to the incremental feature selection method described in Section 6.4.4. The chosen features are then represented with 92 bits, following the approach presented in Section 6.5. As for the static features, 50 parameters, out of the considered 68 of Table 6.3, are selected to represent each signature image, by employing the incremental feature selection approach described in Section 6.4.4. More in detail, the distribution distance based on the KL divergence, presented in Section 6.4.5.2, is used during feature selection for the systems employing individual variances for each user. On the other hand, the distribution distance based on the computation of EER, presented in Section 6.4.5.1, is used during feature selection for the systems employing a common feature

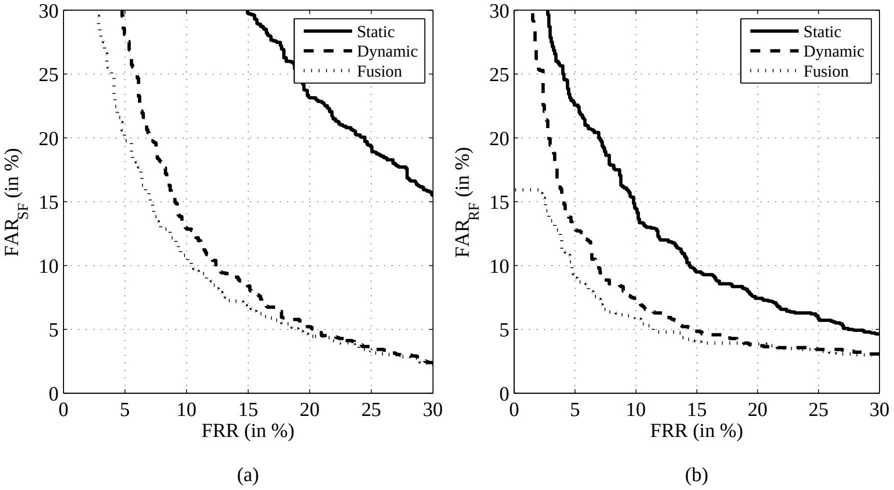


Figure 6.11: Performance of the proposed multi-level on-line based signature authentication system, using $E = 5$ signatures for the enrollment, with common variances for each user.

variance for each user.

The insertion of the binarized dynamic features into the signature images is performed employing the proposed Radon-DCT embedding domain. As it has been showed by the results presented in Section 6.6.1, embedding data in the proposed R-DCT domain results in better mark extraction performances, with respect of the use of the ridgelet embedding domain. Moreover, it is also worth pointing out that, thanks to the fact that the PSNR of the images marked in the R-DCT domain is high, the static features extracted from a marked image are basically the same which can be extracted from a unmarked one. The employed watermarking technique thus allows to use the marked signature images for recognition purposes, even if the considered images are compressed with a JPEG quality value equal to 80.

The ROC curves reported in Figures 6.10-6.13, referred to the comparison between False Rejection Rate (FRR) and False Acceptance Rate considering skilled forgeries (FAR$_{SF}$), show the systems performances achieved for the considered scenarios. Specifically, the performances achievable employing only the 50 selected static features, as well as the performances achievable employing only the 17 selected dynamic features, are illustrated for each considered case. Moreover, the *min-max* normalization technique described in Section 5.3.2.3, together with the *sum* rule for the fusion of normalized scores, is employed

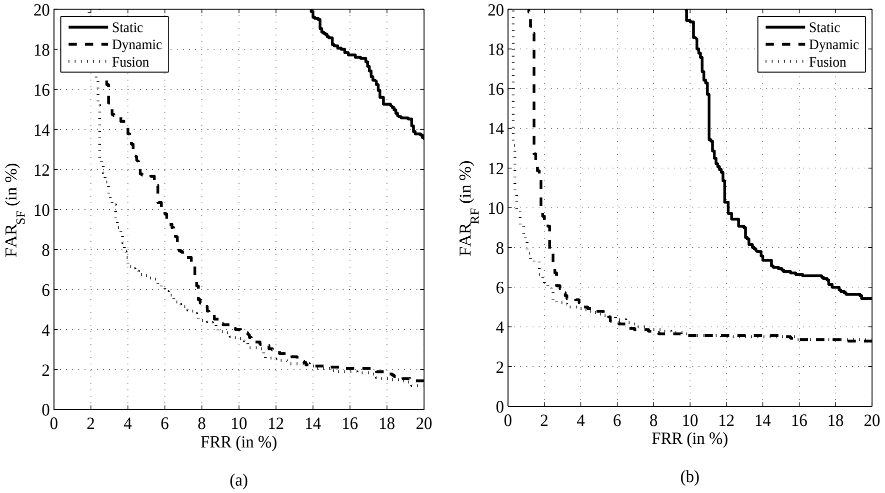


Figure 6.12: Performance of the proposed multi-level on-line based signature authentication system, using $E = 10$ signatures for the enrollment, with individual variances for each user.

to combine the dissimilarity measures obtained when matching static and dynamic feature vectors. As already remarked in this Thesis, the parameters needed for the implementation of the min-max normalization technique have been estimated using the training data set, and later applied to fuse the authentication scores obtained over the test data set.

The recognition results which can be obtained for the different considered scenarios are summarized in Table 6.4, which illustrates the achieved EERs, with reference to the use of skilled forgeries.

As it can be expected, the recognition rates achievable when employing $E = 10$ signatures during enrollment are far better than those obtained when taking only $E = 5$ signatures. Moreover, the combination of dynamic and static features always produce better results, when compared to the use of static or dynamic features by themselves. However, the obtained improvement, with respect to the performances related to the use of only dynamic features, can be significantly appreciated only when $E = 10$. This is due to the fact that, in the proposed architecture, for each user a single image is taken as representative of his static signature features. Although the signature selected as the host of the mark is the one, among those acquired during enrollment, whose static features are the closest to the estimated mean, the verification performances achievable using a single signature as template for the static features are significantly worse than those obtained with 17 dynamic

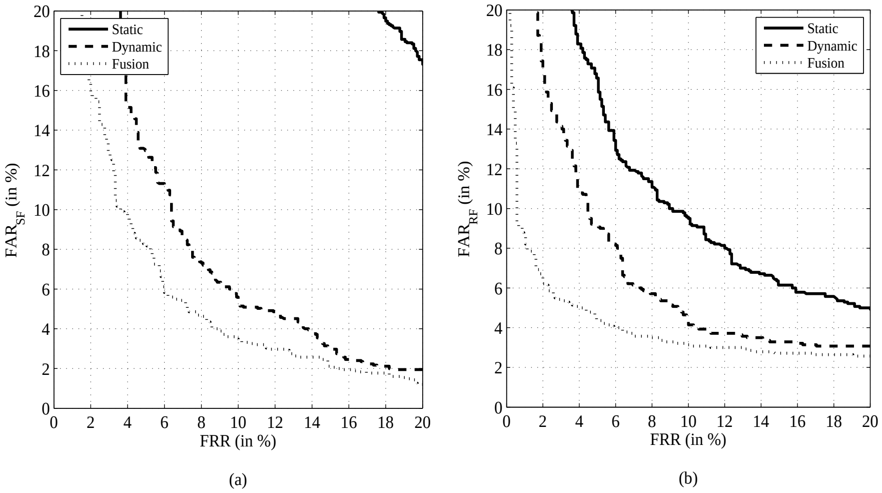


Figure 6.13: Performance of the proposed multi-level on-line based signature authentication system, using $E = 10$ signatures for the enrollment, with common variances for each user.

features. The great disparity in verification performance between static and dynamic features does not allow to produce outstanding improvements from the combination of both features types.

An interesting result can be observed when comparing the results obtained by employing individual features variances for each user, with those obtained when using common variances for each enrolled users. In fact, there is not a significant difference from the performances obtained following the two approaches. When taking $E = 5$ signatures from each user during enrollment, the results obtained when considering common variances are even better than those achieved by employing individual variances. It can then be argued that a system employing common feature standard deviations for each user, thus storing less sensitive information about each enrolled subject, can be efficiently employed for the deployment of real world applications. Obviously, the cardinality of the training set which is employed for the estimate of such variances should be enough large (it comprises signatures taken from 30 users, in the proposed implementation).

Scenario	static features	dynamic features	fusion
$E = 5$, individual variances	26.81	12.18	11.81
$E = 5$, common variances	21.94	11.23	10.40
$E = 10$, individual variances	17.07	7.43	5.99
$E = 10$, common variances	18.82	7.56	5.99

Table 6.4: EERs (expressed in %) achieved for the different considered scenarios, when dealing with skilled forgeries.

6.8 Security-scalable watermarking based system: Discussion

In this Chapter, a multi-level signature authentication system, where watermarking techniques are employed to hide and keep secret some dynamic signature features in a static representation of the signature itself, is proposed. User authentication can be performed according to two different security levels: the marked signature images can be used to guarantee a low security level, letting their static characteristics being analyzed by automatic algorithms or security attendants, while the embedded dynamic features can be extracted and used, by themselves or together with the static ones, to provide a higher level of security.

In order to define a robust watermarking approach, tailored to images representing signatures, the properties of the Radon transform are exploited, and a novel embedding domain, called Radon-DCT, is then defined. Moreover, in order to employ only the most reliable dynamic features for generating the marks, and to represent the considered features with the less possible number of bits, a feature selection procedure, along with a novel feature binarization procedure, are presented.

Extensive experimental results are provided to show the effectiveness of the proposed methods. Specifically, the capabilities of the presented approaches for the embedding of binary strings into signature images, and for the selection of the most discriminative features out of a given set, are compared to other approaches already proposed in literature, resulting in overall better performances.

Eventually, it has been shown how it is possible to perform efficiently users verification by employing features standard deviations common for all the enrolled subject, instead of using individual variances for each of them. This possibility allows to improve the security of the considered system, being possible to store less sensitive information regarding the biometric characteristics of the involved users.

Chapter 7

Conclusions and Future Work

In this Thesis, we investigate the security and privacy issues which have to be taken into account when designing a biometric based recognition system, and propose three different architectures which allow to employ protected signature templates when performing people authentication.

The unauthorized acquisition of the employed biometric data is probably the most dangerous threat concerning biometric based recognition systems, and can significantly affect the users' privacy and security. In fact, if a biometric template is stolen, the user's biometric can be easily replicated and misused by the attacker. Moreover, being the individuals' biometric traits limited in number, a user cannot renew or reissue his biometrics as he could do with a password or a token. It is also worth pointing out that biometric data can contain relevant information regarding people personality and health: if this information is misused, the users' privacy is unavoidably compromised.

The presented work is focused on the protection of signature templates. People recognition based on signatures is one of the most accepted biometric based authentication methods since, being part of everyday life, it is perceived as a non-invasive and non-threatening process by the majority of the users. Moreover, signature has a high legal value, since it has always played the role of document authentication, and it is accepted both by governmental institutions as well as for commercial transactions as a mean of identification. Although the necessity of providing protection to the signature templates employed in a system can be argued, due to the fact that an individual can change and reissue his signature when compromised, it is worth pointing out that such a procedure requires a significant effort by the user, and it would result in a significant loss in verification performance for the considered system. In fact, as it can be expected from a behavioral biometrics, different signature realizations, taken from the same user, usually exhibit a lot of variability, mainly due to lack of user's habit in the act of signing, as well as to different conditions of execution. This variability obviously increases if a user has to be recognized by means a signature with which he is not used to. Moreover, due to signature's high legal value, the loss of a signature template can result in unpleasant legal involvements.

In this Thesis we investigate how to provide protection to already proposed signature based recognition systems. Specifically, we consider authentication approaches belonging to all the three possible categories of signature recognition, that is, based on global signature features, on the local analysis of functional signature features, and on the regional analysis of functional signature feature. We then define the protection schemes which best suit to the characteristics of each of these approaches: a biometric cryptosystem is designed to protect the parametric features extracted from a signature, whereas a feature transformation approach is implemented in order to secure the functional features employed in local and regional based verification methods. Eventually, a watermarking based approach is designed in order to hide signature dynamic features in a static image of the signature itself, thus realizing a multi-level signature based recognition system.

7.1 Conclusions

A user adaptive cryptosystem is proposed in order to provide protection and renewability to signature templates consisting of global parametric features. Error correcting codes are employed both to provide the desired security, as well as to manage the intra-class variability of the extracted templates. The original raw data, as well as the template derived from them, cannot be reconstructed from the stored information, thus increasing the system security against possible attacks, while allowing to perform user authentication with performances comparable to an unprotected system. Moreover, the error correcting capabilities of the considered codes can be selected with dependence on the characteristics of each user, thus increasing the achievable recognition performances. The reported experimental results show that the proposed system is able to guarantee verification performances comparable with those achievable in an unprotected system, and that it also outperforms other well know signature based cryptosystems, already proposed in literature.

A feature transformation approach is also proposed for the protection of the signature templates employed in functional features based verification systems. The basic idea of the proposed schemes is to transform the original time dependent signature sequences through non-invertible transforms based on convolutions between random sequence segments. A baseline approach, together with two extended versions of the baseline method, are introduced. The security of the proposed approaches relies on the difficulty to solve a blind deconvolution problem, and it is analyzed in detail also for a scenario where an attacker is able to steal more than a single signature template (record multiplicity attack).

The proposed protection approaches are applied both to an on-line signature based authentication system employing a regional based matchers (exploiting HMM), as well to a system employing a local based matchers (using DTW). Moreover, the recognition rates achievable when combining regional and local matchers, by means of score level fusion techniques, are also discussed. The performances of various protected configurations are compared with those of unprotected systems, showing a very slight loss of performance in terms of EER for the protected schemes. The ability of generating multiple templates from the same original data, while respecting the needed diversity property for cancelable templates, is also deeply investigated.

Eventually, a multi-level signature authentication system, where watermarking techniques are employed to hide and keep secret some dynamic signature features in a static representation of the signature itself, is proposed. The proposed system can perform user authentication by employing only static signature images, when a low security level is needed, or by using the dynamic signature features embedded in the signature image, when a high security level is desired.

A robust watermarking approach, tailored to images representing signatures, is defined employing the properties of the Radon transform, by combining it with the Discrete Cosine Transform. Moreover, in order to employ only the most reliable dynamic features for generating the marks, and to represent the considered features with the less possible number of bits, a feature selection procedure, along with a novel feature binarization procedure, are presented. The reported experimental results testify the effectiveness of the proposed watermarking procedure, as well of the employed feature selection and binarization procedures. Moreover, it has been shown that it is possible to perform efficiently users verification by employing features standard deviations common for all the enrolled subject, instead of using individual variances for each of them. This possibility allows to improve the security of the considered system, being possible to store less sensitive information regarding the biometric characteristics of the involved users.

7.2 Future Work

The definition of cancelable biometrics, that is, protection schemes which allow to perform biometric recognition in a protected domain, is an emerging research field whose importance is due to the several privacy and security issues which arise when employing biometric data for authentication purposes.

When defining a novel protection scheme, the requirements of security, renewability and performances always have to be taken into account. However, properly defining a protection scheme which optimizes all the desired properties is still an open and hard to solve problem, due to the intrinsic intra-class variability of biometric acquisitions. For example, when considering the approaches presented in this paper, the proposed signature cryptosystem can be considered optimum from the point of view of security and renewability, although it cannot guarantee outstanding recognition rates, being the template matcher based on a simple Hamming distance between binary vector. On the other hand, the proposed feature transformation approach is significantly promising from the point of view of achievable recognition performances, being possible to employ it with sophisticated matching strategies such as DTW and HMM; however, it is difficult to deterministically evaluate its security, while a proper renewability can be achieved only with an accurate selection of the employed transformation keys.

A template protection scheme which optimally satisfy all the needed requirements of security and renewability, while guaranteeing the same recognition performances offered by the best functional features based unprotected approaches, still has to be defined. Possible lines of research can be found in the combination of multiple classifiers in different protected domains, or in the definition of a biometric cryptosystem employing functional based signature features.

The proposed approach for a multi-level signature based authentication system can be further investigated by defining a new embedding domain, which should allow the insertion of more features in a static signature representation, and which should result more robust with respect of additive Gaussian noise. The selection of the employed dynamic features, as well as their binarization, can be further investigated. Moreover, better authentication performances can be obtained by exploiting different verification approaches using static signature features. The possibility of employing a common standard deviation for the features of each enrolled users is also an interesting line of research, because it allows to reduce the required storage space, and limit the amount of information which has to be stored for each user, thus improving the security of the considered system.

Bibliography

[1] H. Bigdoli, "Handbook of Information Security, Key Concepts, Infrastructure, Standards, and Protocols", Wiley, 2006.

[2] K.D. Mitnick, W.L. Simon, S. Wozniak, "The Art of Deception: Controlling the Human Element of Security", Wiley, 2002.

[3] D. V. Klien, "Foiling the Cracker; A Survey of, and Improvements to Unix Password Security", *USENIX Workshop on Security*, August 1990.

[4] W. E. Burr, D. F. Dodson, W. T. Polk, "Information Security: Electronic Authentication Guideline", *Technical Special Report 800-63*, NIST, April 2006.

[5] A.K. Jain, A.A. Ross, S. Pankanti, "Biometrics: a tool for information security", *IEEE Transactions on Information Forensics and Security*, Vol. 1, No. 2, pp. 125-143, 2006

[6] A.K. Jain, "An introduction to biometric recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp: 4–20, 2004.

[7] R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha and A.W. Senior, "Guide to Biometrics", Springer, New York, USA, 2004.

[8] S.Z. Li, A.K. Jain (Editors), "Handbook of Face Recognition", Springer, 2005

[9] A.K. Jain, D. Maltoni, D. Maio, "Handbook of Fingerprint Recognition", Springer, 2005.

[10] J. Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp. 21-30, 2004.

[11] H. Borgen, P. Bours, S.D Wolthusen, "Visible-Spectrum Biometric Retina Recognition", *IIHMSP Conference*, 2008

[12] M.K.H Leung, A.C.M. Fong, A.C.M. Siu Cheung Hui, "Palmprint Verification for Controlling Access to Shared Computing Resources" *IEEE Pervasive Computing*, Vol. 6, No. 4, pp: 40-47, 2007

[13] P. Varchol, D. Levicky, J. Juhar, "Multimodal biometric authentication using speech and hand geometry fusion", *IEEE IWSSIP Conference*, 2008.

[14] Ping Yan; K.W. Bowyer, "Biometric Recognition Using 3D Ear Shape", *IEEE Transactions on PAMI*, Vol. 29, No. 8, pp: 1297-1308, 2007.

[15] S. Wua, W. Linb, S. Xiea, "Skin heat transfer model of facial thermograms and its application in face recognition", *Pattern Recognition*, Vol. 41, No. 8, 2008.

[16] S. Soltysiak, H. Valizadegan. "DNA as a Biometric Identifier", Computer Science and Engineering Department, Michigan State University, `http://www.cse.msu.edu/ cse891/Sect601/CaseStudy/DNABiometricIdentifier.pdf`, 2008.

[17] Z. Korotkaya "Biometric Person Authentication: Odor", Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology, `http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf`, 2004.

[18] C.L. Lin, K.C. Fan, "Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns", *IEEE Transactions on CSVT*, Vol. 14, No. 2, 2004.

[19] Y. Wang, F. Agrafioti, D. Hatzinakos, K.N. Plataniotis, "Analysis of Human Electrocardiogram for Biometric Recognition", *EURASIP JASP*, 2008.

[20] S. Marcel, J.R. Millan, "Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, pp: 743-752, 2007.

[21] A.K. Jain, F.D. Griess, S.D. Connell, "On-line Signature Verification", *Pattern Recognition*, Vol. 35, No. 12, pp. 2963-2972, Dec. 2002.

[22] J. Chapran, M.C. Fairhurst, R.M. Guest, C. Ujam, "Task-related population characteristics in handwriting analysis", *IET Computer Vision*, Vol. 2, No. 2, 2008.

[23] M. Goffredo, J.N. Carter, M.S. Nixon, "Front-view Gait Recognition", *IEEE BTAS*, pp: 1-6, 2008.

[24] N.L. Clarke, S.M. Furnell, "Authentication mobile phone users using keystroke analysis", *International Journal of Information Security*, Vol. 6, No. 6, pp: 1-14, 2007.

[25] M.I. Faraj, J. Bigun, "Audiovisual person authentication using lip-motion from orientation maps", *Pattern Recognition Letters*, Vol. 28, No. 11, pp: 1368-1382, 2007.

[26] P. Smaragdis, M. Shashanka, "A Framework for Secure Speech Recognition", *IEEE Transactions on ASLP*, Vol. 15, No. 4, pp: 1404-1413, 2007

[27] R. Clarke, "Human identification in information systems: Management challenges and public policy issues", *Information Technology & People*, Vol. 7, No. 4, pp:6–37, 1994.

[28] J. L. Wayman, "Fundamentals of biometric authentication technologies", *International Journal Image Graphics*, Vol. 1, No. 1, pp. 93113, 2001.

[29] A.K. Jain, S.C. Dass, K. Nandakumar "Utilizing soft biometric traits for person authentication", *ICBA*, Hong Kong, July 2004.

[30] "Biometrics: Personal Identification in Networked society", A.K. Jain, R. Bolle and S. Pankanti (Eds.), Kluwer Academic Publishers, 1999.

[31] S. Prabhakar, S. Pankanti and A.K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy Magazine* 1, pp: 33–42, 2003.

[32] M. Faundez-Zanuy, "Privacy Issues on Biometric Systems", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, No. 2, pp: 13–15, 2005.

[33] E. Mordini, "Biometrics, Human Body and Medicine: A Controversial History", *Ethical, Legal and Social Issues in Medical Informatics*, P. Duquenoy, C. George, K. Kimppa, editors, Hershey, PA: Idea Group Inc., 2008.

[34] D. Zhang, editor, “Medicine Biometrics”, Springer, New York, USA, 2008.

[35] U.K. Biometric Working Group, “Biometric security concerns”, Technical Report, CESG, September 2003,

[36] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, “Handbook of Fingerprint Recognition”, Springer-Verlag, 2003.

[37] U. Uludag, A.K. Jain, “Attacks on biometric systems: a case study in fingerprints”, *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, pp. 622–633, San Jose, CA, January 18-22, 2004.

[38] A.K. Jain, A. Ross and U. Uludag, “Biometric template security: challenges and solutions”, *EUSIPCO*, September 2005.

[39] C. Roberts, “Biometric Attack Vectors and Defences”, *Computers & Security*, Vol. 26, No. 1, September 2006.

[40] A.K. Jain, K. Nandakumar, A. Nagar, “Biometric Template Security”, *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, January 2008.

[41] N. Ratha, J. H. Connell and R. M. Bolle, “An analysis of minutiae matching strength”, *Proc. Int. Conf. AVBPA*, pp. 223-228, 2001.

[42] A. Adler, “Can images be regenerated from biometric templates?”, *Proc. Biometrics Consortium Conference*, 2003.

[43] J. Galbally, J. Fierrez and J. Ortega Garcia, “Bayesian Hill–Climbing attack and its Application to Signature Verification” *Lecture Notes on Computer Science*, Vol. 4642, pp. 386–395, 2007.

[44] A. Ross, J. Shah and A. K. Jain, “Towards reconstructing fingerprints from minutiae points,” *Proc. SPIE, Biometric Technology for Human Identification II*, Vol. 5779, pp. 6880, (Orlando, FL), March 2005.

[45] "Privacy & Biometrics, Building a Conceptual Foundation", NSTC, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, Sept. 2006.

[46] J.D. Woodward Jr., "The law and use of Biometrics", *Handbook of Biometrics*, A. K. Jain, P. Flynn, A.A. Ross editors, Springer 2008.

[47] "Article 29 - Data Protection Working Party 2003, Working Document on Biometrics", 12168/02/EN, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

[48] "IBG BioPrivacy Initiative", http://www.bioprivacy.org (accessed October 2008).

[49] R. Cappelli, A. Lumini, D. Maio, D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates", *IEEE Transactions on PAMI*, Vol. 29, No. 9, pp. 1489-1503, September 2007.

[50] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[51] http://www.speedproject.eu/ "EU project Signal Processing in the Encrypted Domain", Funded in the framework of the IST Programme FET.

[52] "Signal Processing in the Encrypted Domain", *EURASIP Journal on Information Security, Special Issue*, A. Piva, S. Katzenbeisser (eds.), October 2007.

[53] I. Cox, M. Miller, J. Bloom, M. Miller and J. Fridrich, "Digital Watermarking and Steganography", Second Edition, Morgan Kaufmann, 2007.

[54] M. Barni, F. Bartolini, "Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications", Marcel Dekker Ltd, 2004.

[55] A.K. Jain, U. Uludag, "Hiding Biometric Data", *IEEE Transactions on PAMI*, Vol. 25, No. 11, pp: 1494–1498, 2003.

[56] N.K. Ratha, J.H. Connell and R. Bolle, "Secure data hiding in wavelet compressed fingerprint images", *ACM Multimedia 2000 Workshops Proc.*, pp: 127–130, 2000.

[57] S. Pankanti, M.M. Yeung, “Verification Watermarks on Fingerprint Recognition and Retrieval”, *Proc. SPIE*, Vol. 3657, pp: 66–78, 1999.

[58] A.K. Jain, U. Uludag and R. L. Hsu, “Hiding a Face in a Fingerprint Image”, *Int. Conf. on Pattern Rec.*, 2002.

[59] M. Vatsa, R. Singh, P. Mitra and A. Noore, “Digital Watermarking Based Secure Multimodal Biometric System”, *IEEE Intemational Conference on Systems, Man and Cybernetics*, pp. 2983–2987, 2004.

[60] A. Giannoula, D. Hatzinakos, “Data Hiding for Multimodal Biometric Recognition”, *International Symposium on Circuits and Systems (ISCAS)*, 2004.

[61] P. Hennings, M. Savvides and B.V.K. Vijaya Kumar “Hiding Phase-Quantized Biometrics: A Case of Steganography for Reduced-Complexity Correlation Filter Classifiers”, *SPIE Proceeedings on Security, Steganography, and Watermarking of Multimedia Contents VII*, Vol. 5681, pp. 465–473, 2005.

[62] E. Maiorana, P. Campisi and A. Neri, “Multi-level Signature based Biometric Authentication using Watermarking”, *SPIE Defense and Security, Mobile Multimedia/Image Processing for Military and Security Applications*, Vol. 6579, Orlando (FL), 2007.

[63] E. Maiorana, P. Campisi and A. Neri, “Biometric Signature Authentication Using Radon Transform-Based watermarking Techniques,” *IEEE Biometric Symposium*, Baltimore, MD, USA, Sept. 2007.

[64] S. Katzenbeisser, “On the Integration of Watermarks and Cryptography,” *Lecture Notes in Computer Science*, Vol. 2939, pp.50–60, 2004.

[65] I.J. Cox, G. Doerr and T. Furon, “Watermarking is Not Cryptography,” *Lecture Notes in Computer Science*, Vol. 4283, pp.1–15, 2006.

[66] N.K. Ratha, J.H. Connell, R. Bolle, “Enhancing Security and Privacy of Biometric-based Authentication Systems”, *IBM Systems Journal*, Vol. 40, No. 3, 2001.

[67] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, *Biometric Cryptosystems: Issues and Challanges*, *Proc. of IEEE*, Vol. 92, No. 6, pp. 948-960, June 2004.

[68] K. Nandakumar, A. K. Jain and S. Pankati, “Fingerprint–based Fuzzy Vault: Implementation and Performance”, *IEEE Trans. on Information Forensic and Security*, Vol. 2, No. 4, 2007.

[69] A. Juels, M. Wattenberg, “A Fuzzy Commitment Scheme”, *6th ACM Conf. Computer and Communication Security*, pp: 28–36, 1999.

[70] A. Juels, M. Sudan, “A Fuzzy Vault Scheme”, *Des. Codes Cryptography*, Vol. 38, No. 2, pp. 237–257, 2006.

[71] G. Davida, Y. Frankel, B.J. Matt and R. Peralta, “On the relation of Error Correction and Cryptography to an Off Line Biometric Based Identification Scheme”, *Proceedings of WCC99, Workshop on Coding and Cryptography*, 1999.

[72] P. Tuyls, E. Verbitsky, T. Ignatenko, D. Schobben and T.H. Akkermans, “Privacy Protected Biometric Templates: Acoustic Ear Identification”, *SPIE Proc.*, Vol. 5404, pp. 176–182, 2004.

[73] P. Tuyls, A. Akkermans, T. Kevenaar, G.J. Schrijen, A. Bazen and R. Veldhuis, “Practical biometric template protection system based on reliable components”, *AVBPA Proc.*, 2005.

[74] M. Van der Veen, T. Kevenaar, G.-J. Schrijen, T.H. Akkermans and F. Zuo, “Face biometrics with renewable templates”, *SPIE Proc. on Security, Steganography, and Watermarking of Multimedia Contents*, Vol.6072, 2006.

[75] E.J.C. Kelkboom, B. Gökberk, T.A.M. Kevenaar, A.H.M. Akkermans and M. van der Veen, “3D Face: Biometrics Template Protection for 3D face recognition”, *Lecture Notes on Computer Science*, Vol.4642, pp. 566–573, 2007.

[76] P. Campisi, E. Maiorana; M. Gonzalez and A. Neri, “Adaptive and distributed cryptography for signature biometrics protection”, *SPIE Proceedings on Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, 28 Jan. 1 Feb. 2007, San Jose (CA), 2007.

[77] E. Maiorana, P. Campisi and A. Neri, “User Adaptive Fuzzy Commitment for Signature Templates Protection and Renewability,” *SPIE Journal of Electronic Imaging, Special Section on Biometrics: Advances in Security, Usability and Interoperability,* Vol. 17. No.1, January-March 2008.

[78] T.C. Clancy, N. Kiyavash and D.J. Lin, “Secure Smartcard-based Fingerprint Authentication”, *ACM SIGMM Workshop on Biometrics Methods and Applications*, pp. 45–52, 2003.

[79] S. Yang, I. Verbauwhede, “Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme”, *Proc. ICASSP*, pp. 609–612, 2005.

[80] U. Uludag, S. Pankati and A.K. Jain, “Fuzzy Vault for Fingerprints”, *Proc. Audio and Video based Biometric Person Authentication*, pp. 310–319, 2005.

[81] M. Freire-Santos, J. Fierrez-Aguilara and J. Ortega-Garcia, “Cryptographic key generation using handwritten signature”, *SPIE Defense and Security Symposium, Biometric Technologies for Human Identification*, Vol. 6202, pp. 225–231, 2006.

[82] M.R. Freire, J. Fierrez, M. Martinez-Diaz and J. Ortega-Garcia, “On the applicability of off-line signatures to the fuzzy vault construction”, *Proc. Intl. Conf. on Document Analysis and Recognition, ICDAR*, September 2007.

[83] Y. Cheng Feng, P.C Yuen, “Protecting Face Biometric Data on Smartcard with Reed-Solomon Code”, *Proc. on Computer Vision and Pattern Recognition Workshop*, 2006.

[84] D.H. Nyang, K.H. Lee, “Fuzzy Face Vault: How to Implement Fuzzy Vault with Weighted Features”, *Lecture Notes on Computer Science*, Vol.4554, pp. 491–496, 2007.

[85] Y.J. Lee, K. Bae, S.J. Lee, K.R. Park and J. Kim, “Biometric Key Binding: Fuzzy Vault Based on Iris Images”, *Lecture Notes on Computer Science*, Vol.4642, 2007.

[86] W. Chang, R. Shen, F.W. Teo, “Finding the Original Point Set hidden among Chaff”, *ACM symposium Information, Computer and Communications Security*, 2006.

[87] W.J. Scheirer, T.E. Boult, “Cracking Fuzzy Vault and Biometric Encryption”, in *IEEE Biometric Symposium*, 2007.

[88] F. Monrose, M.K. Reiter, Q. Li and S. Wetzel, “Cryptographic Key Generation from Voice”, *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, 2001.

[89] A. Goh, D.C.L. Ngo, “Computation of Cryptographic Keys from Face Biometrics”, *Lecture Notes in Computer Science. Communications and Multimedia Security*, pp: 1–13, 2003.

[90] C. Vielhauer, R. Steinmetza and A. Mayerhöfer, “Biometric Hash based on statistical Features of online Signatures”, *International Conference on Pattern Recognition (ICPR)*, Vol. 1, pp: 123–126, 2002.

[91] C. Vielhauer, R. Steinmetz, “Handwriting: Feature Correlation Analysis for Biometric Hashes”, *EURASIP Journal on Applied Signal Processing, Special issue on Biometric Signal Processing*, Vol. 4, pp: 542–558, 2004.

[92] H. Feng, C.W. Chan, “Private Key Generation from On-line Handwritten Signatures”, *Information Management and Computer Security*, pp: 159–164, 2002.

[93] Y.W. Kuan, A. Goh, D. Ngoa and A. Teoh, “Cryptographic Keys from Dynamic Hand-Signatures with Biometric Secrecy Preservation and Replaceability”, *Proc. Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, pp: 27–32, 2005.

[94] M. R. Freire, J. Fierrez, J. Galbally and J. Ortega-Garcia, “Biometric hashing based on genetic selection and its application to on-line signatures”, *Lecture Notes on Computer Science*, Vol.4642, pp. 1134–1143, 2007.

[95] Y. Dodis, L. Reyzina and A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, *Advances in Cryptology-Eurocrypt*, 2004.

[96] Y. Sutcu, Q. Lia and N. Memon, “Protecting Biometric Templates with Sketch: Theory and Practice”, *IEEE Transactions on Information Forensics and Security*, Vol.2, No.3, September 2007.

[97] M. Savvides, B.V.K. Vijaya Kumar and P.K. Khosla, “Cancelable Biometric Filters for Face Recognition,” *Proc. Int. Conf. Pattern Recognition,* pp. 922-925, 2004.

[98] T. Connie, A.B.J. Teoh, M.K.O. Goh and D.C.L. Ngo, "PalmHashing: A Novel Approach for Cancelable Biometrics," *Information Processing Letters,* Vol. 93, No. 1, pp. 1-5, Jan. 2005.

[99] 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, No. 11, pp. 2245-2255, Nov. 2004.

[100] C.S. Chin, A.B.J. Teoh and D.C.L. Ngo, "High security Iris verification system based on random secret integration" *Computer Vision and Image Understanding*, Vol. 102, No. 2, May, 2006, pp. 169–177.

[101] A.B.J. Teoh, D.C.L. Ngo and A. Goh, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs", *IEEE Transactions on PAMI*, Vol. 28, No. 12, pp. 1892–1901, 2006.

[102] C.L. Ying, A.B.J. Teoh, "Probabilistic Random Projections and Speaker Verification" *Lecture Notes on Computer Science*, Vol. 4662, pp. 445–454, 2007.

[103] Y. Wang, K.N. Plataniotis, "Face based Biometric Authentication with Changeable and Privacy Preservable Templates," *IEEE Biometric Symposium*, Sept. 2007.

[104] A.A. Ross, K. Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer, USA, 2006.

[105] R.M. Bolle, J.H. Connell and N.K. Ratha, " Biometric perils and patches," *Pattern Recognition*, Vol. 35, pp. 2727–2738, 2002.

[106] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable Key-Based Fingerprint Templates", in *Proceedings 10th Australian Conference Information Security and Privacy*, pp. 242–252, July 2005.

[107] N. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, "Generating Cancelable Fingerprint Templates", *IEEE Transactions on PAMI*, Vol. 29, No. 4, pp. 561–572, April 2007.

[108] T.E. Boult, W.J. Schreirer, R. Woodworth, “Revocable Fingerprint Biotokens: Accuracy and Security Analysis”, *IEEE Conf. on Computer Vision and Pattern Recognition*, pp. 17–22, 2007.

[109] H. Lee, C. Lee, J.Y. Choi, J. Kim and J. Kim, “Changeable Face Representations Suitable for Human Recognition” *Lecture Notes on Computer Science*, Vol. 4662, 2007.

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

[111] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia and A. Neri, “Template Protection for HMM-based On-line Signature Authentication”, *CVPR Conference, Workshop on Biometrics*, Anchorage, USA, 23-28 June 2008.

[112] E. Maiorana, P. Campisi, J. Ortega-Garcia and A. Neri, “Cancelable Biometrics for HMM-based Signature Recognition”, *IEEE BTAS*, October 2008.

[113] P. Gother, “Biometrics Standards”, *Handbook of Biometrics*, A.K. Jain, P. Flynn, A.A. Ross, editors, Springer New York, USA, 2008.

[114] ISO/IEC PRF TR 24714-1, “Information technology - Cross-jurisdictional and societal aspects of implementation of biometric technologies - Part 1: General guidance”, URL: `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=38824`

[115] ISO/IEC WD TR 24714-2, “Biometrics - Jurisdictional and societal considerations for commercial applications - Part 2: Specific technologies and practical applications”, URL: `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43607`

[116] ISO/IEC FCD 19792, “Information technology - Security techniques - Security evaluation of biometrics”, URL: `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51521`

[117] ISO/IEC NP 24745, "Information technology - Biometric template protection", URL: `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52946`

[118] BITE 07 URL: `http://www.biteproject.org/` (accessed October 2008).

[119] HIDE 08 URL: `http://www.hideproject.org/` (accessed October 2008).

[120] PRIME 08 URL: `https://www.prime-project.eu/` (accessed October 2008).

[121] J. Fierrez, J. Ortega-Garcia, D. Ramos and J. Gonzalez-Rodriguez, "HMM-Based On-Line Signature Verification: Feature Extraction and Signature Modeling", *Pattern Recognition Letters*, Vol. 28, No. 16, pp. 2325–2334, Dec. 2007.

[122] M. Faundez-Zanuy, "Signature recognition state-of-the-art", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 20, No. 7, pp. 28–32, 2005.

[123] S. Elliott, A. Hunt, "Dynamic signature forgery and signature strength perception assessment", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 23, No. 6, 2008.

[124] J. Galbally-Herrero, J. Fierrez-Aguilar, J.D. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, M. Tapiador, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks", *Carnahan Conferences Security Technology*, pp: 130-136, 2006.

[125] X. He, Y. Lu, P. Shi, "A Fake Iris Detection Method Based on FFT and Quality Assessment", *Chinese Conference on Pattern Recognition (CCPR)*, 2008.

[126] G. Dimauro, S. Impedovo, M.G. Lucchese,R. Modugno and G. Pirlo, "Recent advancements in automatic signature verification", *Ninth International Workshop on Frontiers in Handwriting Recognition*, pp. 179–184, 26-29 Oct. 2004.

[127] R.Plamondon, G.Lorette, "Automatic signature verification and writer identification: The state of the art", *Pattern Recognition*, Vol. 22, No. 2, pp. 107–131, 1989.

[128] F. Leclerc, R.Plamondon, "Automatic signature verification: The state of the art 1989-1993", *IJPRAI*, Vol.8, No. 3,pp. 643–660, 1994.

[129] R. Plamondon, S.N. Srihari, "Online and off-line handwriting recognition: a comprehensive survey", *IEEE Transactions on PAMI*, Vol. 22, No. 1, Jan. 2000.

[130] J. Fierrez, J. Ortega-Garcia, "On-line signature verification", *Handbook of Biometrics*, Springer, A. K. Jain, A. Ross and P.Flynn editors, pp. 189-209, 2008.

[131] D. Impedovo, G. Pirlo, "Automatic Signature Verification: The State of the Art", *IEEE Transactions on Systems, Man, and Cybernetics PART: C*, Vol. 38, No. 5, pp: 609-635, 2008.

[132] A.K. Jain, R.P.W. Duin and J. Mao, "Statistical pattern recognition: a review", *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 22, No. 1, 2000.

[133] K. Huang, H. Yan, "Off-line signature verification using structural feature correspondence", *Pattern Recognition* 35, pp. 2467–2477 (2002).

[134] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia and D. Maltoni, "An on-line Signature Verification System based on Fusion of Local and Global Information", *AVBPA*, pp: 523–532, 2005

[135] Y. Jonghyon, L. Chulhan and K. Jaihie, "Online signature verification using temporal shift estimated by the phase of Gabor filter", *IEEE Trans. on Signal Processing*, Vol. 53, No. 2, Part 2, pp. 776–783, Feb. 2005.

[136] Marcos Faundez-Zanuy, "On-line signature recognition based on VQ-DTW", *Pattern Recognition*, Vol. 40, pp. 981–992, 2007.

[137] G. Agam, S. Suresh, "Warping-Based Offline Signature Recognition", *IEEE Transactions on Information Forensics and Security*, Vol. 2, No. 3, Part 1, pp. 430–437, 2007.

[138] D.-Y. Yeung *et al.*, "SVC2004: First International Signature Verification Competition", *Proceedings of the International Conference on Biometric Authentication (ICBA)*, Hong Kong, 15-17, July 2004.

[139] A. Kholmatov, B. Yanikoglu, "Identity Authentication Using Improved Online Signature Verification Method", *Pattern Recognition Letters*, Vol. 26, No. 15, 2005.

[140] A. Piyush Shanker, A.N. Rajagopalan, “Off-line signature verification using DTW”, *Pattern Recognition Letters*, Vol. 28, No. 12, pp:1407-1414, 2007.

[141] L. Yang, B. W. Widjaja and R. Prasad, “Application of Hidden Markov Models for signature verification”, *Pattern Recognition*, Vol.2 8, No.2, pp. 161–170, 1995.

[142] L. Nanni, A. Lumini, “A novel local on-line signature verification system”, *Pattern Recognition Letters*, Vol. 29, No.5, pp: 559-568, 2008.

[143] M. Fuentes, S. Garcia-Salicetti and B. Dorizzi, “On line signature verification: Fusion of a Hidden Markov Model and a neural network via a support vector machine”, *International Workshop on Frontiers in Handwriting Recognition*, pp. 253–258, 2002.

[144] C. Quek, R.W. Zhou, “Antiforgery: a novel pseudo-outer product based fuzzy neural network driver signature verification system”, *Pattern Recognition*, Vol. 23, 2002.

[145] J. Fierrez-Aguilar, S. Krawczyk, J. Ortega-Garcia, A.K. Jain, “Fusion of Local and Regional Approaches for On-Line Signature Verification”, *IWBRS*, pp: 188-196, 2005.

[146] B.L. Van, S. Garcia-Salicetti, B. Dorizzi, “On using the viterbi path along with HMM likelihood information for online signature verification”, *IEEE Trans. on Systems, Man and Cybernetics, part B*, No. 5, pp. 1237-1247, 2007.

[147] H. Lei, V. Govindaraju, “A comparative study on the consistency of features in on-line signature verification”, *Pattern Recognition Letters*, Vol. 15, pp. 2483–2489, 2005.

[148] W.K. Yip, A. Goh, D.C.L. Ngo, and A.B.J. Teoh, “Generation of Replaceable Cryptographic Keys from Dynamic Handwritten Signatures”, in *ICB06*, pp. 509–515, 2006.

[149] A. Lumini, L. Nanni, “An improved BioHashing for human authentication”, *Pattern Recognition*, Vol. 40, No. 3, pp: 1057-1065, 2007.

[150] P. Campisi, E. Maiorana, and A. Neri, “On-line signature based authentication: template security issues and countermeasures”, in Biometrics: Theory, Methods, and Applications, N. V. Boulgouris, K.N. Plataniotis, and E.Micheli-Tzanakou, editors, Wiley/IEEE, January 2009.

[151] E. Maiorana, P. Campisi, A. Neri, "Signature-based Authentication System using Watermarking in the Ridgelet Domain", *SPIE Europe Security & Defence Symposium*, 17-20 September 2007.

[152] A. Jain, S. Prabhakar, A. Ross, "Fingerprint Matching: Data Acquisition and Performance Evaluation, MSU Technical Report TR99-14", URL: `citeseer.ist.psu.edu/jain99fingerprint.html`, 1999.

[153] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Torre-Toledano, J. Gonzalez-Rodriguez, "BioSec baseline corpus: A multimodal biometric database", *Pattern Recognition*, Vol. 40, No. 4, pp: 1389-1392, 2007.

[154] S. Garcia-Salicetti, et al., "BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities", *LNCS*, Vol. 2688, pp: 845853, 2003.

[155] D. Dumas, et al., "MyIdea - Sensors Specifications and Acquisition Protocol", University de Fribourg in Switzerland, Computer Science Department Research Report, 2005.

[156] E. Bailly-Bailliere, et al., "The BANCA database and evaluation protocol", *IAPR AVBPA, Springer LNCS*, Vol. 2688, pp: 625-638, 2003.

[157] BioSec, *Biometrics and Security, FP6 IP IST-2002-001766*, URL: `http://www.biosec.org/`, 2003.

[158] J. Fierrez, et al. "BiosecurID: A Multimodal Biometric Database", *Workshop on User-Centric Technologies and Applications*, 2007.

[159] Biosecure, *Biometrics for Secure Authentication, FP6 NoE IST-2002- 507634*, URL: `http://www.biosecure.info/`, 2007.

[160] J. Ortega-Garcia *et al.*, "MCYT baseline corpus: A bimodal biometric database", *IEE Proceedings Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, Vol. 150, No. 6, pp. 395–401, December 2003.

[161] D. Dessimoz, et al., “Multimodal biometrics for identity documents (MBioID)”, *Forensic Science International*, Vol. 167, pp. 154-159, 2007.

[162] S. Steininger, et al., “Development of user-state conventions for the multimodal corpus in SmartKom”, *MRMSE Workshop*, pp. 33-37, 2002.

[163] J.G.A. Dolfing, E.H.L. Aarts, J.J.G. Van Oosterhout, “On-line signature verification with hidden Markov models”, *IEEE 14th Int. Conf. on Pattern recognition*, pp. 13091312, 1998.

[164] M.E. Munich, P. Perona, “Visual identification by signature tracking”, *IEEE Transactions on PAMI*, Vol. 25, No. 2, pp: 200-217, 2003.

[165] `http://atvs.ii.uam.es/mcyt100s.html`

[166] R. Baron, R. Plamondon, “Acceleration measurement with an instrumented pen for signature verification and handwriting analysis”, *IEEE Trans. on Instrumental Measurement*, Vol. 38, No. 6, pp: 11321138, 1989.

[167] G.A.P. Cirrone, S. Donadio, S. Guatelli, A. Mantero, B. Mascialino, S. Parlati, M.G. Pia, A. Pfeiffer, A. Ribon and P. Viarengo, “A Goodness-of-Fit Statistical Toolkit”, *IEEE Transactions on Nuclear Science*, Vol. 51, 2004.

[168] M. Purser, “Introduction to Error-Correcting Codes”, Artech House, Boston, 1995.

[169] Federal Information Processing (FIP) Standards Publication 180-1, Security Hash Standard, `http://www.itl.nist.gov/fipspubs/fip180-1.htm`, 1995.

[170] V. Rijmen, E. Oswald, “Update on SHA-1”, *Lecture Notes in Computer Science*, Vol. 3376, Springer, 2005.

[171] X. Wang, Y.L. Yin, H. Yu, “Finding Collisions in the Full SHA-1”, *CRYPTO*, 2005.

[172] C. De Cannire, C. Rechberger, “Finding SHA-1 Characteristics: General Results and Applications”, *Advances in Cryptology, ASIACRYPT*, Springer, Vol. 4284, 2006.

[173] W. Nelson, E. Kishon, “Use of dynamic features for signature verification”, *IEEE International Conference on Systems, Man, and Cybernatics*, Vol 1, pp: 201205, 1991.

[174] w. Nelson, W Turin, T. Hastie, "Statistical methods for on-line signature verification", *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 8, pp: 749770, 1994.

[175] L.L. Lee, T. Berger, E. Aviczer, "Reliable on-line human signature verification systems", *IEEE Transactions on PAMI*, Vol. 18, pp: 643647, 1996.

[176] R. Palaniappan, D.P. Mandic, "Biometrics from Brain Electrical Activity: A Machine Learning Approach", *IEEE Transactions on PAMI*, Vol. 29, No. 4, April 2007.

[177] L. Ma, T. Tan, Y. Wang, D. Zhang, "Local intensity variation analysis for iris recognition", *Pattern Recognition*, Vol. 37, No. 6, pp. 12871298, 2004.

[178] W. Diffie, M.E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. 22, pp: 644-654, November 1976.

[179] A. Cichocki, S. Amari, "Adaptive Blind Signal and Image Processing", John Wiley & Sons, 2002.

[180] P. Campisi, K. Egiazarian, "Blind image deconvolution: theory and applications", CRC press, 2007.

[181] S. Haykin, *Blind Deconvolution*, Prentice-Hall, New Jersey, 1994

[182] L. Zhang, A. Cichocki, S. Amari, "Multichannel blind deconvolution of nonminimum-phase systems using filter decomposition", *IEEE Transactions on Signal Processing*, Vol. 52, No. 5, pp. 1430-1442, May 2004.

[183] L.R. Rabiner, "A tutorial on Hidden Markov Models and selected applications in speech recognition", *Proceedings of the IEEE*, Vol. 77, No. 2, pp. 257–286, 1989.

[184] H. Sakoe, S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition", *IEEE Transactions on Acoustics, Speech, and Signal Processing*, Vol. 26, No. 1, pp. 43–49, February 1978.

[185] J. Hennebert, R. Loeffel, A. Humm, R. Ingold, "A New Forgery Scenario Based on Regaining Dynamics of Signature", *Proc. ICB* pp. 366-375, 2007.

[186] R. Brunelli, D. Falavigna, “Person Identification using multiple cues”, *IEEE Transactions on PAMI*, Vol. 17, No. 10, pp: 955-966, 1995.

[187] R. Cappelli, D. Maio, D. Maltoni, “Combining fingerprint Classifiers”, *Workshop on multiple classifier Systems*, pp:351-361, 2000.

[188] F.R. Hampel, P.J. Rousseeuw, E.M. Ronchetti, W.A. Stahel, “Robust Statistics: the Approach based on Influence Functions”, John Wiley and Sons, 1986.

[189] S. R. Deans, “The Radon Transform and some of its Applications”, John Wiley and Sons, 1983.

[190] M. N. Do, M. Vetterli, “The Finite Ridgelet Transform for Image Representation”, *IEEE Transactions on Image Processing*, Vol. 12, No. 1, pp: 16–28, 2003.

[191] B. Chen, G. Wornell, “Quantization Index Modulation: a Class of Provably Good Methods for Digital Watermarking and Information embedding”, *IEEE Transactions on Information Theory*, Vol. 47, 2001.

[192] P. Campisi, D. Kundur and A. Neri, “Robust Digital Watermarking in the Ridgelet Domain”, *IEEE Signal Processing Letters*, Vol. 11, No. 10, 2004.

[193] L. Mao, H. -Z. Wu, Z. -H. Wei and Y. Bao, “Perceptual Digital Watermark of Images Using Ridgelet Transform”, *Third International Conference on Machine Learning and Cybernetics*, Shanghai, 2004.

[194] R. Quixtiano-Xicohtencatl, L. Flores-Pulido, O.F. Reyes-Galaviz, “Feature Selection for a Fast Speaker Detection System with Neural Networks and Genetic Algorithms”, *15th International Conference on Computing (CIC)*, 2006.

[195] M.L. Raymer, W.F. Punch, E.D. Goodman, L.A. Kuhn, A. Jain, “Dimensionality reduction using genetic algorithms”, *IEEE Transaction on Evolutionary Computation*, Vol. 4, No. 2, pp:164-171, July 2000.

[196] F. van Den Bergh, A.P. Engelbrecht, “A cooperative approach to Particle Swarm Optimization”, *IEEE Trans. on Evolutionary Computation*, Vol. 8, No. 3, 2004.

[197] G.L.F. Azevedo, G.D.C. Cavalcanti, E.C.B. Filho, “An approach to feature selection for keystroke dynamics systems based on PSO and feature weighting”, *IEEE Congress on Evolutionary Computation (CEC)*, pp:3577 - 3584, 2007.

[198] G. Baofeng, M.S. Nixon, “Gait Feature Subset Selection by MutualInformation”, *IEEE Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, 2007.

[199] P. Brittan, M.C. Fairhurst, “Feature selection in automatic signature verification”, *IEE Colloquium on Image Processing for Biometric Measurement*, 1994.

[200] J. Richiardi, K. Hamed, A. Drygajlo, “Local and global feature selection for on-line signature verification”, *Conference on Document Analysis and Recognition*, 2005.

[201] H. Crane, J. Ostrem, “Automatic signature verification using a three-axis force-sensitive pen”, *IEEE Trans. on Systems, Man, and Cybernetics*, 1983.

[202] H. Lei, V. Govindaraju, “A study on the consistency of features for on-line signature verification”, *Joint IAPR International workshops on Structural, Syntactic, and Statistical Pattern Recognition (SSPR)*, 2004.

[203] F. Bauer, B. Wirtz, “Personalized Parameter Selection for Automatic Signature Verification”, *Conference on Document Analysis and Recognition (ICDAR)*, Vol. 1, 1995.

[204] H. Niemann, “Pattern Classification”, Wiley, 2000.

[205] E. Parzen, “On Estimation of a Probability Density Function and Mode”, *Annals of Mathematical Statistics*, Vol. 33, pp: 10651076, 1962.