UNIVERSIDAD AUTÓNOMA DE MADRID
ESCUELA POLITÉCNICA SUPERIOR
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

VULNERABILITIES AND ATTACK PROTECTION IN SECURITY SYSTEMS BASED ON BIOMETRIC RECOGNITION

–TESIS DOCTORAL–

VULNERABILIDADES Y PROTECCIÓN FRENTE A ATAQUES EN SISTEMAS DE SEGURIDAD BASADOS EN RECONOCIMIENTO BIOMÉTRICO

Author: Javier Galbally Herrero
(Ingeniero de Telecomunicación, Universidad de Cantabria)

A Thesis submitted for the degree of:

Doctor of Philosophy

Madrid, November 2009

Colophon

This book was typeset by the author using LaTeX2e. The main body of the text was set using a 11-points Computer Modern Roman font. All graphics and images were included formatted as Encapsuled Postscript (^{TM} Adobe Systems Incorporated). The final postscript output was converted to Portable Document Format (PDF) and printed.

This Thesis was printed with the financial support from EPS-UAM and the Biometric Recognition Group-ATVS.

Department:	Ingeniería Informática Escuela Politécnica Superior Universidad Autónoma de Madrid (UAM), SPAIN
PhD Thesis:	Vulnerabilities and attack protection in security systems based on biometric recognition
Author:	**Javier Galbally** Ingeniero de Telecomunicación (Universidad de Cantabria)
Coadvisor:	**Prof. Javier Ortega-Garcia** Doctor Ingeniero de Telecomunicación (Universidad Politécnica de Madrid) Universidad Autónoma de Madrid, SPAIN
Coadvisor:	**Dr. Julian Fierrez** Doctor Ingeniero de Telecomunicación (Universidad Politécnica de Madrid) Universidad Autónoma de Madrid, SPAIN
Year:	2009
Committee:	President: **Prof. Carmen Garcia-Mateo** Universidad de Vigo, SPAIN Secretary: **Dr. Daniel Ramos** Universidad Autónoma de Madrid, SPAIN Vocal 1: **Dr. Raffaele Cappelli** Università di Bologna, ITALY Vocal 2: **Prof. Ángel Sánchez** Universidad Rey Juan Carlos, SPAIN Vocal 3: **Prof. Miguel A. Ferrer** Universidad de las Palmas de Gran Canaria, SPAIN

The research described in this Thesis was carried out within the Biometric Recognition Group – ATVS at the Dept. of Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid (from 2005 to 2009). The project was partially funded by a PhD scholarship from Spanish Ministerio de Educacion y Ciencia.

The author was awarded with a PhD scholarship from Spanish Ministerio de Educacion y Ciencia between 2006 and 2010 which supported the research summarized in this Dissertation.

The author has been awarded with the IBM Best Student Paper Award in the IAPR International Conference on Pattern Recognition 2008, for one publication originated from this Dissertation: Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Davide Maltoni and Julian Fierrez, "Fake Fingertip Generation from a Minutiae Template", Proc. of IAPR ICPR 2008, Tampa, Florida, USA, December 2008.

Part of the work described in this Dissertation was published as an Invited Paper at the Pattern Recognition Letters Special Issue on ICPR'08 Awarded Papers: Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de-Rivera, Davide Maltoni, Julian Fierrez, Javier Ortega-Garcia, and Dario Maio, "Fake Fingertip Generation from a Minutiae Template", PRL Special Issue on ICPR'08 Awarded Papers, 2009.

The author was finalist of the EBF European Biometric Research Award 2009, from the European Biometrics Forum, for part of the research work originated from this Dissertation: Javier Galbally, "Impact of Fake Finger Attacks from Stolen Minutiae Templates and Quality-Based Countermeasures".

Abstract

Absolute security does not exist: given funding, willpower and the proper technology, every security system can be compromised. However, the objective of the security community should be to develop such applications that the funding, the will, and the resources needed by the attacker to crack the system prevent him from attempting to do so.

This Thesis is focused on the vulnerability assessment of biometric systems. Although being relatively young compared to other mature and long-used security technologies, biometrics have emerged in the last decade as a pushing alternative for applications where automatic recognition of people is needed. Certainly, biometrics are very attractive and useful for the final user: forget about PINs and passwords, you are your own key. However, we cannot forget that as any technology aimed to provide a security service, biometric systems are exposed to external attacks which could compromise their integrity. Thus, it is of special relevance to understand the threats to which they are subjected and to analyze their vulnerabilities in order to prevent possible attacks and increase their benefits for the users.

In this context, the present PhD Thesis pretends to give some insight into the difficult problem of biometric security evaluation through the systematic study of biometric systems vulnerabilities and the analysis of effective countermeasures that can minimize the effects of the detected threats, in order to increase the confidence of the final users in this thriving technology. This way, the experimental studies presented in this Dissertation can help to further develop the ongoing security evaluation standardization efforts, and may be used as guidelines to adapt the existing best practices in security evaluation to the specificities of particular security applications based on biometric recognition.

The Thesis has been developed following the *security through transparency* principle, largely applied in other security related areas such as cryptography, which pleads for making security systems as public as possible. This paradigm relies on the fact that vulnerabilities exist regardless of their publication, therefore: let's face the problems and find solutions for them (controlled risk), before somebody else finds the way to take advantage of our secrets (unpredictable consequences). That is not to say that obscurity cannot provide any protection, rather that the protection is out of our control and most probably temporary. We believe that in order to make biometric devices and applications secure it is necessary to understand and assess the threats, and publicly report quantitative measures of the impact of these threats so that effective countermeasures, technical and procedural, can be issued if necessary.

The problem of vulnerability assessment in biometric systems had already been addressed in some previous works, but in most cases not using a statistically significant approach, or any systematic and reproducible protocol. In this Dissertation, after summarizing the most relevant works related to the Thesis, we describe the security evaluation methodology that has been

followed throughout the experimental chapters. These are dedicated to the vulnerability study of three commonly employed biometrics, namely: fingerprint, signature, and face; using the biometric data and benchmarks previously described.

The experimental part of the Thesis starts with the security evaluation of fingerprint-based recognition systems against two different direct attacks: starting from a latent fingerprint and starting from a standard ISO minutiae template (this last study questions the widespread belief of minutiae templates non-reversibility). An indirect hill-climbing attack is also implemented and different countermeasures for the studied attacks are analyzed (a liveness detection method based on quality measures for the direct approaches, and a score quantization scheme for the hill-climbing algorithm).

We then study the vulnerabilities of on-line signature recognition systems. Two type of indirect attacks are implemented: a novel hill-climbing attack based on Bayesian adaptation, and a brute-force attack carried out with synthetically generated signatures. The hill-climbing algorithm was used against a feature-based verification system and a comparative study between the most robust and the best performing features is presented as a way to increase its robustness against the attack. In the case of the brute force attack carried out with synthetically generated signatures, the experiments are performed by attacking real signature models obtained with a HMM-based recognition system with synthetic samples. The feasibility of using synthetic duplicated signatures in the enrollment stage to increase the robustness of the system against user intravariability, is studied as a countermeasure that can minimize the success chances of the brute-force attack.

Finally, an evaluation of the robustness of two face recognition systems (one PCA-based and one working on GMMs) against the Bayesian-based hill-climbing attack is reported, and the effectiveness of score quantization as a way to reject the attack is explored. The experimental results show that the two face verification systems studied are highly vulnerable to this type of attacking approach, even when no real images are used to initialize the algorithm. Furthermore, the attack shows its ability to reconstruct the user's real face image from the scores, thus arising security issues concerning the privacy of the client. The experimental evidence obtained from the evaluation of signature and face verification systems against this novel hill-climbing algorithm proves the ability of this attacking strategy to adapt to totally different environments and therefore its big attacking potential.

The research work described in this Dissertation has led to novel contributions which include the development of three new methods for vulnerability assessment and attack protection of biometric systems, namely: *i*) a hill-climbing attack based on Bayesian adaptation, *ii*) an on-line signature synthetic generation method based on spectral analysis, and *iii*) a liveness detection approach for fingerprint recognition based on quality related features. Moreover, different original experimental studies have been carried out during the development of the Thesis (e.g., first time that a minutiae template is reverse engineered to generate a gummy finger). Besides, the research work completed throughout the Thesis has been complemented with the generation of several novel literature reviews and with the acquisition of new biometric data.

A mis padres.
A mis hermanos.
A mi hermana.

A Carmen.

Quis custodiet ipsos custodes?
(Who watches the watchmen?)
(¿Quién vigila a los vigilantes?)

–Juvenal, *Sátiras, VI 346-348*, S. I.

Acknowledgements

This PhD Thesis summarizes the work carried out during my Ph.D. studies with the Biometric Recognition Group - ATVS since 2005. This research group was established in 1994 at the Dept. of Ingeniería Audiovisual y Comunicaciones (DIAC) of the Universidad Politécnica de Madrid (UPM) and since 2004 is affiliated to the Dept. of Ingeniería Informática of the Universidad Autónoma de Madrid (UAM). The financial support for the first six months of the Ph.D. studies came from a research grant with Centro Criptológico Nacional (CCN). Subsequent years have been financially supported by a Ph.D. scholarship from Ministerio de Educación y Ciencia (MEC), and various Spanish and European projects.

Foremost, I would like to thank my advisors Prof. Javier Ortega-García and Dr. Julián Fiérrez for their guidance and support over the past four years. The confidence they have always shown in me has definitely fostered my motivation. During these years I have benefited from their courage, vision, discipline and intelligent effort, which have shaped my working attitudes. Apart from his constant support and advice in the academic field, I cannot but thank Prof. Ortega-García for sharing with me his very particular (and may I say, very funny and limited) football knowledge which is, thankfully, largely exceeded by his culinary taste.

In the framework of the ATVS research group, I have also received support from Prof. Joaquín González-Rodríguez, feeling fortunate to learn from his wise advice.

As well, I am particularly indebted with Prof. Ignacio Santamaría who opened his door for me to his group (Grupo de Tratamiento Avanzado de Señal, GTAS, Universidad de Cantabria) when I was pursuing my Master degree, and with Dr. Javier Vía for his patience as co-advisor of my MSc Thesis. Their guidance, support, and lessons learned during my collaboration with them motivated me to endeavor a research career in signal processing and pattern recognition. I would also like to thank a number of professors that marked me during my years as an undergraduate student, specially Profs. Luis Vielva, Jesús Ibáñez, Carlos Pantaleón, and Elena Álvarez. I also want to mention here Don Lorenzo Vara, from my school years at Colegio San Agustín, because I will never forget many of the things that he taught me.

During the journey of my Ph.D. degree I have been fortunate to meet many excellent professionals and colleagues. I am especially grateful to Dr. Daniel Ramos-Castro for his continuous support, for his valuable advice and knowledge not only on academic issues, for his reviews and comments on the Thesis, and for opening my eyes to new ways of seeing things, and my ears to damn good music. I have also benefited and enjoyed from a close contact with Profs. Doroteo T. Toledano, Guillermo González de Rivera, Javier Garrido, and Juan A. Sigüenza, as well as very fruitful discussions with Dr. Marino Tapiador.

I would also like to acknowledge two fellow researchers at ATVS who have actively contributed to some of the research lines that have finally shaped the Thesis, and for their constant support during the long (and tedious) writing process: Dr. Fernando Alonso-Fernandez, and

Marcos Martinez-Diaz.

The opportunity of visiting foreign institutions during my Ph.D. studies was a real luck. I especially remember my first research stay at the Università di Bologna. I had the fortune to meet Prof. Davide Maltoni there, who kindly host me at the Biometric System Laboratory (BioLab) where I met a fantastic group of people. I would like to especially mention Drs. Raffaele Cappelli and Alessandra Lumini whose extraordinary care during my visit and their intelligence and constant support during those two months were essential for the development of part of this work. Also, they were partly responsible of my happiness during the stay, with their kind attention and help, together with their colleagues at the laboratory who I will never forget, Annalisa Franco, Matteo Ferrara, Mattia Romagnoli, Matteo Silimbani, and Lorenzo Baldacci. I would also like to mention here the BANG! deck of cards, that so many great moments gave us.

My second stay was at the IDIAP Research Institute, with Dr. Sébastien Marcel. During those three months I received an enormously motivating support and confidence from Dr. Marcel, and I could benefit from his mastery in the field of computer vision, which led to some contributions contained in this Thesis. I had also the opportunity to meet Dr. Christopher McCool, whose kindness and patience as well as his wide knowledge in face recognition helped me in my research and made me feel at home in the daily work.

My last two-month research stay was conducted with Prof. Réjean Plamondon at the École Polytechnique de Montréal, Canada, where the Dissertation was completed. I really appreciate his support in spite of his multiple commitments as director of the Scribens Laboratory.

From such research stays, there is a huge number of colleagues and friends who I want to thank as they meant to me more than they probably think. With apologies to all those wonderful people not mentioned here, I have to especially thank: Álvaro and Anaïs (for their friendship and for letting me share their home, their friends, and their food), Corrado e Bordo (the italian big guys), Pierre Ferrez and Cédric Dufour (great skiers), Hugo Penedones, Edgar Francisco Roman (Paco), Joan I. Biel, Tatiana and Lisa (the italian connection), Cosmin and Fabio (my gym mates), Niklas and Jordi (my fellow sufferers). All of them, among many others, have made possible the difficult task for a Spaniard to stop missing his country at least for a while.

I have to especially thank here my italian *family*, not a very standard one, but a family all the same: Michele Spinelli, Niccolo Cerioni, Marcolino Piazza, and Domenico Amorese. I lived with them some of the best, funniest, and greatest moments I ever had. Miki, Cirio, Marco, Mimmo: *Grazie mille, siete i più bravi stronzi che ho conosciuto, non vi dimenticherò mai.*

And of course I want to thank all the work mates (and friends) at ATVS who truly welcomed a very annoying guy from Santander and, in spite of him being a real pain in the neck, made him feel at home. This would not have been the same, or even possible, without you. Although you are still not able to understand the difference between *rabas* and *calamares*, and you keep saying that the beach is full of *tierra* instead of *arena*, I love you guys. So this huge THANK YOU goes to (in no particular order): Julián Fiérrez (once again, thank you man), Fernando Alonso (not the F1 driver), Daniel Ramos (amazing singer, better person), Alberto Montero

(the saint), Almudena Gilpérez (*how strong it appears to me*), Ignacio López (a great climber and a not-so-great beer drinker), Alicia Beisner (Disney star), Javier Franco (*Tip y Coll* miss you), Javier Simón (blues and *pilón* fan), Verónica Peña (why with Javi?), Lucas Pérez (and his charming wife Marisa, my swiss connection), Daniel Hernández (the uncreation), Manuel Freire (it was definitely a terrible mistake), Susana Pecharromán (the first Susana), Miriam Moreno (Ms Smiley), Víctor González (*china, churra, chorra... vaya tela*), Gustavo Sanz (the big one), Marcos Martínez (right away), Pedro Tomé (no, to everything), Alejandro Abejón (catch it if you can), Ismael Mateos (thank you for your cooperation), Danilo Spada (the social engineer), Emanuele Maiorana (the italian *atvsiano*), Sara Carballo (my first time... as advisor), Virginia Ruiz (yes she can). And last but not least, let me thank Javier González (and his more-than-a-brother Santi, my *chocolate con churros* mates), that not only made me feel at home, but opened his when I needed it. To all of you, thanks for the memories.

Es evidente que nunca fui el mejor hijo, ni hermano, ni amigo, ni pareja. Y sin embargo, mis padres, mis hermanos, mi hermana, mis amigos, y sobre todo Carmen, siempre estuvieron allí.

Gracias.

Javier Galbally Herrero
Madrid, November 2009

Contents

List of Figures

List of Tables

Chapter 1

Introduction

How secure is this technology?. Why should I trust it?. Who assures the level of security offered by this system?. In other words, *who watches the watchmen?*. These and other similar questions often raise when dealing with Information Technology solutions for security applications. This PhD Thesis is focused on the statistical analysis of biometric systems vulnerabilities and attack protection methods, in order to propose a set of guidelines, supported by experimental results, that can help evaluators to give an evidence-based response to these difficult issues.

Automatic access of persons to services is becoming increasingly important in the information era. This has resulted in the establishment of a new technological area known as biometric recognition, or simply *biometrics* [Jain *et al.*, 2006]. The basic aim of biometrics is to discriminate automatically between subjects –in a reliable way and according to some target application– based on one or more signals derived from physical or behavioral traits, such as fingerprint, face, iris, voice, hand, or written signature. These personal traits are commonly denoted as *biometric modalities* or also as *biometrics*.

Although person authentication by machine has been a subject of study for more than thirty years [Atal, 1976; Kanade, 1973], it has not been until the last decade that biometrics research has been established as an specific research area. This is evidenced by recent reference texts [Jain *et al.*, 2008b; Ratha and Govindaraju, 2008; Ross *et al.*, 2006], specific conferences [Boyer *et al.*, 2008; Lee and Li, 2007; Tistarelli and Maltoni, 2007; Vijaya-Kumar *et al.*, 2008], common benchmark tools and evaluations [Cappelli *et al.*, 2006b; LivDet, 2009; Mayoue *et al.*, 2009; Przybocki and Martin, 2004; Yeung *et al.*, 2004], cooperative international projects [BioSec, 2004; Biosecure, 2007; COST, 2007; MTIT, 2009], international consortia dedicated specifically to biometric recognition [BC, 2009; BF, 2009; BI, 2009; EBF, 2009], standardization efforts [ANSI/NIST, 2009; BioAPI, 2009; ISO/IEC JTC 1/SC 27 , 2009; ISO/IEC JTC 1/SC 37 , 2009], and increasing attention both from government [BWG, 2009; DoD, 2009] and industry [IBIA, 2009; International Biometric Group, 2009].

Biometric technology presents several advantages over classical security methods based on

something that you know (PIN, Password, etc.) or something that you have (key, card, etc.). Traditional authentication systems cannot discriminate between impostors who have illegally acquired the privileges to access a system and the genuine user, and cannot satisfy negative claims of identity (i.e., I am not E. Nigma) [Jain *et al.*, 2006]. Furthermore, in biometric systems there is no need for the user to remember difficult PIN codes that could be easily forgotten or to carry a key that could be lost or stolen.

However, in spite of these advantages, biometric systems present a number of drawbacks [Schneier, 1999], including the lack of secrecy (e.g., everybody knows our face or could get our fingerprints), and the fact that a biometric trait cannot be replaced (if we forget a password we can easily generate a new one, but no new fingerprint can be generated if an impostor "steals" it). Furthermore, biometric systems are vulnerable to external attacks which could decrease their level of security [Adler, 2005; Hill, 2001; Matsumoto *et al.*, 2002], thus, it is of special relevance to understand the threats to which they are subjected and to analyze their vulnerabilities in order to prevent possible attacks and increase their benefits for the final user.

However, due to the fact that biometrics, as an automatic means of human recognition, constitutes a relatively novel field of research, most efforts undertaken by the different parties involved in the development of this technology (researchers, industry, evaluators, etc.) have been mainly (but not exclusively) directed to the improvement of its performance (i.e., finding ways to obtain lower error rates). This has left partially uncovered other important areas such as the security assessment of the systems, which has been largely analyzed in other mature security technologies (e.g., cryptography), where precise standards and procedures exist for the systematic and independent evaluation of the applications.

Thus, it is of great importance for the definitive introduction of biometric systems in the security market, to develop a common framework to evaluate the security capabilities of this new technology in comparison with other existing and tested security methods. In this context, in addition to the creation of specific laboratories for the independent testing of biometric systems [BSI, 2009], several standardization efforts for the security evaluation within the field of Information Technologies are currently being carried out at international level. Some examples of these projects are the Common Criteria [CC, 2006], and its complementary Common Evaluation Methodology [CEM, 2006], the Biometric Evaluation Methodology [BEM, 2002] proposed by the English CESG Biometric Working Group [BWG, 2009] and based on the CEM, or the Common Vulnerability Scoring System [CCVS, 2007]. Very recently, the first standard specifically thought for the security evaluation of biometric-based applications has been published by the International Organization for Standardization (ISO) [ISO/IEC 19792, 2009].

All these initiatives try to cover a very wide range of systems and technologies and, thus, they give very general directives about the different aspects to be taken into account in a security evaluation. For this reason there is a big need for complementary documents (such as the Supporting Documents [CC, 2009b] and the Protection Profiles [CC, 2009a] of the Common Criteria - CC) that help all the interested parties (developers, vendors, and evaluators) to apply the indications given in the general norms to the particular specificities of a given technology.

The generation of these complementary documents is specially important in the biometric field due to the large amount of different existing biometric modalities, and the multiple areas of knowledge that it covers (pattern recognition, computer vision, electronics, etc.) However, in spite of this necessity, not enough effort has been made within the biometric community in this direction, resulting in many cases in the inaccurate perception by the users that the security level provided by biometric systems is lower than the one offered by other long-used security technologies.

Although some biometric products have already been certified following some of these initiatives (specifically the Common Criteria, e.g., [Canadian Certification Body, 2001; German Certification Body, 2008]), there is still a long way to go before security certification of biometric systems is a common and extended practice as it occurs in other Information Technologies. This PhD Thesis pretends to bring some insight into the difficult problem of biometric security evaluation through the systematic study of biometric systems vulnerabilities and the analysis of effective countermeasures that can minimize the effects of the detected threats, in order to increase the confidence of the final users in this thriving technology. This way, the experimental studies presented in this Dissertation can help to further develop the ongoing standardization efforts for the security evaluation of biometric systems.

1.1. Biometric Systems

A biometric system is essentially a pattern recognition system that makes use of biometric traits to recognize individuals. The objective is to establish an identity based on '*who you are or what you produce*', rather than by '*what you possess*' or '*what you know*'. This new paradigm not only provides enhanced security but also avoids, in authentication applications, the need to remember multiple passwords and maintain multiple authentication tokens. 'Who you are' refers to *physiological* characteristics[1] such as fingerprints, iris, or face. 'What you produce' refers to *behavioral* patterns which entail a learning process and that characterize your identity such as the voice or the written signature.

The digital representation of the characteristics or features of a biometric trait is known as *template*. Templates are stored in the system database through the *enrollment* or *training* process, which is depicted in Figure 1.1 (top). The database can either be centralized (this is the case of most biometric systems working at the moment), or distributed (as in Match-on-Card systems where each user carries the only copy of his template in a personal card [Bergman, 2008]). Once the users have been enrolled to the system, the recognition process can be performed in two modes [Jain *et al.*, 2006]:

- **Identification**. In this mode, the question posed to the system is: is this person in the database?, the answer might be 'No' (the person is unknown to the system), or any of

[1] Although the term *physiological characteristic* is commonly used when describing biometrics, the purpose is to refer to the morphology of parts of the human body, therefore the proper term is *morphological characteristic*.

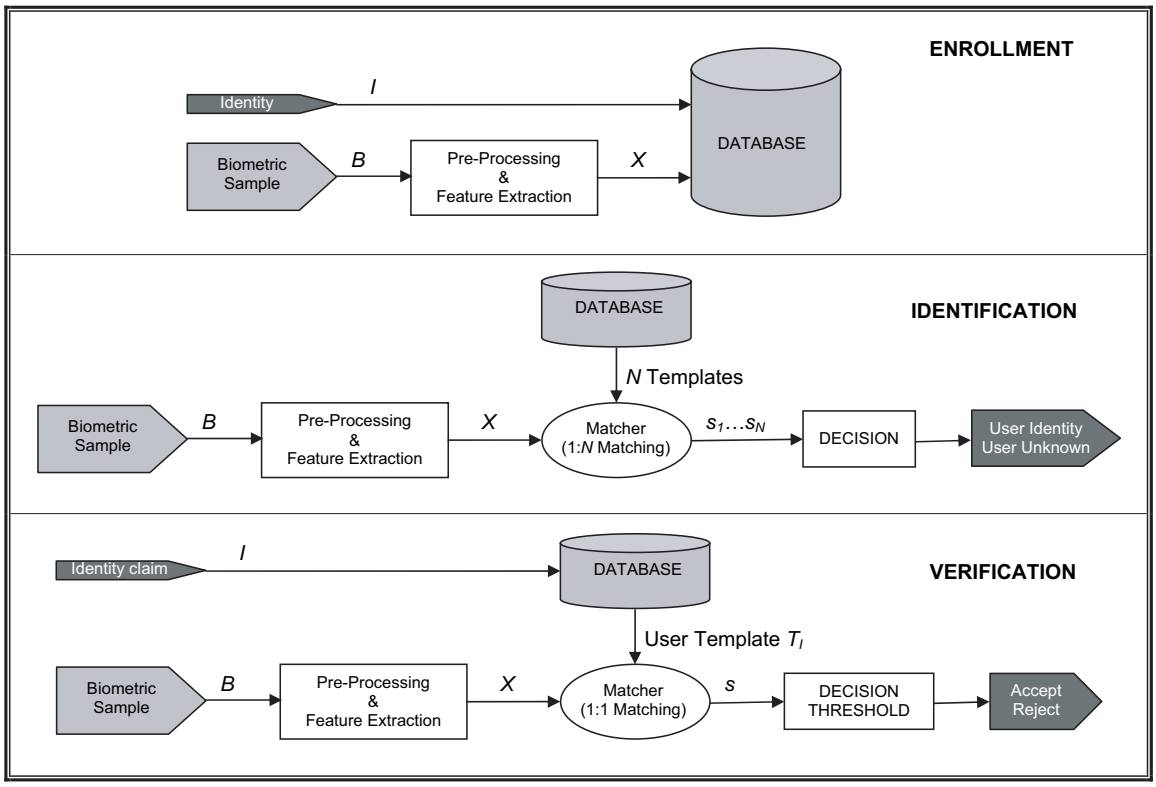


Figure 1.1: *Diagrams of the typical modes of operation in a biometric system.*

the registered identities in the database. In order to give the answer the system has to perform a "one to many" matching process, as it has to compare the input biometric to all the stored templates (Fig. 1.1, center).

In most practical cases, under the identification operation mode, the system usually returns, in a ranked manner, those identities that are more likely to be the searched person (i.e., those that have produced a higher similarity score), and then a human expert decides whether the subject is or not within that reduced group of people. Typical identification applications include Automated Fingerprint Identification Systems [Komarinski, 2005].

- **Verification**. In this case what we want to know is if a person is really who she claims to be (i.e., is this person truly E. Nigma?). This way, under the verification mode (Fig. 1.1, bottom), the system performs a "one to one" matching process where the submitted biometric trait is compared to the enrolled pattern associated with the claimed identity, in order to determine if the subject is a *client* (the identity claim is *accepted*), or an *impostor* (the identity claim is *rejected*). Typical verification applications include network logon, ATMs, physical access control, credit-card purchases, etc.

This Thesis is focused on the security evaluation of biometric systems working under the verification mode (also known as *authentication*). In this mode, the *clients* or *targets* are known to the system (through the enrollment process), whereas the *impostors* can potentially be the

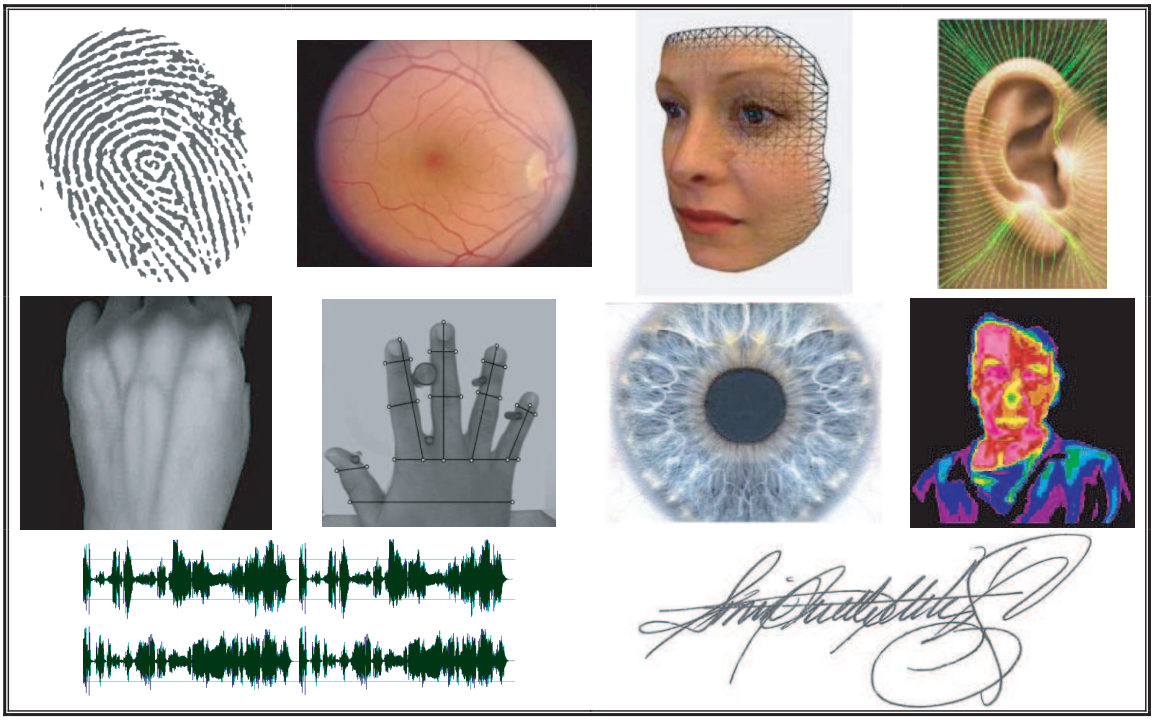


Figure 1.2: *Examples of common biometrics.*

world population. The result of the comparison between the feature vector X (extracted from the biometric sample B provided by the user) and the template T_I corresponding to his/her claimed identity I is a similarity score s which is compared to a decision threshold. If the score is higher than the decision threshold, then the claim is accepted (client), otherwise the claim is rejected (impostor).

1.1.1. Biometric Modalities

A number of different biometrics have been proposed and are used in various applications [Jain *et al.*, 2006]. As mentioned before, biometric traits can be classified into *physiological* biometrics (also known as *anatomical* or *morphological*) which include images of the ear, face, hand geometry, iris, retina, palmprint or fingerprint, and *behavioral* biometrics including voice, written signature, gait or keystroking. This classification is just indicative, as some of the traits are not easy to categorize in any of the groups. The voice, for instance, is commonly accepted to be a behavioral biometric (as the voice is something that we *learn* to *produce*), however its distinctiveness largely depends on physiological characteristics (e.g., vocal tracts, mouth, nasal cavities, or lips). On the other hand, other very distinctive human feature, the DNA, is usually not considered a biometric modality as recognition systems based on it still require manual operation and cannot be used in (pseudo) real-time. Example images from various biometrics are given in Fig. 1.2.

In theory, any human characteristic can be used as a biometric identifier as long as it satisfies

these requirements:

- **Universality**, which indicates to what extent a biometric is present in the world population.
- **Distinctiveness**, which means that two persons should have sufficiently different biometrics.
- **Permanence**, which indicates that the biometric should have a compact representation invariant over a sufficiently large period of time.
- **Collectability**, which refers to the easiness of the acquisition process and to the ability to measure the biometric quantitatively.

Other criteria required for practical applications include:

- **Performance**, which refers to the efficiency, accuracy, speed, robustness and resource requirements of particular implementations based on the biometric.
- **Acceptability**, which refers to which people are willing to use the biometric and in which terms.
- **Circumvention**, which reflects the difficulty to fool a system based on a given biometric by fraudulent methods.
- **Exception handling**, which has to do with the possibility to complete a manual matching process for those people that cannot interact in a normal way with the system (e.g., impossibility to perform the feature extraction process due to an excessive degradation of the trait).
- **Cost**, which refers to all the costs that would be necessary to introduce the system in a real-world scenario.

An ideal biometric system should meet all these requirements, unfortunately, no single biometric trait satisfies all the above mentioned properties. While some biometrics have a very high distinctiveness (e.g., fingerprint or iris), they are relatively easy to circumvent (e.g., using a gummy finger, or an iris printed photograph). On the other hand, other biometrics such as the face thermogram or the vein pattern of the retina are very difficult to circumvent, but their distinctiveness is low and are not easy to acquire.

1.2. Security Related Issues in Biometric Systems

First of all, it is important to remember that absolute security does not exist: given funding, willpower and the proper technology, nearly any security system can be compromised. However,

the objective of the security community should be to develop such applications that the funding, the will, and the resources needed by the attacker to break the system prevent him from attempting to do so.

In the next sections a number of security related issues are discussed in order to clarify the perspective followed during the development of the Thesis, and to define our position within the complex field of security research.

1.2.1. Transparency vs Obscurity

When addressing the problem of providing a security service, two main approaches may be adopted to guarantee that the level of security offered to the user is not compromised: *security through obscurity* (also *security by obscurity*) or *security through transparency* (also known as *security by design*).

The security through obscurity principle relies on secrecy (of design, implementation, formats and protocols used, etc.) to provide security. A system using this approach may have theoretical or practical security vulnerabilities, but its designers believe that attackers are unlikely to find or to exploit them. Developers supporting this methodology argue that if details of countermeasures employed in biometric systems are publicized, it may help attackers to avoid or defeat them. Similarly, if attackers know what countermeasures are not employed, this will help them to identify potential weaknesses in the system, enabling the attacks towards those weak areas. Furthermore, an attacker's first step is usually information gathering; this step is delayed by security through obscurity.

In opposition, the security through transparency scheme follows the Kerckhoffs' principle (stated by Auguste Kerckhoffs in the 19th century) [Kerckhoffs, 1883]: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Although it was first thought for cryptography, the principle was later reformulated to be applied to any security system as "the enemy knows the system". Undoubtedly, any security system depends on keeping *some* things secret, the question is, *what* things?. The Kerckhoffs' principle points out that the things which are kept secret ought to be those which are least costly to change if inadvertently disclosed. In other words, the fewer and simpler the things one needs to keep secret in order to ensure the security of the system, the easier it is to maintain that security. Quoting B. Schneier, one of the world's leading security technologists, "*Kerckhoffs' principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness —and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility*" [Schneier, 2000].

Applying security through transparency to biometrics would mean, in words of the Biometric Working Group [BWG, 2009]: "*make public exposure of countermeasures and vulnerabilities which will lead to a more mature and responsible attitude from the biometrics community and promote the development of more secure systems in the future*" [BWG, 2003].

Our view on biometric security, based on which this Thesis has been developed, is aligned

with the security through transparency principle. This way, throughout the Dissertation different threats that may affect biometric systems are pointed out, systematically evaluated, and new countermeasures that can guarantee the final level of security offered to the user are proposed.

That does not mean that obscurity cannot provide any protection, rather that the protection is unpredictable (you cannot guarantee that an attacker will not find out your secrets) and most probably temporary. We believe that in order to make biometric devices and applications secure it is necessary to understand the threats and put in place effective countermeasures, technical and procedural. As commented before, a parallel may be drawn with other mature Information Technologies where vulnerabilities have been long-analyzed and where knowledge is no suppressed. Rather, the approach is to report problems to the developers so that they can be fixed and patches issued.

Of course, we cannot forget that biometrics is not cryptography. Biometric traits are unique identifiers, but they are not secrets as cryptographic keys [Schneier, 1999], (everybody knows our face, or could get our fingerprints) so they cannot be treated as such. Thus, the secrecy requirements for biometric systems might differ from those that apply to cryptography. In particular, Kerckhoffs' Principle generalizes to the following design guideline applicable to biometrics: minimize the number of secrets in your security system. To the extent that you can accomplish that, you increase the robustness of your security. To the extent you cannot, you increase its fragility.

In the end, a balance between (excessive) publicity and knowledge suppression has to be met, founded, as in other areas, on pragmatic principles based on experience. For biometrics, a similar approach can be expected to be adopted. We believe, as many other parties [BWG, 2003], that tracking down threats, evaluating vulnerabilities, and proposing countermeasures, is the path that leads to a stronger and more robust biometric technology. This is the path followed in this Thesis.

1.2.2. Security Evaluation vs Vulnerabilities Evaluation

There is often a tendency to focus on a few specific issues when security is discussed. The subject of biometrics is particularly prone to this (the question, *what about spoofing*? usually surfaces quickly). This approach however runs the risk of overlooking the far more complex set of factors that determine effective security in real world applications.

In a security evaluation all the security issues related to the final application should be clearly understood and analyzed. This includes all the different elements involved in providing a high quality service to the final user, and which include not only the individual modules comprised within the biometric system, but also other hardware and software components, the communication channels in between elements of the application, the operating environment, and the different processes and protocols defined in order to give the global security functionality. This implies that the overall security evaluation of a complete application is not reduced to the vulnerability assessment of individual components but covers a very wide range of aspects that go from technical, to environmental, behavioral or procedural issues. Therefore, in practice,

certain components vulnerabilities might not be possible to be exploited due to the interactions with other application elements, or to the particular conditions of the real scenario where the application will be operating.

This Thesis is focused on the study and statistical analysis of biometric-specific vulnerabilities of biometric systems (other non-biometric dangers that may affect the different modules of the system are not considered). As pointed out before, *biometric systems* are the main but not the only component of a *security application*, hence, when performing the security testing of an overall application evaluators should determine whether non-biometric specific threats have any effect on the functionality of the biometric system, or if, on the other hand, specific biometric vulnerabilities have a harmful impact on other elements of the application.

Similarly, only specific biometric-based countermeasures for the detected vulnerabilities are explored. However, although not studied, other non-biometric countermeasures could be applicable for some of the attacks.

As discussed above, from a strict point of view, vulnerability testing is just one of the tasks to be performed within a security evaluation. However, throughout this Dissertation either terms (vulnerability and security evaluation) are used interchangeably to refer to *vulnerability assessment* (also *vulnerability evaluation*).

1.3. Motivation of the Thesis

Provided that security evaluation is a key issue for the acceptance of any security-based technology among the final users, and that biometric technology is a very powerful tool for security applications where human identification is needed, this Thesis is focused on the vulnerability assessment of biometric systems. The research carried out in this area has been mainly motivated by five observations from the state-of-the-art.

First, although several works have already studied different specific vulnerabilities of biometric systems [Hennebert *et al.*, 2007; Hill, 2001; Thalheim and Krissler, 2002], the problem has been addressed on most cases from a *yes-or-no* perspective (i.e., the question being answered is, *can a biometric system be bypassed using this attacking method?*). However, in most of those valuable research contributions, a far more complex question remains unanswered: ***how*** *vulnerable is the biometric system to the attack?*. Identifying the threats is the first stage in a vulnerability evaluation, however quantifying the danger is just as important in order to assess the security level provided by the application.

The second observation is strongly related to the first one. In these existing publications, experimental results are obtained and reported without following any general or systematic protocol, and thus, even in the case of performing an statistical analysis of a given vulnerability, results cannot be compared, losing this way part of their utility.

The third observation comes from the different initiatives that are currently trying to develop standard security evaluation protocols [BEM, 2002; CC, 2006; ISO/IEC 19792, 2009]. These standards are in general directed to the very wide range of Information Technology security

products, which means that additional documents are required in order to apply the general guidelines given in the norms to the particular specificities of a given technology (e.g., with practical evaluation examples, lists of possible threats and vulnerabilities, etc.) This is specially important in the biometric field due to the large amount of different existing biometric modalities (e.g., fingerprints, face, iris, handwritten signature, etc.), and the multiple areas of knowledge that it covers (pattern recognition, computer vision, electronics, etc.)

The fourth observation that has motivated this Thesis is the constant need to search for new weak points in security applications (and in this particular case, in biometric systems), in order to make them public and motivate the industry to look for solutions to the threat. This observation is aligned with the security principle (largely applied in other areas such as cryptography) *security through transparency* [Kerckhoffs, 1883], which pleads for making security systems as public as possible. This paradigm relies on the fact that vulnerabilities exist regardless of their publication, therefore: let's face the problems and find solutions for them (controlled risk), before somebody else finds the way to take advantage of our secrets (unpredictable consequences).

The last observation is that the development of new countermeasures for the studied biometric vulnerabilities is currently a research challenge. Although different efforts have been carried out in this direction [Adler, 2004; Jain *et al.*, 2008a; Schuckers, 2002], there is still no definitive solution for some of the analyzed security breaches, and new ways to protect the systems should be designed against the detected vulnerabilities.

1.4. The Thesis

The Thesis developed in this Dissertation can be stated as follows:

> *Searching for new threats (can the system be broken using this attacking approach?), evaluating those vulnerabilities following a systematic and replicable protocol (how vulnerable is the system to this approach?), proposing new countermeasures that mitigate the effects of the attack, and publicly reporting the results of the whole process, help to develop a more mature and secure biometric technology.*

1.5. Outline of the Dissertation

The main objectives of the PhD Thesis are as follows: 1) reviewing and studying the problem of vulnerability assessment in biometric systems in order to identify and evaluate new possible threats; 2) devising practical countermeasures for the analyzed security breaches in order to enhance the robustness of biometric systems against attacks; and 3) applying the proposed techniques and methodologies to common scenarios, systems, and databases widely available for the biometrics research community, with emphasis on fingerprint, signature, and face verification systems.

The Dissertation is structured according to a traditional complex type with background theory, practical methods, and three independent experimental studies in which the methods are applied [Paltridge, 2002]. The chapter structure is as follows:

- Chapter 1 introduces the topic of security in biometric systems and gives the motivation, outline and contributions of this PhD Thesis.
- Chapter 2 summarizes related works which have given rise to the motivations of the Thesis.
- Chapter 3 considers the issue of performance evaluation in biometric systems and presents the common methodology followed in the Dissertation for security evaluation of biometric systems. The biometric databases used in this Dissertation are also introduced.
- Chapter 4 introduces three novel methods proposed in the framework of this Thesis and that are later used in the experimental part of the Dissertation. These methods are: *i*) a new hill-climbing attacking approach based on Bayesian adaptation, *ii*) a liveness detection technique for fingerprint recognition systems based on quality measures capable of countermeasuring spoofing attacks, and *iii*) a synthetic handwritten signature generation algorithm based on spectral analysis (useful both for vulnerability assessment and attack protection).
- Chapter 5 studies the problem of vulnerability assessment in fingerprint recognition systems, revealing a new security breach in applications using standard ISO templates without encryption. Different countermeasures for the studied attacks are analyzed, including the liveness detection method based on quality measures proposed in Chapter 4, and score quantization against hill-climbing attacks.
- Chapter 6 studies the problem of vulnerability assessment in signature recognition systems, using for this purpose the Bayesian-based hill-climbing attack and the synthetic generation method proposed in Chapter 4. Different countermeasures are analyzed for the considered attacks, including selection of robust features and enrollment enhancement with synthetic data.
- Chapter 7 studies the problem of vulnerability assessment in face recognition systems. The Bayesian-based hill-climbing attack, previously studied against signature-based systems, is successfully applied here thus proving its versatility and its high attack potential. Score quantization is also explored as a way to minimize the effects of the attack.
- Chapter 8 concludes the Dissertation summarizing the main results obtained and outlining future research lines.

The dependence among the chapters is illustrated in Fig. 1.3. For example, before reading any of the experimental Chapters 5, 6 and 7 (shaded in Fig. 1.3), one should read first Chapters 3 and 4. Before Chapter 3 one should start with the introduction in Chapter 1, and

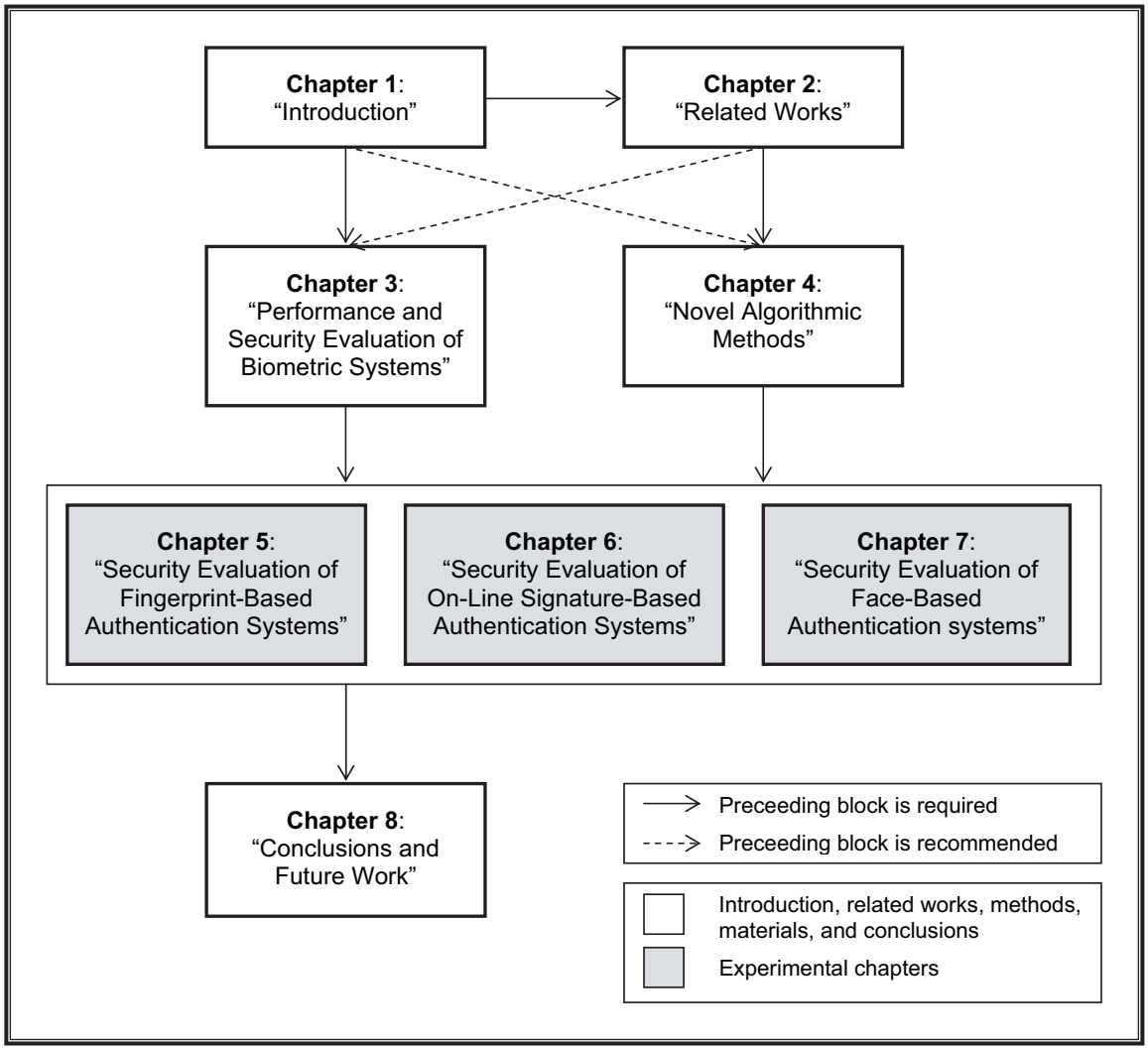


Figure 1.3: *Dependence among Dissertation chapters.*

the recommendation of reading Chapter 2. Following the guidelines given in Fig. 1.3 and assuming a background in biometrics [Jain *et al.*, 2006], the experimental chapters can be read independently.

The methods developed in this PhD Thesis are strongly based on popular approaches from the pattern recognition literature. The reader is referred to standard texts for a background on the topic [Duda *et al.*, 2001; Theodoridis and Koutroumbas, 2006]. This is especially useful for dealing with Chapter 4. Chapters 4 and 5 assume a knowledge of the fundamentals of image processing [Gonzalez and Woods, 2002], and computer vision [Bigun, 2006b].

1.6. Research Contributions

The research contributions of this PhD Thesis are as follows (for clarity the publications repeated in different items of the list appear as citations, journal papers included in ISI JCR appear in bold):

- LITERATURE REVIEWS.

1. Direct and indirect attacks to biometric systems.

   - J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez. Fake fingertip generation from a minutiae template. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 1–4, 2008a. (IBM Best Student Paper Award).
   - **J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters*, 2009b. Invited paper. To appear.**
   - **J. Galbally, C. McCool, J. Fierrez, and S. Marcel. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, 2010. To appear.**

2. Liveness detection approaches.

   - J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. Fingerprint liveness detection based on quality measures. In *Proc. IEEE Int. Conf. on Biometrics, Identity and Security (BIdS)*, 2009a.

3. Synthetic generation of biometric traits.

   - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Synthetic generation of handwritten signatures based on spectral analysis. In *Proc. SPIE Biometric Technology for Human Identification VI (BTHI VI)*, 2009f.

4. Multimodal biometric databases.

   - J. Galbally, J. Fierrez, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano-Rey, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, and C. Orrite-Uruñuela. Biosecurid: a multimodal biometric database. In *Proc. MADRINET Workshop*, pages 68–76, 2007d.

- NOVEL METHODS.

  1. Novel hill-climbing attack based on Bayesian adaptation.

     - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 386–395. Springer LNCS-4642, 2007b.
     - **[Galbally *et al.*, 2010].**

  2. Novel on-line signature synthetic generation method based on spectral analysis.

     - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Improving the enrollment in dynamic signature verification with synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009e.
     - [Galbally *et al.*, 2009f].

  3. Novel liveness-detection approach for fingerprint recognition based on quality measures.

     - [Galbally *et al.*, 2009a].

- NEW BIOMETRIC DATA.

  1. A large multimodal biometric database (BiosecurID) including eight different modalities from 400 subjects collected on four acquisition sessions was acquired in the framework of this PhD Thesis.

     - **J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications*, 2009. To appear.**

  2. A database of over 800 fingerprint images coming from 68 different subjects, and as many fake samples captured from the corresponding gummy fingers generated with and without cooperation of the user (i.e., 800 real images, 800 fake images with cooperation, and 800 fake samples without cooperation).

     - J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador. On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, volume 1, pages 130–136, 2006.

- NEW EXPERIMENTAL STUDIES

  1. Direct attacks to fingerprint-based recognition systems using gummy fingers generated with and without the cooperation of the user.

     - [Galbally *et al.*, 2006].

2. Direct attacks to fingerprint-based recognition systems using gummy fingers generated from standard ISO minutiae templates.

   - [Galbally *et al.*, 2008a].
   - **[Galbally *et al.*, 2009b]**.

3. Indirect hill-climbing attacks to biometric systems based on on-line signature verification.

   - [Galbally *et al.*, 2007].

4. Indirect hill-climbing attacks to face-based verification systems.

   - [Galbally *et al.*, 2010].

5. Brute-force attacks to biometric systems based on on-line signature verification using synthetic samples.

   - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Evaluation of brute-force attack to dynamic signature verification using synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Machine Intelligence (ICDAR)*, 2009d.

6. Comparative study of the most robust and best performing global features for on-line signature verification systems.

   - J. Galbally, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. Feature selection based on genetic algorithms for on-line signature verification. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 198–203, 2007a.
   - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Performance and robustness: a trade-off in dynamic signature verification. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1697–1700, 2008b.

7. Enrollment and performance improvement in on-line signature verification systems using synthetic samples.

   - [Galbally *et al.*, 2009e].

Other contributions so far related to the problem developed in this Thesis but not presented in this Dissertation include:

- LITERATURE REVIEWS.

1. Recent advances in multimodal biometric databases.

   - **J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. W. R. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran. The multi-scenario multi-environment BioSecure multimodal database (BMDB). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2009. To appear.**

2. Signature verification on handheld devices.

   - M. Martinez-Diaz, J. Fierrez, J. Galbally, F. Alonso-Fernandez, and J. Ortega-Garcia. Signature verification on handheld devices. In *Proc. MARINET Workshop*, pages 87–95, 2007.

- NOVEL METHODS.

1. Biometric hashing based on genetic selection and its application to on-line signatures.

   - M. R. Freire, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Biometric hashing based on genetic selection and its application to on-line signatures. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 1134–1143. Springer LNCS-4642, 2007.

- NEW BIOMETRIC DATA.

1. A new multimodal biometric database, collected within the Biosecure Network of Excellence [Biosecure, 2007], comprising three datasets acquired each of them in a different scenario: controlled, mobile, and internet.

   - **[Ortega-Garcia *et al.*, 2009].**

2. Database of 800 real iris images and their corresponding fake samples captured from high quality iris image impressions.

   - V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BioID)*, 2008.

- NEW EXPERIMENTAL STUDIES.

1. Classification of handwritten signatures based on name legibility and its application to privacy preserving applications.

   - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Classification of handwritten signatures based on name legibility. In *Proc. SPIE Biometric Technology for Human Identification IV (BTHI IV)*, 2007c.

2. Analysis of side-channel attacks based on the matching time to fingerprint recognition systems.

   - J. Galbally, S. Carballo, J. Fierrez, and J. Ortega-Garcia. Vulnerability assessment of fingerprint matching based on time analysis. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BIOID)*. Springer LNCS-5707, 2009c.

3. Analysis of direct attacks to iris verification systems using high quality printed images.

   - [Ruiz-Albacete *et al.*, 2008].

4. Study of the robustness of signature verification systems to direct attacks performed by imitators with increasing skills.

- F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally, and J. Ortega-Garcia. Robustness of signature verification systems to imitators with increasing skills. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009.

5. Performance of the best performing features for dynamic signature verification in mobile devices.

- M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Towards mobile authentication using dynamic signature verification: useful features and performance evaluation. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, 2008.

Chapter 2

Related Works

This chapter summarizes the works related to this PhD Thesis. We have focused on the three fields within biometrics research in which novel contributions have been made, namely: *i*) vulnerability evaluation to both direct and indirect attacks, *ii*) proposal of new countermeasures (with special attention to those related with liveness detection), and *iii*) synthetic generation of biometric traits. The aim of this chapter is not to generate a comprehensive and exhaustive review of the existing publications dealing with each of the three mentioned topics, but to summarize the most relevant works closely related to this Thesis, and which can help the reader to compose a general view of the state of the art on each of the matters (specially on those biometric traits which have been considered in the experimental part of the Thesis).

The chapter is structured as follows. First we give an overview of the most important works in the study of the vulnerabilities of biometric systems both to direct and indirect attacks (Sect. 2.1). In Sect. 2.2 we summarize the most important contributions in the countermeasures field, specifically focusing on liveness detection approaches. The next section (Sect. 2.3) is dedicated to make a summary of the most important works related to the generation of synthetic biometric traits, emphasizing those which address the problem of dynamic signature generation that has been studied in this Thesis. Finally the summary and conclusions of the chapter are presented (Sect. 2.4).

This chapter is based on the publications: Galbally *et al.* [2009a, 2006, 2010]

2.1. Vulnerabilities

In the past few years, a considerable effort has been carried out in analyzing, classifying and solving the possible security breaches that biometric verification systems may present [Adler, 2008; Buhan and Hartel, 2005; Nixon *et al.*, 2008; Ratha *et al.*, 2001b]. In Fig. 2.1 a diagram with the attack classification that will be followed in this section is shown. Attacks that will be analyzed in the experimental part of the Dissertation appear in grey.

As shown in Fig. 2.1, the attacks that can compromise the security provided by a biometric system may be categorized into two basic types [Jain *et al.*, 2006]:

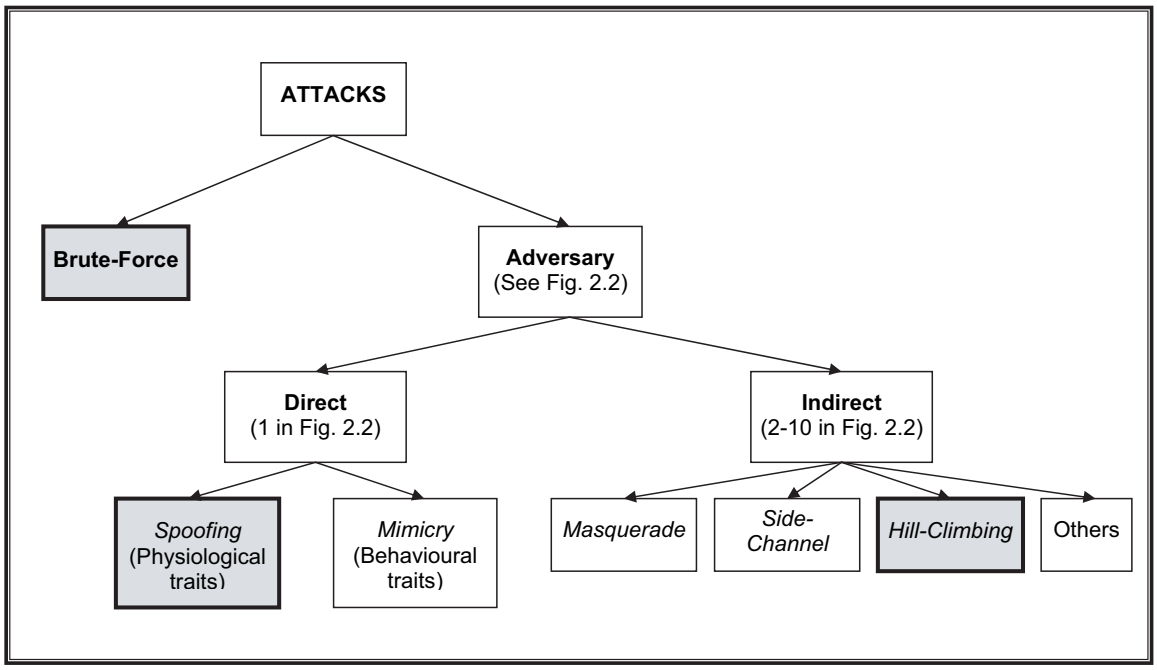


Figure 2.1: *Classification of the attacks to a biometric system as considered in Sect. 2.1. The different attacks that will be analyzed in the experimental part of the Dissertation are shadowed in grey and highlighted with a thicker frame.*

- **Brute-force attacks**: also known as *zero-effort attacks* or *intrinsic failure* [Jain *et al.*, 2008a]. This threat, impossible to prevent and present in all biometric systems, is derived from the fact that there is always a non-zero probability that two biometric samples coming from two different subjects are sufficiently alike to produce a positive match (the same way that there is a non-zero probability of guessing by chance a four digit PIN). This probability mainly depends on the system accuracy and on the biometric trait individuality [Kholmatov and Yanikoglu, 2008; Pankanti *et al.*, 2002]. In these type of attacks the impostor uses the system in a normal and straight forward manner.

- **Adversary attacks**: this refers to the possibility that a malicious subject (attacker), enrolled or not to the application, tries to bypass the system interacting with it in a way for which it was not thought (e.g., hacking an internal module, using a fake biometric trait, deliberately manipulating his biometric trait to avoid detection, etc.)

As brute-force vulnerabilities are inherent to the statistical nature of biometric systems, the biometric community has focused in the study of adversary attacks, which have been systematically categorized in eight classes by Ratha *et al.* [2001a] depending on the point to which they are directed. A total 10 points of attack are depicted in Fig. 2.2, where the first eight correspond to those introduced by Ratha *et al.* [2001a], and the last two are similar to attacks 4 and 5. These adversary attacks can be grouped in direct and indirect attacks as follows (see Fig. 2.2):

- **Direct attacks**. These threats correspond to type 1 in Fig. 2.2 and are aimed directly

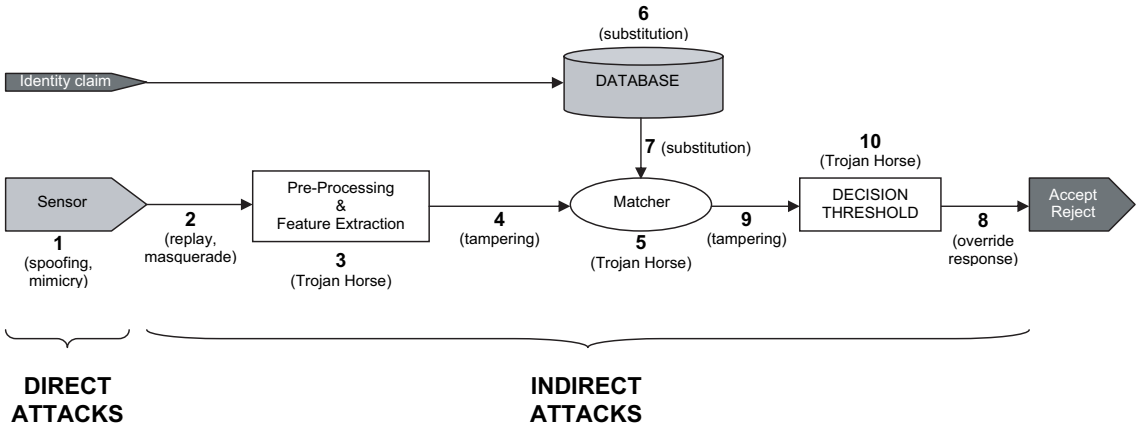


Figure 2.2: *Architecture of an automated biometric verification system. Possible adversary attack points are numbered from 1 to 10. The first eight are taken from [Ratha et al., 2001a], while points 9 and 10 are similar to attacks 4 and 5. The direct and indirect attacks classification is also shown.*

to the sensor trying to gain access to the system by impersonating a real user [Schuckers, 2002]. When they are executed against a biometric system working on a physiological trait (e.g., fingerprint, iris, face) they are also known as *spoofing* and try to enter the system by presenting a fake biometric trait or *artefact* (e.g., gummy finger, high quality iris or face image) to the acquisition device [Lane and Lordan, 2005; Thalheim and Krissler, 2002]. In the case of biometric systems based on behavioural traits (e.g., signature, voice) these type of approaches are known as *mimicry*, where the attacker tries to break the system by imitating the legitimate user producing the so-called *skilled forgeries* [Eriksson and Wretling, 1997; Hennebert *et al.*, 2007]. It is worth noting that in this type of attacks no specific knowledge about the system is needed (matching algorithm used, feature extraction, feature vector format, etc.) Furthermore, the attack is carried out in the analog domain, outside the digital limits of the system, so the digital protection mechanisms (digital signature, watermarking, etc.) cannot be used.

- **Indirect attacks**. This group includes all the remaining nine points of attack identified in Fig. 2.2. Attacks 3, 5 and 10 might be carried out using a *Trojan Horse* that replaces the feature extractor, the matcher, or the decision threshold respectively, and outputs a feature vector, matching score, or final decision different from the original. In attack 6 the system database is manipulated (a template is changed, added or deleted) in order to gain access to the application (also known as *substitution* attack [Ratha *et al.*, 2001b], it can also be executed as a type 7 attack between the database and the matcher). The remaining points of attack (2, 4, 7, 8 and 9) are thought to exploit possible weak points in the communication channels of the system, extracting, adding or changing information from them.

  These indirect attacks are also classified in the bibliography in terms of the techniques that might be used to carry them out [Ratha *et al.*, 2001b]: *replay attacks* (type 2, a recorded

or synthetic image is injected in the system), *masquerade attack* (type 2, an image is reconstructed from a compromised template and submitted to the system bypassing the sensor), *tampering* (type 4 and 9, feature vectors are modified in order to obtain a high verification score, or the matching score is directly altered), and *overriding response* (type 8, the accept/reject answer from the system is changed).

In opposition to attacks at the sensor level, in the indirect attacks the intruder needs to have some additional information about the internal working of the recognition system and, in most cases, physical access to some of the application components (feature extractor, matcher, database, etc.) is required.

Maltoni *et al.* [2003] have furthermore listed the threats that may affect any security application, not only based on biometric recognition. Among all the possible attacks several are emphasized, namely: *i*) *Denial of Service* (DoS) where the attacker damages the system so that it can no longer be accessed by the legal users, *ii*) *circumvention*, in this case an unauthorized user gains access to the system, *iii*) *repudiation*, in this type of threat it is the legitimate user who denies having accessed the system, *iv*) *contamination or covert acquisition*, this is the case of the direct attacks identified by Ratha *et al.* [2001a], *v*) *collusion*, in this attack a user with special privileges (e.g. administrator) allows the attacker to bypass the recognition component, *vi*) *coercion*, legitimate users are forced to help the attacker enter the system. For security systems based on biometric recognition the contamination and circumvention attacks can be identified respectively with the direct and indirect attacks previously mentioned.

In the next sections (Sect. 2.1.1 and 2.1.2) a summary of the most representative works related to the direct and indirect attacks considered in the experimental part of the Thesis is given.

2.1.1. Direct Attacks

It has been shown in several works, not always in a systematic and replicable way, that a biometric system can be fooled by means of presenting a synthetic trait to the sensor. Although special emphasis has been made in the study of spoofing techniques for fingerprint-based recognition systems [Matsumoto *et al.*, 2002], different contributions can be found describing direct attacks to biometric systems based on iris [Thalheim and Krissler, 2002], face [Lewis and Statham, 2004], signature [Hennebert *et al.*, 2007], or even hand geometry and vein pattern [Geradts and Sommer, 2006].

2.1.1.1. Fingerprint

The first effort in biometric spoofing can be traced back to the 1920s and was executed by Wehde and Beffel [1924], who used his knowledge in photography and engraving to generate gummy fingers from latent prints. Using forensic techniques the latent fingerprint was highlighted and a photograph taken. That picture was later used to engrave a copper plate that could be used to leave false latent fingerprints on objects.

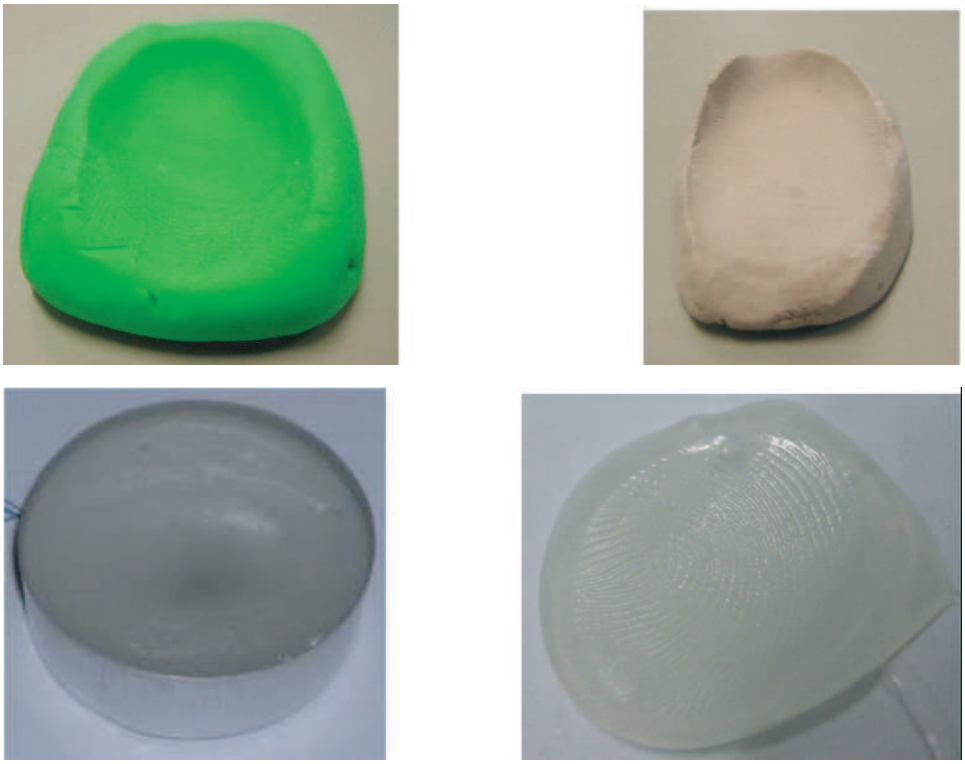


Figure 2.3: *Molds of different materials for the generation of gummy fingers with a cooperative user. Figure extracted from [Wiehe* et al.*, 2004].*

In modern times, one of the first published evaluations of fingerprint based recognition systems against spoofing methodologies was carried out by Willis and Lee [1998]. More recently, Van der Putte and Keuning [2000] and Matsumoto *et al.* [2002] carried out independent studies where several widely available biometric fingerprint sensors were put to test showing that false artificial fingers made with soft materials were able to fool the different systems. The authors classified the different methods to create gummy fingers in two main categories:

- **Cooperative acquisition**. In this case the legitimate user takes part in the attack by placing his finger in a small amount of suitable material such as wax or molding silicone; the impression creates a mold from which artificial fingers can be cast.
- **Non-cooperative acquisition**. It is unlikely that in a real-world scenario a user would voluntarely allow to produce an artificial copy of his fingerprints. In this case the gummy fingers can be generated using a similar process to that introduced by Wehde and Beffel [1924]. Once the latent fingerprint has been lifted it can be printed on to a Printed Circuit Board (PCB) that will serve as mould to produce the artefact.

Similar works testing different well-known sensors (including devices produced by Biometrika, Digital Persona, Fujitsu, Identix, Siemens or Precise Biometrics) and using several attacking methods and materials to generate the gummy fingers have been later published [Blomme, 2003;

Gronland *et al.*, 2005; Kakona, 2001; Kang *et al.*, 2003; Thalheim and Krissler, 2002; Wiehe *et al.*, 2004]. Different molds used in [Wiehe *et al.*, 2004] for the generation of fake fingers following a cooperative acquisition procedure are shown in Fig. 2.3.

2.1.1.2. Face

In the case of face recognition systems, face photographs of the legitimate users have been used to test their robustness against direct attacks [Thalheim and Krissler, 2002]. Different 2D facial biometric systems were spoofed by presenting these simple images of the users to the sensor, or even very basic drawings of a human face [Lewis and Statham, 2004]. A more sophisticated attack using a laptop monitor where a face video is played was reported by Thalheim and Krissler [2002].

2.1.1.3. Signature

In signature-based systems direct attacks are performed by means of accurately imitating the real user's signature (i.e., mimicry) producing the so called skilled-forgeries. Different studies have been conducted to determine the vulnerabilities of signature recognition systems to forgeries produced with an increasing level of skill [Alonso-Fernandez *et al.*, 2009; Hennebert *et al.*, 2007].

2.1.2. Indirect Attacks

Although Hill [2001] reported an attack to a biometric system database (type 6 attack in Fig. 2.2) in which the compromised templates were used to carry out a masquerade attack to the input of the feature extractor (type 2 attack), most of the works regarding indirect attacks use some type of variant of the hill-climbing technique introduced by Soutar *et al.* [1999]. In this preliminary work a basic *hill-climbing attack* is tested over a simple image recognition system using filter-based correlation. This attack takes advantage of the score given by the matcher (type 9 attack) to iteratively change a synthetically created template until the score exceeds a fixed decision threshold and the access to the system is granted. Thus, depending on whether we create a synthetic image file or we directly generate the synthetic feature vector, these attacks can belong to type 2 (*replay* attack) or 4 (*tampering*), respectively.

When the hill-climbing attack is directed to the input of the feature extractor (type 2 attack), no information about the template storage format is required. Only the size and file format presented to the feature extractor is needed. Adler [2003] studied a type 2 hill-climbing attack to a face recognition system. The input image is conveniently modified until a desired matching score is attained (an example execution of the attack is shown in Fig 2.4). This work reported results on three commercial recognition systems and showed that after 4,000 iterations, a score corresponding to a very high similarity confidence (99.9%) is reached for all systems tested. This work was extended to make the algorithm robust to score quantization [Adler, 2004], and then applied to attack face encrypted templates [Adler, 2005].

Figure 2.4: *Example of the attack performed in [Adler, 2003]. From left to right and top to bottom, estimated images at various iterations of the attack, average face from four different starting images, and target user. Figure extracted from [Adler, 2003].*

Face recognition systems have also been attacked using different approaches to hill-climbing algorithms. Mohanty *et al.* [2007] report a novel linear method to reconstruct face templates from matching scores that uses an affine transformation to model the behaviour of a given face recognition algorithm. The break-in scheme which showed to be robust to score quantization (as is not based on an iterative process) was tested on three different face recognition systems (including a commercial application) that were successfully broken for over 70% of the attempts.

Another hill-climbing algorithm, this time thought to exploit the vulnerabilities of minutiae-based fingerprint recognition systems was presented by Uludag and Jain [2004]. In this attack a synthetic random minutia template is presented to the input of the matcher (type 4 attack) and, according to the score generated, it is iteratively changed until the system returns a positive verification. The minutiae in the template are modified one at a time and the change is only stored if the score returned by the matcher improves the previous one, otherwise it is discarded. Thus, to carry out this type of attack we need: *i*) the resolution and size of the images captured by the sensor (which is usually a parameter specified by the vendor), *ii*) the template format, and *iii*) access to the matcher input (to present the synthetic templates) and output (to get the necessary feedback from the scores). In this case we know *how* the information is stored, but not *what* the information is.

Figure 2.5: *Two sets of four impressions coming from two different synthetic fingerprints generated with the method described in [Cappelli, 2003]. Figure extracted from [Cappelli* et al.*, 2002].*

On the other hand, Cappelli [2003] describe a fast and reliable method to generate realistic synthetic fingerprint images (two sets of synthetic fingerprint impressions are shown in Fig 2.5), which is implemented in the software tool SFinGe (Synthetic Fingerprint Generator). Using this application, a type 4 attack (to the input of the matcher) with synthetically generated templates could easily be converted to a type 2 attack (to the input of the feature extractor) using the corresponding synthetic fingerprint images. Thus, the attack would be simplified as the intruder would not need to know the storage format used in the system. Furthermore, different algorithms to reconstruct the real fingerprint image from its minutia-based template have been proposed [Cappelli *et al.*, 2007b; Hill, 2001; Ross *et al.*, 2007]. In this case, if a legitimate user's template is compromised it could be used to carry out type 2 attack against the system (reconstructing the real fingerprint image) [Cappelli *et al.*, 2007a; Hill, 2001], or even a direct attack (building a gummy fingerprint from the image). Those important threats will be studied in Sect. 5.2.

Signature-based recognition systems have also been tested against hill-climbing approaches. Yamazaki *et al.* [2005] explored, on a very limited database of Kanji signatures (Japanese-Chinese characters), the feasibility to perform these attacks against an on-line signature verification system based on Dynamic Time Warping (DTW). More recently, Muramatsu [2008] carried out similar experiments using the publicly available SVC database [Yeung *et al.*, 2004], and a private dataset collected at their laboratory (both of them comprising oriental signatures). In both works the hill-climbing attacks reach good performance results.

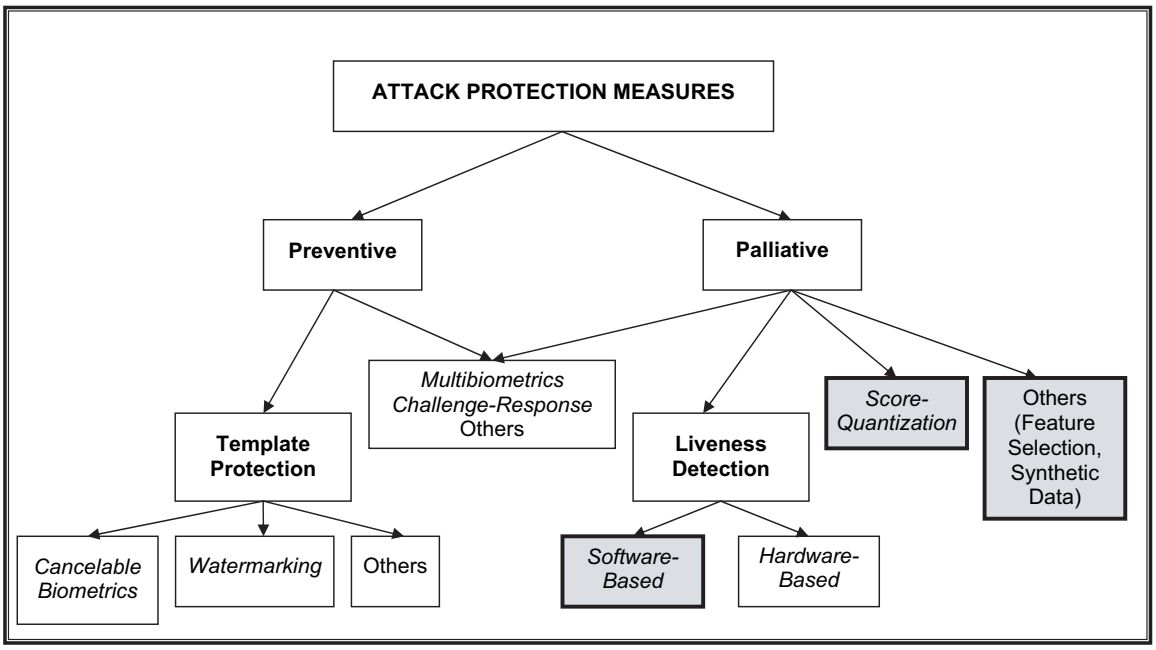


Figure 2.6: *Classification of the attack protection methods as considered in Sect. 2.2. The different approaches that will be analyzed in the experimental part of the Dissertation are shadowed in grey and highlighted with a thicker frame.*

2.1.3. Side-Channel Attacks

Although hill-climbing attacks have proven their efficiency against biometric systems, they still present the restriction of needing the score produced by the matcher to be able to break the system (which might not always be easy or even possible to obtain).

A bigger threat to biometric systems would arise if they could be attacked using some type of easily measurable information such as the matching time, or the power consumed by the system in the matching process. This type of approaches (known as *side-channel attacks*), which have recently been started to be studied in the biometric area [Galbally *et al.*, 2009c], have already been used to successfully attack cryptographic security systems [Kocher, 1995; Kocher *et al.*, 1999], and present the advantage of using parameters which are always accessible to an eventual attacker and difficult to be manipulated or distorted by the system designer (in opposition to the similarity score used in traditional hill-climbing algorithms).

2.2. Attack Protection

Different countermeasures to avoid or minimize the risks arising from adversary attacks (see Sect. 2.1) have been proposed in the literature. In Fig. 2.6 we show a general diagram of the classification followed in this section (those methods considered in the experimental part of the Dissertation are highlighted in grey).

From a general point of view, the biometric-based attack protection methods can be divided

into (see Fig. 2.6):

- **Preventive**: those aiming to avoid that a certain attack is perpetrated, and consist in general of security measures thought to offer specific protection for templates [Adler, 2008; Cavoukian *et al.*, 2008; Jain *et al.*, 2008a; Tuyls *et al.*, 2005]. These countermeasures include *cancelable biometrics*, which apply repeatable but noninvertible distortions to the biometric signal or the feature vector (i.e., their goal is to create a cancelable user biometric template that can be replaced if it is compromised) [Ratha *et al.*, 2007, 2001b; Saavides *et al.*, 2004], or *watermarking*, where extra information is embedded into the host data (e.g., eigen-face coefficients into a fingerprint image) [Jain and Uludag, 2003; Yeung and Pankanti, 2000].

- **Palliative**: those whose objective is, once the attack has been produced, to minimize its probabilities of breaking into the system. Among the palliative countermeasures to direct attacks (anti-spoofing techniques) the ones that have received more attention from researchers and industry are the *liveness detection* approaches, which use some physiological measure to distinguish between real and fake traits [Antonelli *et al.*, 2006; Tan and Schuckers, 2006](a review with the most relevant works in liveness detection is given in Sect. 2.2.1).

  Regarding indirect attacks, among other non-biometric solutions such as limiting the number of consecutive unsuccessful access attempts, a specific design of the matching algorithm can also be implemented in order to reduce the effects of this type of threats, providing this way an additional level of security. This is the case of *score quantization* which has been proposed as a biometric-based countermeasure against hill-climbing attacks [Adler, 2004]. These type of approaches try to avoid the attack by quantizing the score so that the hill-climbing algorithm does not get the necessary feedback to iteratively increase the similarity measure (the effects of score quantization as a countermeasure to hill-climbing attacks will be studied in Sects. 5.4.2 and 7.2.1.) Other techniques aimed at increasing the robustness of the system, such as feature selection of robust parameters or performance enhancement through the use of synthetic data, might also be used to prevent indirect attacks (the performance of these methods will be studied in Sect. 5.4).

The previous classification is not a closed one and certain countermeasures, depending on the architecture of the application, can be included in either groups (i.e., preventive or palliative), this is the case, for instance, of *multibiometrics* or *challenge-response* countermeasures. In *Multibiometrics* solutions, which have been proposed as an attack protection scheme against direct attacks [Chibelushi *et al.*, 2002; Namboodiri *et al.*, 2004; Prabhakar *et al.*, 2003], an accurate biometric, such as fingerprint or iris, is combined with another trait (possibly a weaker one) that is difficult to acquire covertly, such as the retina vein pattern or the face thermogram, so that the system robustness against spoofing techniques increases. In the case of *Challenge-response* schemes, the user is asked to reply (e.g., smile, blink, frown, talk, etc.) to a stimulus

coming from the system in order to detect static spoofs (e.g., face or iris images) [Daugman, 2004; Pan *et al.*, 2008]

A combination of both type of countermeasures, preventive and palliative, is the most desirable solution to reduce the vulnerabilities of biometric systems. This way, in case the preventive countermeasures are bypassed, the palliative ones will still give a good degree of protection to the user.

The group of preventive security measures (mostly template protection algorithms) represents on its own a very vast field of research which falls out of the scope of this Thesis, where we have focused in the analysis of different palliative countermeasures to reduce the risks of the studied vulnerabilities. Among others, a novel anti-spoofing approach based on liveness detection is proposed for fingerprint-based systems (see Chapter 4). In the next section we provide an overview of the most relevant works dealing with liveness assessment.

2.2.1. Liveness Detection

Two requirements have to be fulfilled by a direct attack to be successful, 1) that the attacker retrieves by some unnoticed means the legitimate user's biometric trait, and is able to generate an artefact from it (e.g., gummy finger, iris image), and 2) that the biometric system acquires and recognizes the captured sample produced with the fake trait as that of the real user. The first of the conditions is out of the reach of biometric systems designers as there will always be someone that can think of a way of illegally recovering a certain trait. Thus, researches have focused in the design of specific countermeasures that permit biometric systems to detect fake samples and reject them, improving this way the robustness of the systems against direct attacks. Among the studied anti-spoofing approaches, special attention has been paid to those known as *liveness detection* techniques, which use different physiological properties to distinguish between real and fake traits. These methods for liveness assessment represent a challenging engineering problem as they have to satisfy certain requirements [Maltoni *et al.*, 2003]:

- *Non-invasive*: the technique should in no case penetrate the body or present and excessive contact with the user.
- *User friendly*: people should not be reluctant to use it.
- *Fast*: results have to be produced in very few seconds as the user cannot be asked to interact with the sensor for a long period of time.
- *Low cost*: a wide use cannot be expected if the cost is very high.
- *Performance*: it should not degrade the recognition performance of the biometric system.

Over the last recent years different liveness detection algorithms have been proposed for traits such as fingerprint [Chen and Jain, 2005], face [Li *et al.*, 2004], or iris [Daugman, 2004]. These algorithms can broadly be divided into:

- **Software-based techniques**. In this case fake traits are detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake fingers are extracted from the fingerprint image, and not from the finger itself). These approaches include the use of skin perspiration [Tan and Schuckers, 2006], or iris texture [Wei *et al.*, 2008]. Software-based approaches can make use of *static features* being those which require one or more impressions (e.g., the finger is placed and lifted from the sensor one or more times), or *dynamic features* which are those extracted from multiple image frames (e.g., the finger is placed on the sensor for a sort time and a video sequence is captured and analyzed). In Chapter 4 of this Dissertation a novel software-based approach for liveness detection in fingerprint-based systems is proposed, and its performance further analyzed in Sect. 5.4.1.

- **Hardware-based techniques**. In this case some specific device is added to the sensor in order to detect particular properties of a living trait such as the blood pressure [Lapsley *et al.*, 1998], the odor [Baldiserra *et al.*, 2006], or the pupil hippus [Pacut and Czajka, 2006].

Software-based techniques have the advantage over the hardware-based ones of being less expensive (as no extra device in needed), and less intrusive for the user (very important characteristic for a practical liveness detection solution) [Coli *et al.*, 2008; Tan *et al.*, 2008].

2.2.1.1. Fingerprint

Different solutions for fingerprint liveness detection have been proposed in the literature. Regarding software-based approaches, two main groups can be distinguished depending on the skin features measured: those methods based on features related to the skin perspiration, and those using skin elasticity properties. In the case of hardware-based solutions, different possibilities have been explored, including the skin odor, the heart beat, or the blood pressure.

One of the first efforts in fingerprint liveness detection was carried out by Derakhshani *et al.* [2003] who initiated a research line using the skin perspiration pattern (different perspiration patterns from living fingers are shown in Fig 2.7). In this work they considered the periodicity of sweat and the sweat diffusion pattern as a way to detect fake fingerprints using a ridge signal algorithm. In a subsequent work Schuckers and Abhyankar [2004], they applied a wavelet-based algorithm improving the performance reached in their initial study, and, yet in a further step [Tan and Schuckers, 2006], they extended both works with a new intensity-based perspiration liveness detection technique which leads to detection rates between 90% and 100%. Recently, a novel region-based liveness detection approach also based on perspiration features and another technique analyzing the valley noise have been proposed by the same group [DeCann *et al.*, 2009; Tan and Schuckers, 2008].

Different fingerprint distortion models have been described in the literature [Bazen and Gerez, 2003; Cappelli *et al.*, 2001; Chen *et al.*, 2005b], which have led to the development of liveness detection techniques based on the flexibility properties of the skin [Antonelli *et al.*,

Figure 2.7: *Sweat patterns of three different real fingers. Figure extracted from [Abhyankar and Schuckers, 2005].*

Figure 2.8: *Set of frames acquired while a real (top) and fake (bottom) fingers were rotated over the surface of a fingerprint scanner. Figure extracted from [Antonelli* et al.*, 2006].*

2006; Chen and Jain, 2005; Zhang *et al.*, 2007]. In particular, the liveness detection approach proposed by Antonelli *et al.* [2006] is based on the differentiation of three fingerprint regions, namely: *i*) an inner region in direct contact with the sensor where the pressure does not allow any elastic deformation, *ii*) an external region where the pressure is very light and the skin follows the finger movements, and *iii*) an intermediate region where skin stretching and compressions take place in order to smoothly combine the previous two. In the acquisition process the user is asked to deliberately rotate his finger when removing it from the sensor surface producing this way a specific type of skin distortion which is later used as a fingerprint liveness measure (two sequences of the images produced this way by a real and fake finger are shown in Fig. 2.8). The method, which proved to be quite successful (90% detection rates of the artificial fingers are reported), was later implemented in a prototype sensor by the company Biometrika [Biometrika, 2009].

The same research group developed, in parallel to the skin elasticity method, a liveness detection procedure based on the corporal odor. Baldiserra *et al.* [2006] use a chemical sensor to discriminate the skin odor from that of other materials such as latex, silicone or gelatin. Although the system showed a remarkable performance detecting fake fingerprints made of silicone, it still showed some weakness recognizing imitations made of other materials such as gelatine, as the sensor response was very similar to that caused by human skin.

Other liveness detection approaches for fake fingerprint detection include the analysis of perspiration and elasticity related features in fingerprint image sequences [Jia and Cai, 2007], the use of electric properties of the skin [Martinsen *et al.*, 2007], using wavelets for the analysis of the finger tip surface texture [Moon *et al.*, 2005], the use of the power spectrum of the fingerprint image [Coli *et al.*, 2007], or analyzing the ring patterns of the Fourier spectrum [Jin *et al.*, 2007].

Recently, the organizers of the First Fingerprint Liveness Detection Competition (LivDet) [LivDet, 2009], have published a comparative analysis of different software-based solutions for fingerprint liveness detection [Coli *et al.*, 2008]. The authors study the efficiency of several approaches and give an estimation of the best performing static and dynamic features for liveness detection.

Outside the research field some companies have also proposed different methods for fingerprint liveness detection such as the ones based on ultrasounds [Optel, 2009; Ultra-Scan, 2009], on electrical measurements (some work has been done but apparently costs are too high), or light measurements (PosID [2009] proposed a method based on temperature changes measured on an infrared image).

2.2.1.2. Face

Different liveness detection approaches have also been proposed in order to enhance the robustness of face recognition systems to direct attacks [Pan *et al.*, 2008]. An effective way to protect against spoofs based on a static image of the face relies on the detection of motion of the facial image [Bigun *et al.*, 2004]. Another possibility is the combination of the face trait with another related and easily measurable biometric such as the voice [Chetty and Wagner, 2005; Chibelushi *et al.*, 2002]. Other works have reported good results in face liveness detection using thermal images (which are claimed to provide sufficient information to distinguish between identical twins) [Prokoski and Biel, 1999], or Fourier analysis [Li *et al.*, 2004].

2.2.1.3. Signature

When considering behavioural biometrics such as signature, the detection of attacks at the sensor level is almost impossible as, for this particular case, these threats might be considered equivalent to *zero-effort* attacks in the sense that there is no anomaly in the interaction between the attacker and the system. Thus, although some efforts have been made for the specific detection of imitations [Guo *et al.*, 2000, 2001; Nelson and Kishon, 1991], the most effective method to prevent direct attacks in biometric systems working on behavioural traits is to improve

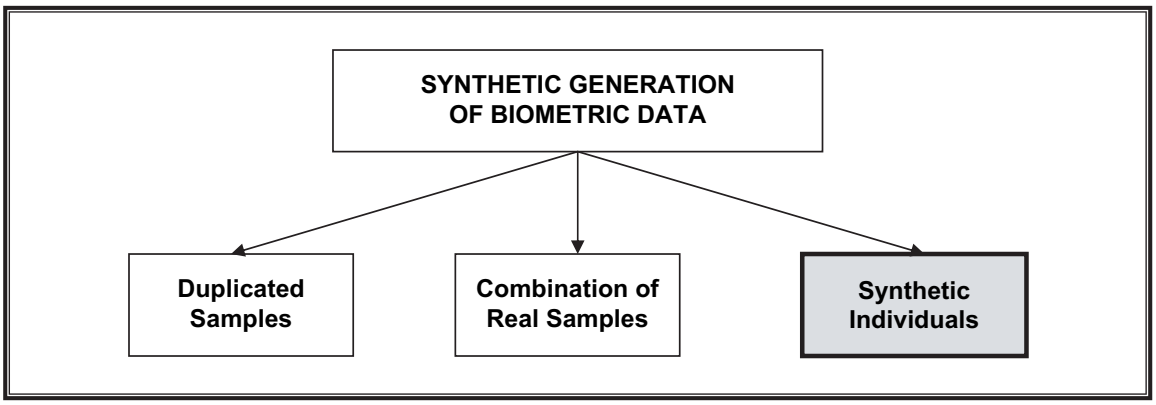


Figure 2.9: *Classification of the different methods to generate synthetic biometric data considered in Sect. 2.3. Shadowed in grey and highlighted with a thicker frame appears the class in which is included the method for the generation of synthetic on-line signatures proposed in Sect. 4.3.*

the performance of the application under the skilled forgeries scenario [Fierrez and Ortega-Garcia, 2008].

2.3. Synthetic Generation of Biometric Data

A growing interest is arising in the biometric community for the generation of synthetic biometric traits such as voice [Dutoit, 2001], fingerprints [Cappelli, 2003], iris [Zuo *et al.*, 2007], handwriting [Lin and Wang, 2007], face [Poh *et al.*, 2003], or signature [Popel, 2007]. The generation of these synthetic samples is of interest, among other applications, for performance evaluation and vulnerability assessment of biometric systems [Cappelli *et al.*, 2006b].

More specifically, synthetically generated biometric databases: *i*) facilitate the performance evaluation of recognition systems instead of the costly and time-consuming real biometric databases, and *ii*) provide a tool with which to evaluate the vulnerability of biometric systems to attacks carried out with synthetically generated traits.

It should be emphasized that, although there are multiple works which address the problem of generating synthetic traits [Orlans *et al.*, 2004; Yanushkevich *et al.*, 2007], not all of them consider the term *synthetic* in the same way. In particular, three different strategies for producing synthetic biometric samples can be found in the current literature (see Fig. 2.9):

- **Duplicated samples**. In this case the generation algorithm starts from one or more *real* samples of a given person and, through different transformations, produces different synthetic (or duplicated) samples corresponding to the same person. This type of algorithms are useful to *increase* the amount of already acquired biometric data but not to generate completely new datasets. Therefore, its utility for performance evaluation and vulnerability assessment in biometrics is very limited. On the other hand, this class of methods can be helpful to synthetically augment the size of the enrollment set of data in identification and verification systems, a critical parameter for instance in signature biometrics [Fierrez

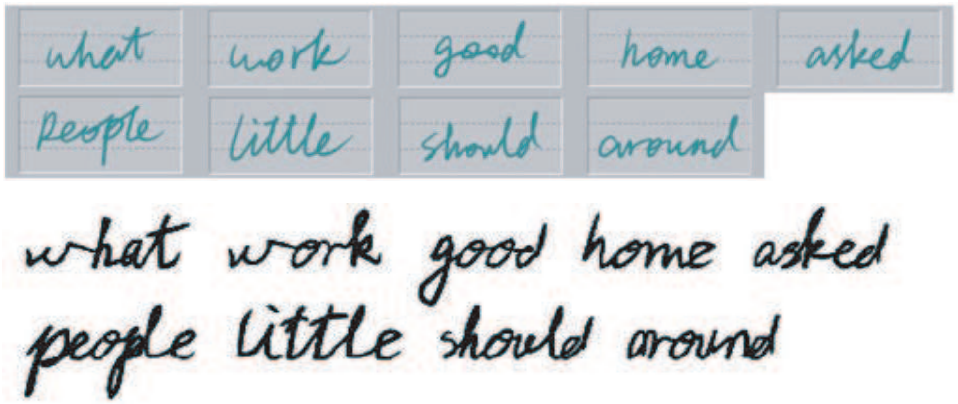


Figure 2.10: *Real (top) and its corresponding synthetic handwriting (bottom) generated using the concatenating approach described in [Lin and Wang, 2007]. Figure extracted from [Lin and Wang, 2007].*

and Ortega-Garcia, 2008].

The great majority of existing approaches for synthetic signature generation are based on this type of strategy [Djioua *et al.*, 2006; Munich and Perona, 2003; Oliveira *et al.*, 1997; Rabasse *et al.*, 2007; Richiardi, 2008]. This approach has also been applied to handwriting [Mori *et al.*, 2000; Mouchere *et al.*, 2007; Wang *et al.*, 2002], and face synthesis [Poh *et al.*, 2003; Sumi *et al.*, 2006; Wang and Zhang, 2004; Wilson *et al.*, 2002].

- **Combination of different real samples**. This is the approach followed by most speech [Black and Campbell, 1995; Toda *et al.*, 2002] and handwriting synthesizers [Ballard *et al.*, 2007; Guyon, 1996; Lin and Wang, 2007; Varga *et al.*, 2005]. This type of algorithms start from a pool of *real* units, n-phones (isolated or combination of sounds) or n-grams (isolated or combination of letters), and using some type of concatenation procedure combine them to form the synthetic samples (in Fig 2.10 we show some examples of synthetically generated handwriting following the approach described in [Lin and Wang, 2007]). Again, these techniques present the drawback of needing *real* samples to generate the synthetic trait and therefore their utility for performance evaluation and vulnerability assessment in biometrics is also very limited. As in the previous case, this perspective for the generation of synthetic data is useful to produce multiple biometric samples of a given real user, but not to generate synthetic individuals.

- **Synthetic-individuals**. In this case, some kind of *a priori* knowledge about a certain biometric trait (e.g., minutiae distribution, iris structure, signature length, etc.) is used to create a model that characterizes that biometric trait for a population of subjects. New *synthetic* individuals can then be generated sampling the constructed model. In a subsequent stage of the algorithm, multiple samples of the synthetic users can be generated by any of the procedures for creating duplicated samples.

  Regarding performance evaluation and vulnerability assessment in biometrics this ap-

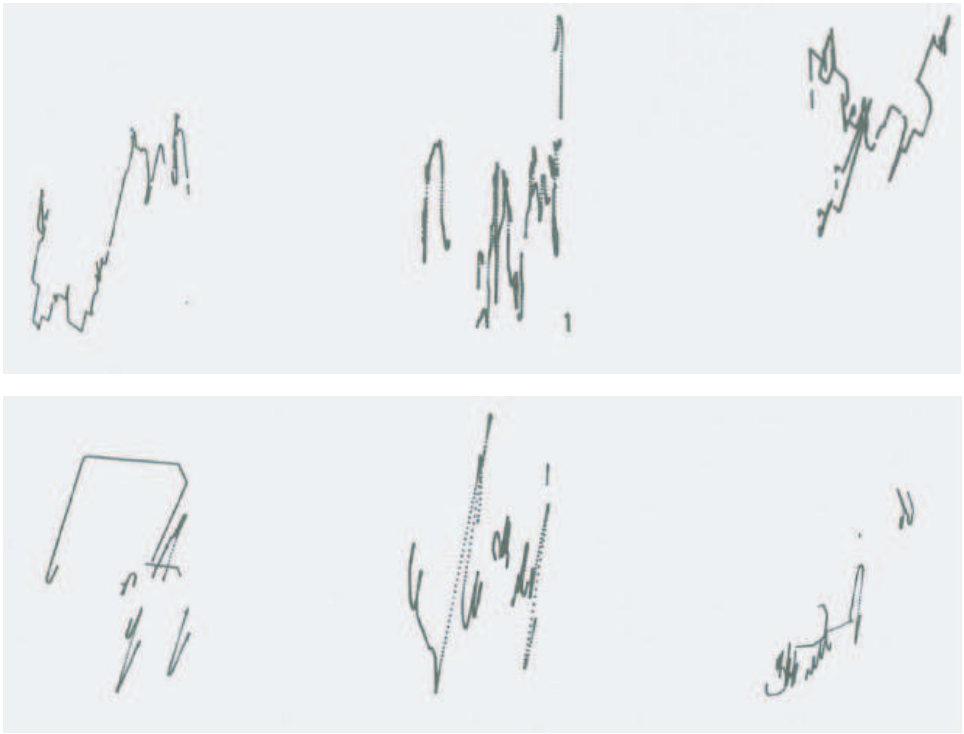


Figure 2.11: *Six examples of different synthetic signatures (synthetic individuals) generated with the model-based method described in [Popel, 2007]. Figure extracted from [Popel, 2007].*

proach has the clear advantage over the two previously presented, of not needing any real biometric samples to generate completely synthetic databases. This way, these algorithms constitute a very effective tool to overcome the usual shortage of biometric data without undertaking highly resource-consuming acquisition campaigns.

Different model-based algorithms have been presented in the literature to generate synthetic individuals for biometric traits such as iris [Cui *et al.*, 2004; Shah and Ross, 2006; Zuo *et al.*, 2007], fingerprint [Cappelli, 2003], or speech [Klatt, 1980; Pinto *et al.*, 1989]. Bezine *et al.* [2007] on one hand and Djioua and Plamondon [2009] on the other hand have proposed two different models to characterize the handwriting process but have not carried out any conclusive experiments regarding the suitability of the models for synthesis of totally artificial subjects. To the best of our knowledge, Popel is the only author who has described this type of approach for synthetic signature generation using a complicated model based on information extracted from the time domain [Popel, 2007]. Six different synthetic signatures generated following this approach are shown in Fig. 2.11.

In Chapter 4 of this Dissertation a novel model-based approach for the generation of synthetic signatures (synthetic individuals) is proposed and evaluated.

2.4. Chapter Summary and Conclusions

In this chapter we have summarized the main works related to this PhD Thesis. We have started by describing the general threats to which biometric systems are exposed, classifying them into different categories, and presenting the most important works in each of those categories. Then we have focused on the different countermeasures that have been proposed in the literature to minimize the effects of the attacks, paying special attention to liveness detection methods. Finally, a general view in the generation of synthetic biometric traits has been given, specifically in on-line signature which is the problem that has been addressed in the Thesis.

Being this chapter a summary of the state-of-the-art, no new material has been presented. Although the exposition of some parts of the chapter is based on some of the cited publications, most of the structure and presentation has followed a personal perspective.

Chapter 3

Performance and Security Evaluation of Biometric Systems

This chapter summarizes the common practices in performance testing of biometric systems and presents the security evaluation methodology followed in the Thesis for the vulnerability assessment of biometric systems. The biometric databases used for both types of evaluations (performance and security) are also described, with special attention to the BiosecurID multimodal database due to its great importance in the development of the Thesis.

The chapter is organized as follows. First we summarize the guidelines for performance evaluation used in this Dissertation (Sect. 3.1). Then we provide a description of the proposed protocol for security evaluation followed in the different vulnerability studies carried out in the Thesis (Sect. 3.2). Finally we give an overview of the main existing multimodal biometric databases (Sect. 3.3) and we thoroughly describe the most important one used in this Thesis (Sect. 3.4).

This chapter is based on the publications: Fierrez *et al.* [2009].

3.1. Performance Evaluation of Biometric Systems

The practice in first research works on biometrics starting over three decades ago was to report experimental results using biometric data specifically acquired for the experiment at hand [Atal, 1976; Kanade, 1973; Nagel and Rosenfeld, 1977]. This approach made very difficult the fair comparison of different recognition strategies, as the biometric data was not made publicly available.

With the popularity of biometric systems and the creation of new research groups working in the same topics, the need for common performance benchmarks was recognized early in the past decade [Jain *et al.*, 2004b; Phillips *et al.*, 2000b]. In this environment, the first series of international competitions for person authentication based on different biometric traits were organized. In these competitions, biometric data along with specific experimental protocols were

established and made publicly available. Some examples include the following campaigns: NIST Facial Recognition Technology Evaluations (FERET), starting in 1994 [Phillips *et al.*, 2005, 2000b]; NIST Speaker Recognition Evaluations (SRE), held yearly since 1996 [Przybocki and Martin, 2004]; NIST Iris Challenge Evaluations (ICE), first organized in 2005 [Phillips, 2006]; Fingerprint Verification Competitions (FVC), held biannually since 2000 [Cappelli *et al.*, 2006b]; the Signature Verification Competition (SVC), organized in 2004 [Yeung *et al.*, 2004]; and the BioSecure Multimodal Evaluation Campaign held in 2007 [Mayoue *et al.*, 2009]. Comparative evaluations of commercial biometric technologies can also be found nowadays by standards institutions like NIST [Grother *et al.*, 2003; Wilson *et al.*, 2004a] and CESG [Mansfield *et al.*, 2001], or consulting firms like the International Biometric Group [2009]. All these initiatives and interest have led to the achievement by at least one laboratory exclusively focused in the performance evaluation of biometric systems (the Biometric Services International [BSI, 2009], a non-profit company working under the National Biometric Security Project [NBSP, 2009]) of the ISO/IEC 17025:2005 accreditation for testing [ISO/IEC 17025, 2005].

In this environment, and as a result of the experience gained in biometric performance evaluation, the UK Biometrics Working Group has generated a set of best practices for testing and reporting performance results of biometrics systems [Mansfield and Wayman, 2002], to which we adhere in this PhD Thesis.

Performance evaluation of biometric recognition systems can be carried out at three different levels [Phillips *et al.*, 2000a]: technology, scenario, and operational.

The goal of a technology evaluation is to compare competing algorithms thus identifying the most promising recognition approaches and tracking the state-of-the-art. Testing of all algorithms is carried out on a standardized database. Performance with this database will depend upon both the environment and the population from which the data are collected. Because the database is fixed, the results of technology tests are repeatable. Some important aspects of a given database are: 1) Number of users, 2) number of recording sessions, and 3) number of different samples per session. Most standardized benchmarks in biometrics are technology evaluations conducted by independent groups or standards institutions [Maio *et al.*, 2004; Petrovska-Delacretaz *et al.*, 2009; Phillips *et al.*, 2000b; Przybocki and Martin, 2004; Yeung *et al.*, 2004].

The goal of scenario evaluations is to measure overall system performance for a prototype scenario that models an application domain. Scenario evaluations are conducted under conditions that model real-world applications [Bone and Blackburn, 2002; Mansfield *et al.*, 2001]. Because each system has its own data acquisition sensor, each system is tested with slightly different data, and thus scenario tests are not repeatable. An operational evaluation is similar to a scenario evaluation. While a scenario test evaluates a class of applications, an operational test measures performance of a specific algorithm for a specific application [Bone and Crumbacker, 2001].

In this Thesis we carry out the performance evaluation experiments as technology evaluations of different systems working in the *verification* mode where the user makes a positive claim of

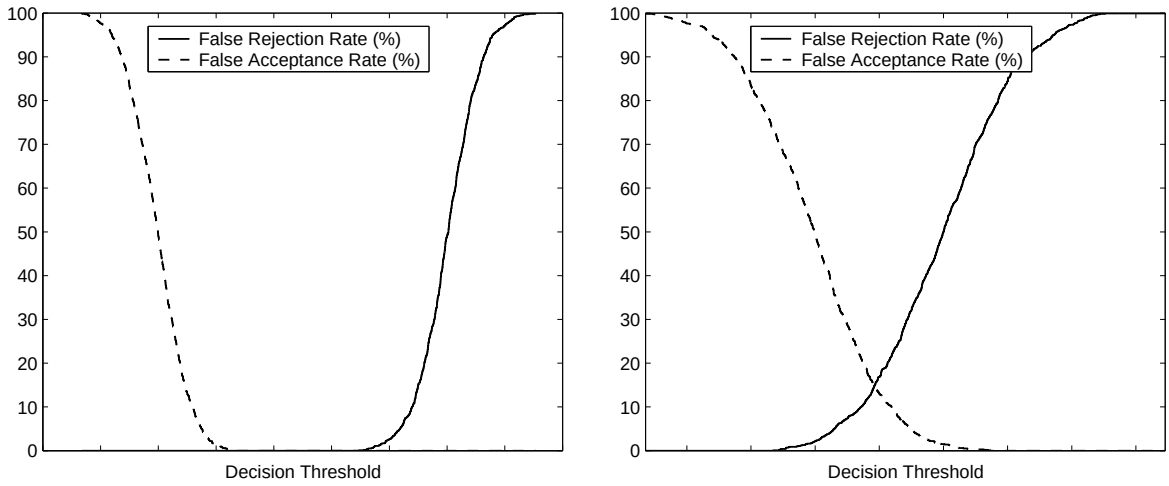


Figure 3.1: *FA and FR curves for an ideal (left) and real (right) authentication systems.*

identity (i.e., I am E. Nigma), requiring a one-to-one comparison of the submitted sample to the enrolled template for the claimed identity. In opposition, as introduced in Chapter 1, in the *identification* mode the user makes either no claim or an implicit negative claim of identity (i.e., I am not enrolled in the database), and a one-to-many search is required.

3.1.1. Performance Measures of Authentication Systems

The performance of biometric systems is estimated under normal operation conditions where the users try to access the system interacting with it in a straight forward manner. In opposition, security evaluations are carried out under attacking scenarios where an attacker tries to access (break) the system interacting with it using some type of approach or methodology for which the application was not thought. In the normal operation scenario of a verification biometric system two types of access attempts or claims of identity are defined [Mansfield and Wayman, 2002]: *i*) *genuine claim of identity*: a user making a truthful positive claim about identity in the system (the user truthfully claims to be him/herself, leading to a comparison of a sample with a truly matching template), and *ii*) *impostor claim of identity*: a user making a false positive claim about identity in the system (the user falsely claims to be someone else, leading to the comparison of a sample with a non-matching template). Genuine attempts are aslo referred to as *client* attempts, while impostor attempts are also known as *zero-effort* attempts, and constitute the most basic form of attack to a biometric system.

Considering these two different types of access attempts (genuine and impostor) biometric authentication can be considered as a detection task, involving a tradeoff between two types of errors [Ortega-Garcia *et al.*, 2004]: 1) False Rejection (FR), occurring when a user making a genuine claim of identity is rejected by the system, and 2) False Acceptance (FA), taking place when a user making an impostor claim of identity is accepted into the system. Although each type of error can be computed for a given decision threshold, a single performance level is

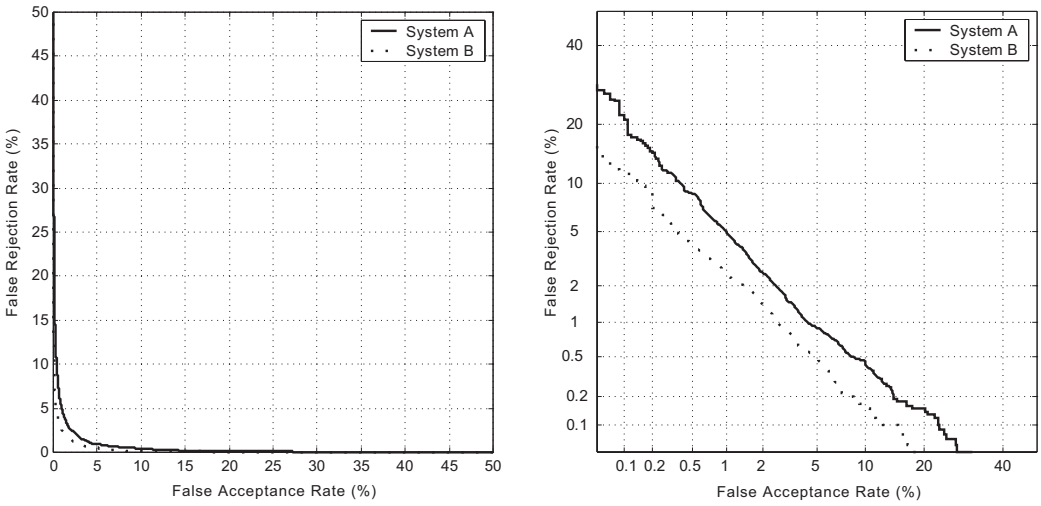


Figure 3.2: *Example of verification performance with ROC (left) and DET curves (right).*

inadequate to represent the full capabilities of the system. Therefore the performance capabilities of authentication systems have been traditionally shown in the form of FA and FR Rates versus the decision threshold, as depicted in Fig. 3.1 for an ideal system (left), and a real system (right). In order to estimate the FRR and FAR of a given system, a set of genuine and impostor matching scores (resulting respectively from genuine and impostor access attempts) have to be generated using the available biometric data. Several methods have been described in the literature in order to maximize the use of the information embedded in the training samples during a test including resubstitution, holdout, cross-validation, and variants of the jackknife sampling using the leave-one-out principle [Jain *et al.*, 2000; Theodoridis and Koutroumbas, 2006].

Another commonly used graphical representation of the capabilities of an authentication system, specially useful when comparing multiple systems, is the ROC (Receiver -or also Relative- Operating Characteristic) plot, in which FA Rate (FAR) versus FR Rate (FRR) is depicted for variable decision threshold. A variant of the ROC curve, the so-called DET (Detection Error Tradeoff) plot, is used in this Thesis [Martin *et al.*, 1997]. In this case, the use of a non-linear scale makes the comparison of competing systems easier. A comparison between ROC and DET curves for two hypothetical competing authentication systems A and B is given in Fig. 3.2.

A specific point is attained when FAR and FRR coincide, the so-called EER (Equal Error Rate). The global EER of a system can be easily detected by the intersection between the DET curve of the system and the diagonal line y = x. Nevertheless, and because of the discrete nature of FAR and FRR plots, EER calculation may be ambiguous according to the above-mentioned definition, so an operational procedure for computing the EER must be followed. In the present contribution, the procedure for computing the EER described by Maio *et al.* [2002b] has been applied.

3.2. Security Evaluation of Biometric Systems

The performance evaluation of biometric systems introduced in the previous section, is only one form of biometric testing that can be considered when performing an overall evaluation of a biometric application. Other tests include reliability, vulnerability and security, user acceptance or cost/benefit [Wayman *et al.*, 2005].

In particular, the need for independent, repeatable and consistent security assessment of biometric systems is evidenced by the generation of different security evaluation standards [BEM, 2002; CC, 2006; ISO/IEC 19792, 2009], the organization of competitions searching for new countermeasures against attacks [LivDet, 2009], and the publication of numerous research works [Galbally *et al.*, 2007; Ratha *et al.*, 2001a; Uludag and Jain, 2004]. All these efforts stress the necessity of addressing the vulnerability evaluation of biometric systems from a rigorous and systematic perspective.

Due to the intrinsic statistical nature of biometric recognition, the evaluation of the security threats that affect them should be carried out in a similar fashion to that used in the performance assessment of the systems (see Sect. 3.1). Determining if a certain attack (e.g., direct attack using a gummy finger generated from a latent fingerprint of the user) is or not feasible is not enough for a vulnerability evaluation. In order to estimate the robustness of a given biometric system to the attack, a large and representative dataset (e.g., of real and gummy fingers) in terms of users and samples should be acquired to find out, from a statistical point of view and not just on a yes or no basis, *how* vulnerable to the attack is the system being tested.

In this scenario, we propose a systematic security evaluation protocol for biometric systems that can be applied regardless of the attack, system, or biometric trait being considered, and which has been used in the different vulnerability studies carried out within the Thesis (Chapters 5, 6 and 7). The protocol includes a set of guidelines for the security analysis and reporting in a useful and meaningful manner for other researchers. In particular, the steps followed in this Thesis for the security evaluation of biometric systems are:

1. Description of the attack for which we want to determine the vulnerability of the biometric system.

2. Description of the biometric system that will be evaluated.

3. Description of the information about the system under evaluation required to be known by the attacker.

4. Description of the database that will be used in the evaluation.

5. Description of the experimental protocol that will be followed in the evaluation.

6. Execution of a performance evaluation (see Sect. 3.1) of the system being tested. The performance evaluation will permit to determine how good is the system and, more important, the operating points where it will be attacked (as the success chances of an attack

are highly dependent on the FA and FR rates of the system). Furthermore, defining the operating points will enable to compare, in a more fair manner, the vulnerabilities of different systems to the same attack (i.e., we can determine for a given FAR or FRR which of them is less/more robust to the attacking approach).

7. Execution of the vulnerability evaluation in the defined operating points, reporting the results in terms of (at least) the Success Rate and Efficiency (defined next) of the attack.

In a security evaluation two main parameters should be computed to determine the risk represented by an attack (and therefore the vulnerability of the system to it):

- **Success Rate (SR)**. It is the expected probability that the attack breaks a given account. It is computed as the ratio between the accounts broken by the attack A_b, and the total accounts attacked A_T, that is $SR = A_b/A_T$. This parameter gives an estimation of how dangerous it is a particular attack for a given biometric system: the higher the SR the bigger the threat.

- **Efficiency**. It indicates the *average* number of *matchings* needed by the attack to try to break an account. It is defined as $E_{ff} = \left(\sum_{i=1}^{A_T} n_i\right)/A_T$, where n_i is the number of comparisons computed to try to break each of the attacked accounts. Note that it is computed in terms of the number of matchings or comparisons performed, and not in terms of the number of iterations carried out by the attack (should it be an iterative algorithm), as in each iteration more than one matching might be computed. This parameter gives an estimation of how easy it is for the attack to break into the system in terms of speed: the lower the E_{ff} the faster the attack.

With the term *account* we refer to the enrolled biometric template/model of a legitimate user which is used as reference to be matched against the test samples.

The SR and Efficiency of an attack consisting on the succession of zero-effort attempts (i.e., brute-force attack) are already computed in the performance evaluation (as in this particular case, $SR_{bf} = FAR$ and $E_{ff-bf} = 1/FAR$), can be given as baseline result with which to compare the SR and efficiency of the attack under consideration. This is a useful comparison as all biometric systems are vulnerable to a brute-force attack (there is always some probability that an impostor attempt is accepted).

Similarly, when a countermeasure is introduced in a biometric system to reduce the risk of a particular attack (previously analyzed), it should be statistically evaluated considering two main parameters:

- Impact of the countermeasure in the system performance. The inclusion of a particular countermeasure might change the FAR and FRR of a system, and these changes should be evaluated and reported (other performance indicators such as speed or computational efficiency might also change, but are not considered here).

- Performance of the countermeasure, i.e. impact of the countermeasure in the SR and Efficiency of the attack.

Following the described perspective for statistical biometric security assessment, in the Thesis we have carried out vulnerability evaluations of different biometric recognition systems to three main types of attacks (already introduced in Chapter 2):

- **Direct Attacks**. These threats are also known as *spoofing* and refer to the use of synthetic biometric traits or *artefacts* (e.g., gummy fingers, high quality face or iris images) to try to access the system.
- **Hill-Climbing Attacks**. These are iterative approaches which take advantage of the matching scores returned by the biometric system to modify a number of synthetically generated templates until access to the system is granted.
- **Brute-Force Attacks**. These attacks are performed as a succession of zero-effort attempts (impostor attempts in the normal operation scenario as defined in Sect 3.1). Therefore, for this particular case, $SR = FAR$ and $E_{ff} = 1/FAR$.

Under these attacking scenarios genuine and impostor attempts might differ from those defined in the normal operation scenario considered for performance evaluation (see Sect. 3.1). As a result, the FAR and FRR of a biometric system can change depending on the experimental context. To avoid confusions, in this Thesis we will use the terms FAR/FRR to refer to both error rates in the normal operation scenario, and FMR/FNMR (False Match Rate, and False Non Match Rate) to designate matching errors in other experimental settings (where genuine and impostor attempts have changed with respect to the normal operation scenario).

3.3. Biometric Databases

One key element for performance and security evaluation of biometric systems is the availability of biometric databases. In particular, most of the last important efforts in biometric data collection have been directed to the acquisition of large multimodal (i.e., comprising different biometric traits of the same users) datasets [Fierrez *et al.*, 2009, 2007b; Ortega-Garcia *et al.*, 2009]. Multimodal databases have the clear advantage over unimodal corpora of permiting to carry out research studies using individual or different combined traits (i.e., multibiometrics) [Fierrez-Aguilar *et al.*, 2005c; Ross *et al.*, 2006]. However, the acquisition of multimodal biometric features corresponding to a large population of individuals, together with the desirable presence of biometric variability of each trait (i.e., multi-session, multiple acquisition sensors, different signal quality, etc.), makes database collection a time-consuming and complicated process, in which a high degree of cooperation of the donators is needed. Additionally, the legal issues regarding data protection are controversial [Flynn, 2007; Wayman *et al.*, 2005]. For these

reasons, nowadays, the number of existing public multimodal biometric databases is quite limited.

Due to the difficulties in database collection, in recent years different research efforts have been conducted within the biometric scientific community to generate databases formed by totally synthetic traits [Cappelli, 2003; Galbally *et al.*, 2009f]. These synthetic databases present the advantage of being automatically generated so there are no size restrictions (in terms of subjects and samples per subject), and are not affected by legal aspects (as do not comprise the data of any real user). However, although synthetic traits contain similar characteristics and information to that of real samples, the performance of automatic recognition systems on synthetic databases differs to some extent to that obtained on real data [Cappelli *et al.*, 2006b; Galbally *et al.*, 2009f]. For these reasons, although the final evaluation of a given biometric system has to be performed under realistic conditions (including a database of real traits), synthetically generated databases constitute a very powerful tool for performance and security testing.

3.3.1. Multimodal Biometric Databases

The multimodal databases currently available have resulted from collaborative efforts in recent research projects. Examples of these joint efforts include European projects like M2VTS [Messer *et al.*, 1999], Biosec [Fierrez *et al.*, 2007b], or the Biosecure Network of Excellence [Ortega-Garcia *et al.*, 2009], and national projects like the French BIOMET [Garcia-Salicetti *et al.*, 2003] or the Spanish BiosecurID [Fierrez *et al.*, 2009].

Multimodal Biometric Databases can be broadly classified into two groups [Faundez-Zanuy *et al.*, 2006]: 1) databases of multimodal biometric signals, and 2) databases of multimodal scores. In the first class the collected data are biometric signals, such as fingerprint images or voice utterances. These signals may be used with a variety of different experimental protocols, both for individual system development and for multimodal experiments at any fusion level (i.e., sensor, feature, or score level), or in the security evaluation of automatic recognition systems. The second class of multimodal databases are intended exclusively for multimodal research based on score fusion. These corpora consist of matching scores from the individual traits considered.

In this section we provide an overview of existing multimodal databases of biometric signals as permit a much wider range of research studies than those comprising the raw scores. First, we present those general datasets which have been used in the experimental part of the Thesis (other specific databases used in the Thesis and acquired for a particular evaluation are described in their respective experimental frameworks). Then, other significant examples of multimodal databases are given.

Three relevant multimodal databases have been used in the experimental part of this Thesis:

- **BiosecurID** [Fierrez *et al.*, 2009]. It was acquired within the project BiosecurID [BiosecurID, 2003], which ran parallel to the execution of the Thesis and originated part of the work described in this Dissertation. Due to the importance of this database in the

development of the Thesis, it will be described in detail in Sect. 3.4.

This database is used in the Thesis in Chapter 4 for the validation of a novel synthetic signature generation method, and for the security evaluation of on-line signature recognition systems in Chapter 6.

- **MCYT**[1] [Ortega-Garcia *et al.*, 2003]. The acquisition was funded by the Spanish Government through its programme to help research and conducted by a consortium of four Spanish academic institutions, namely: ATVS Research group (at Universidad Autonoma de Madrid - UAM), Universidad de Valladolid (UVA), Universidad del Pais Vasco (EHU), and Escola Politecnica de Mataro (EUPMT). The database consists of online signatures and fingerprints from 330 individuals.

  - *MCYT_Fingerprint dataset*. For each individual, 12 samples of each finger are acquired using two different sensors (optical and capacitive, both with a resolution of 500 dpi). Therefore, $330 \times 12 \times 10 \times 2 = 79,200$ fingerprint samples are included in the database. Each of the 12 samples of a given finger were acquired in a not consecutive manner in order to produce the necessary intravariability among images of the same fingerprint. Additionally, the images were collected with three different levels of control: *i*) high, where small rotation or displacement of the finger core from the center of the sensor was permitted (three samples per finger), *ii*) medium (three samples), and *iii*) low (six samples).
  - *MCYT_Signature dataset*. For each individual, 25 client signatures and 25 highly skilled forgeries (with natural dynamics) are obtained for each individual. Both on-line information (pen trajectory, pen pressure and pen azimuth/altitude, sampled at 100 Hz) and off-line information (image of the written signature) are considered in the database. Therefore, $330 \times (25+25) = 16,500$ signature samples are considered in the MCYT on-line corpus. In order to generate intravariability among samples, the client signatures are produced in groups of five, interleaving with five skilled forgeries (of a previous user).

  This database is used in the Thesis both in Chapters 5 and 6 for the security evaluation of fingerprint and signature recognition systems. A detailed description can be found in [Fierrez, 2006].

- **XM2VTS**[2] Messer *et al.* [1999]. The XM2VTS database was acquired in the context of the M2VTS project (Multi Modal Verification for Teleservices and Security applications), a part of the EU ACTS programme, which deals with access control by the use of multimodal identification based on face and voice. The database contains microphone speech and face

[1] The MCYT database is publicly available at http://atvs.ii.uam.es/. Up to date, it has been distributed to more than 100 institutions.

[2] A variety of subsets of the database are available for purchase from the University of Surrey. Up to date, the XM2VTS database has been distributed to more than 100 institutions.

image from 295 people. Every subject was recorded in 4 sessions over a period of 4 months. At each session, two head rotation shots and six speech shots (subjects reading three sentences twice) were recorded. The XM2VTS evaluation protocol (the Lausanne Protocols 1 and 2, LP1 and LP2) specifies training, evaluation, and test sets, so algorithmic recognition performance can be assessed on the basis of comparable evaluation framework.

This database is used in the Thesis in Chapter 7 for the security evaluation of face recognition systems, and is fully described in [Messer *et al.*, 1999].

Other significant examples of multimodal biometric databases already completed and available, or in legal process to be released are:

- **BIOSECURE** [Ortega-Garcia *et al.*, 2009]. One of the Biosecure NoE [Biosecure, 2007] objectives was the acquisition of a multimodal database which extends the efforts conducted in MyIDEA, Biosec, and BiosecurID. The database considers three acquisition scenarios, namely:

  - Unsupervised internet acquisition (internet dataset), including voice, and face (still images and talking faces).
  - Supervised office-like scenario (desktop dataset), including voice, fingerprints (two sensors), face (still images and talking faces), iris, signature (genuine and skilled forgeries) and hand.
  - Acquisition in a mobile device (mobile dataset), including signature (genuine and skilled forgeries), fingerprints (thermal 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.

- **BIOSEC** [Fierrez *et al.*, 2007b]. It was acquired under FP6 EU BioSec Integrated Project [BioSec, 2004], and comprises 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 [Fierrez *et al.*, 2007b] comprised 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).

- **BIOMET** [Garcia-Salicetti *et al.*, 2003]. This multimodal database includes five different modalities: audio, face images (2D and 3D), hand images, fingerprint (captured with an optical and a capacitive sensor), and signature. The database was acquired in three temporally separated sessions (8 months between the first and the last one) and comprises 91 subjects who completed the whole process.

	#Users	#Sessions	#Traits	2Fa	3Fa	Fp	Ha	Hw	Ir	Ks	Sg	Sp
BiosecurID	400	4	8	×		×	×	×	×	×	×	×
MCYT	330	1	2			×					×	
XM2VTS	295	4	2	×								×
Biosecure	Int. 1000 (ap.)	2	2	×								×
	PC 700 (ap.)	2	6	×		×	×		×		×	×
	Mob. 700 (ap.)	2	4	×		×					×	×
BioSec	250	4	4	×		×			×			×
MyIDEA	104 (ap.)	3	6	×		×	×	×			×	×
BIOMET	91	3	6	×	×	×	×				×	×
MBioID	120 (ap.)	2	5	×		×			×		×	×
BANCA	208	12	2	×								×
M3	32	3	3	×		×						×
FRGC	741	Variable	2	×	×							
SmartKom	96	172	4			×	×				×	×
BT-DAVID	100	5	2	×								×

Table 3.1: *Summary of the most relevant features of existing multimodal biometric databases (the ones used in this Thesis appear highlighted in light grey). The nomenclature followed is: # stands for* number of*, 2Fa for Face 2D, 3Fa for face 3D, Fp for Fingerprint, Ha for Hand, Hw for Handwriting, Ir for Iris, Ks for Keystroking, Sg for signature, and Sp for Speech.*

- **MyIDEA** [Dumas *et al.*, 2005]. Includes face, audio, fingerprints, signature, handwriting and hand geometry. Two 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 [Bailly-Bailliere *et al.*, 2003].

Some other multimodal databases are the **MBioID** [Dessimoz *et al.*, 2007] database acquired to study the use of biometric in Identity Documents (2D and 3D face, fingerprint, iris, signature and speech), the **BANCA** [Bailly-Bailliere *et al.*, 2003] database comprising face and voice recordings of 208 subjects, and the new multibiometric, multidevice and multilingual **M3** [Meng *et al.*, 2006] database, which includes face, speech (in Cantonese, Putonghua and English) and fingerprint traits captured on three different devices (desktop PC, pocket PC and 3G mobile phone) of 32 users. Other examples are **FRGC** [Phillips *et al.*, 2005], **SmartKom** [Steininger *et al.*, 2002] or **BT-DAVID** [Chibelushi *et al.*, 1999].

In Table 3.1 a summary of the most relevant features of existing multimodal biometric databases is presented (the ones used in this Thesis are highlighted in light grey). In order to present all the information in a compact manner, both palmprint and palm geometry are considered as Hand trait, and on-line and off-line signature as Signature trait. In case of a different number of participants in each acquisition session (as is the case of the BIOMET database) the number of donors common to all the sessions is presented.

3.4. The BiosecurID Multimodal Biometric Database

The BiosecurID Biometric Multimodal Database was acquired within the BiosecurID project [BiosecurID, 2003], and conducted by a consortium of 6 Spanish Universities, Universidad Autonoma de Madrid (UAM), Universidad Politecnica de Madrid (UPM), Universidad Politecnica de Cataluña (UPC, Campus of Terrasa and Campus of Mataro), Universidad de Zaragoza (UniZar), Universidad de Valladolid (UVA), and Universidad del Pais Vasco (UPV). The main objective of the project was the acquisition of a realistic multimodal and multisession database, statistically representative of the potential users of future biometric applications, and large enough in order to infer valid results from its usage.

Although, as has been presented in the previous section, several multimodal biometric databases are already available for research purposes, none of them can match the BiosecurID database in terms of number of users, number of biometric traits and number of temporal separated acquisition sessions. The data collected in the project are especially useful for the development and testing of automatic recognition systems due to some design characteristics such as: realistic acquisition scenario, balanced gender and population distributions, availability of information about particular demographic groups (age, gender, handedness, visual aid), acquisition of replay attacks (speech and keystroking) and skilled forgeries (signatures) in order to simulate attacking scenarios, and compatibility with other existing databases. Furthermore, it was designed to comply with three main characteristics which make it unique, namely:

1. **Number of subjects**: a total of 400 users were acquired. The number of subjects acquired per site, and the distribution in the database is: UAM 65 (IDs 1–65), UPM 65 (IDs 66–130), UPC Mataro 40 (IDs 131–170), UPC Terrasa 35 (IDs 171–205), UVA 77 (IDs 206–282), UPV 52 (IDs 283–334), UniZar 66 (IDs 335–400).

2. **Number of unimodal biometric traits**: speech, iris, face (photographs and talking faces videos), signature and handwriting (on-line and off-line), fingerprints, hand (palmprint and contour-geometry), and keystroking.

3. **Number of sessions**: 4 sessions distributed in a 4 month time span. Thus, three different levels of temporal variability are taken into account: *i*) within the same session (the samples of a same biometric trait are not acquired consecutively), *ii*) within weeks (between two consecutive sessions), and *iii*) within months (between non-consecutive sessions). This is specially relevant in traits such as face, speech, handwriting or signature which present a significant variation through time.

The BiosecurID database is also thought to represent in a realistic way the population distribution where biometric systems will be deployed. Thus, all sites were asked to acquire 30% of the subjects between 18 and 25 years of age, 20% between 25 and 35, 20% between 35 and 45, and the remaining 30% of the users above 45 years of age. Moreover, the gender distribution was forced to be balanced and only a 10% difference was permitted between male and female sets.

	BiosecurID DB. 400 subjects
Gender Distribution	54% (Male) / 46% (Female)
Age Distribution	30% (18–25) / 20% (25–35) / 20% (35–45) / 30% (>45)
Handedness	80% (Righthanded) / 20% (Lefthanded)
Manual Workers	7% (Yes) / 93% (No)
Vision Aids	66% (None) / 27% (Glasses) / 7% (Lenses)

Table 3.2: *Statistics of the BiosecurID database.*

All relevant non-biometric data of each subject is stored in an independent file (available with the biometric samples) so that experiments regarding specific demographic groups can be easily carried out. The available information in these files includes: age, gender, handedness, manual worker (yes/no), and vision aids (glasses, contact lenses, none). The "manual worker" group includes all users having eroded fingerprints, as identified by the contributors themselves when asked about their daily tasks (e.g., drivers, peasants, etc). In Table 3.2 the most relevant statistics of the BiosecurID database are shown.

3.4.1. Acquisition Environment

Each of the 6 acquisition sites prepared an acquisition kiosk following some very general indications about the environmental conditions, regarding illumination (neutral lighting with no preponderant focuses), noise (indoor conditions with no excessive background noise), and pose of the contributor (sitting in a non-revolving chair). This relaxed environmental conditions allow a desirable variability between the samples acquired in the different sites (e.g., background in facial images) which simulates the changing working conditions of a real-world biometric application. In Fig. 3.3 we show the acquisition kiosk prepared in one of the sites, together with some of the devices used in the acquisition.

During the acquisition procedure a human operator gave the necessary instructions to the contributors so that the acquisition protocol was followed. In spite of this guidance, and of the usage of a specifically designed acquisition software (see Sect. 3.4.3), some human and software errors occurred. In order to ensure that the BiosecurID database complies with the acquisition protocol, all biometric samples were manually verified by a human expert who either corrected or discarded non-valid data. The guidelines followed in the validation process are further described in Sect. 3.4.5.

3.4.2. Acquisition Devices

In Table 3.3 we show a list with all the devices used in the database acquisition and its most relevant features. All of them were connected to a standard PC in which an acquisition software specifically designed following the database protocol was installed. This programme centralized the functioning and launching of all the devices, as well as the naming and storage

Figure 3.3: *Example setup used in the acquisition of the BiosecurID database.*

of the captured samples and management of the database, thus minimizing eventual acquisition errors.

3.4.3. Acquisition Software

A specific software was developed for the acquisition of the database: the BiosecurID DAST (Data Acquisition Software Tool). The main objective of the application was to provide a common working interface for all the participant sites, in order to make the acquisition process faster, and more reliable and homogeneous. The software also centralized the storage, management and maintenance of the database.

The functionalities of BiosecurID DAST are:

- The software allows a human expert to repeat the acquisition of any invalid sample until it is validated.
- The software allows the inclusion of new users, or new sessions, at any point of the acquisition process.
- The donor's identities are stored within the database but in an independent file, which can be encrypted.
- The software generates periodic backups. In order to minimize acquisition errors, the

Modality	Model	Main Features
Speech	Plantronics DSP 400	Noise cancelling. 10Hz - 10KHz.
Fingerprints	Biometrika FX2000	Optical. 569 dpi. Capture area: 13.2 × 24.9 mm. Image size: 400 × 560 pixels.
Fingerprints	Yubee (Atmel sensor)	Thermal Sweeping. 500 dpi. Capture area: 13.9 × 0.5 mm. Image size: 280 × 8 pixels.
Iris	LG Iris Access 3000	CCD. Infrared illumin. Image size: 640 × 480 pixels.
Hand	Scanner EPSON Perfection 4990	4800 × 9600 dpi. 48 bits color depth. Capturing area: 216 × 297 mm.
Face	Philips ToUcam Pro II	CCD. Illumin. 1 lux. Image size: 640 × 480 pixels.
Writing/Signature	Wacom Intuos3 A4/Inking pen	5080 dpi. 1024 pressure levels. Accuracy: +/- 0.25 mm.
Keystroking	Labtec Standard Keyboard SE	Standard.

Table 3.3: *Acquisition devices used for the BiosecurID database.*

acquisition software permits the correction of captured samples and the completion of missing samples.

- The software is highly modular, so that new acquisition devices or new protocols can be easily added or removed.

BiosecurID DAST is divided into one general module in charge of the data management, and a group of peripheral acquisition applications handling each of the sensors which are launched and controlled by the management tool.

Management tool. The management tool is in charge of the following tasks: *i*) initialize the database so that it is stored in a treelike structure folders, *ii*) create and handle the users, *iii*) store the captured samples with the established nomenclature in the treelike structure, *iv*) launch and manage the different sessions executing each individual acquisition module, and *v*) work as a viewer/editor of the biometric samples already captured. The management is carried out according to the acquisition protocol which defines the order in which the different acquisition modules have to be executed, the number of sessions to be completed per user and the number of samples to be captured per session. In Fig. 3.4 two screen captures of the management tool

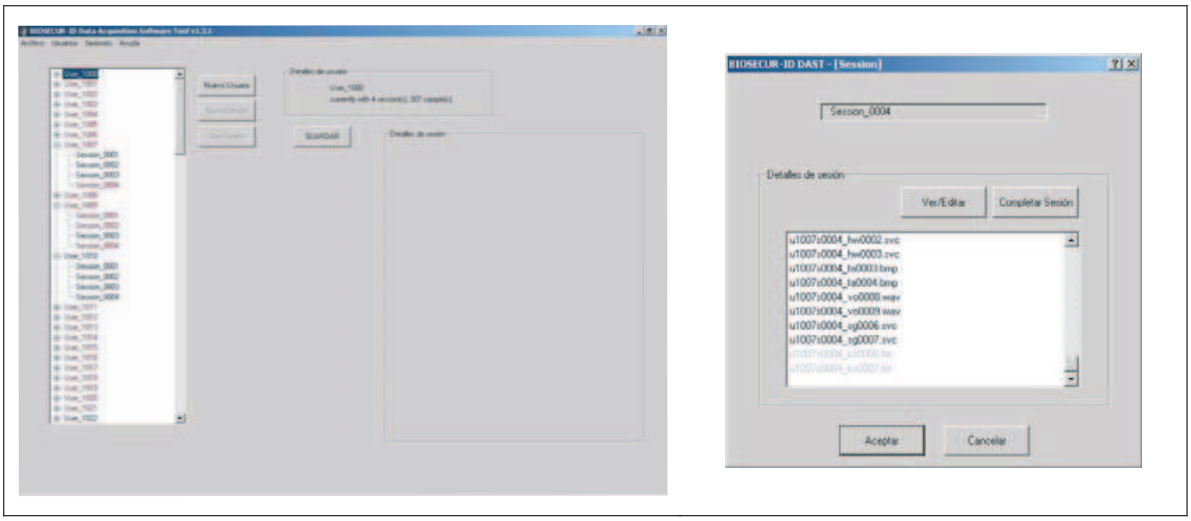


Figure 3.4: *Screen captures of the BiosecurID DAST management tool interface.*

interface are shown.

Acquisition modules. The acquisition modules are independent applications that can be executed in two manners, namely: *i*) automatically run by the BiosecurID DAST management tool following the order established in the acquisition protocol, and *ii*) manually selecting an incomplete or invalid sample (within the BisosecurID DAST management tool) and selecting the edit/view option. The use of independent acquisition modules permits to easily add or remove them from the general application. In Fig. 3.5 screen captures of the different acquisition modules are shown.

3.4.4. Acquisition Protocol

The biometric data along with the personal information captured are personal data and thus have to be protected according to the directives of the country where the responsible institution of the acquisition and management of the data is located (or *controller*)[1], which for BiosecurID is Universidad Autonoma de Madrid in Spain. At the start of the first session a consent form was signed by each subject in which the donors were properly informed about how the personal information will be used, that these data will only be transmitted to other institutions for research purposes and for a limited period of time, and that they have the right to access their data in order to correct, or delete it. The acquisition procedure started only once this consent form was fully understood and signed by the donor. Other requirements of the Spanish data protection authority are[2]: the controller must keep track of the licenses granted for the use of the database, the controller must adhere to ceretain security measures to protect the privacy of the donors, and the database has to be entered in a national register of data files.

In Table 3.4 we summarize the data samples of each biometric trait captured for every user,

[1]Directive 95/96/EC of the European Parliament and the Council of 24 October 1995.
[2]Ley Organica 15/99 (B.O.E. 14/12/1999).

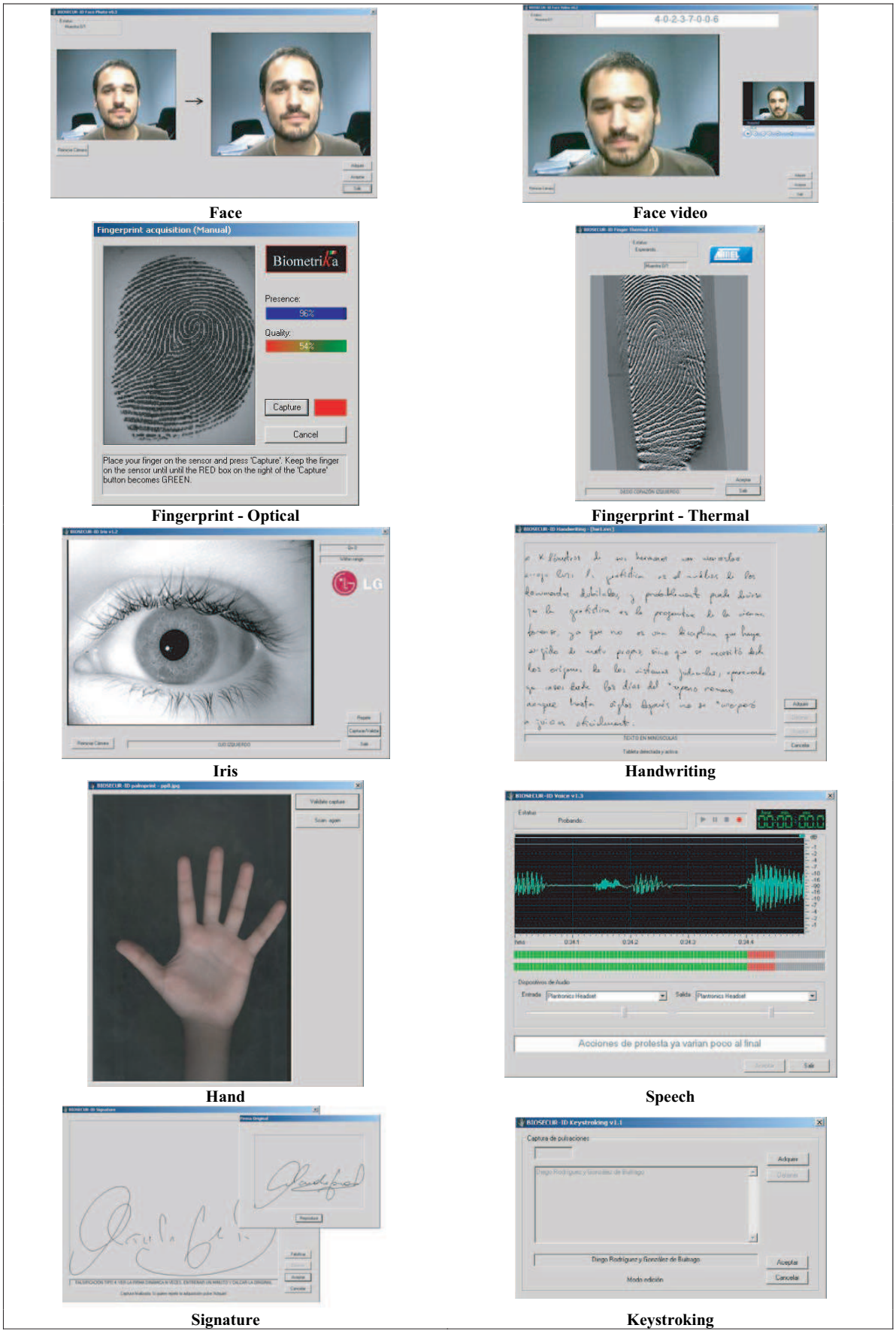


Figure 3.5: *Screen captures of the different BiosecurID DAST acquisition modules.*

namely:

Speech. 10 short sentences in Spanish (the ones used in the Ahumada database [Ortega-Garcia *et al.*, 2000], the same 10 for each donor) distributed along the four sessions (4+2+2+2) recorded at 44KHz stereo with 16 bits (PCM with no compression). In addition to the short sentences, 4 utterances of a user-specific PIN of 8 digits were also recorded, and an utterance of other 3 users' PINs to simulate replay attacks in which an impostor has access to the number of a client. The forged users in each session were $n-3S+2$, $n-3S+1$, and $n-3S$, where n is the ID number inside the database of the current donor, and $S=\{1,2,3,4\}$ is the session number. The 8 digits were always pronounced digit-by-digit in a single continuous and fluent utterance.

Fingerprints. 4 samples (BMP format with no compression) with 2 different sensors (see Table 3.3) of the index and middle fingers of both hands, interleaving fingers between consecutive acquisitions in order to achieve intravariability among images of the same fingerprint.

Iris. 4 samples (BMP with no compression) of each iris, changing eyes between consecutive captures. Glasses are removed for the acquisition, while the use of contact lenses is saved in the non-biometric data file.

Hand. 4 images (JPG format) of each hand, alternating hands between consecutive acquisitions. The scanner used in the acquisition was isolated from external illumination using a box with just a little slot to insert the hand, and covered with a black opaque cloth.

Face. 4 frontal images (BMP not compressed), with no specific background conditions (except that no moving objects are permitted). One video sequence of five seconds saying the 8 digit PIN corresponding to the captured donor. Both the audio (PCM 8 bit) and video (29 frames per second) are captured with the webcam (see Table 3.3). No movement in the background is permitted.

Handwriting. A Spanish text (the same for all subjects) handwritten in lower-case with no corrections or crossing outs permitted. The 10 digits, written separately and sequentially from 1 to 9 and last the 0. 16 Spanish separate words in upper-case. All the writing was captured using an inking pen so that both on-line dynamic signals (following the SVC format [Yeung *et al.*, 2004]) and off-line versions (scanned images) of the data are available. The lower-case text is collected in a different sheet of paper with no guiding lines, just a square highlighting the margins. The upper-case words and the number sequence were stored in a template-like page with boxes for each separate piece of writing.

Signature. 4 genuine signatures per session (2 at the start and 2 at the end) and 1 forgery of each of the precedent three donors (the same three in all the sessions). In order to consider an incremental level of skill in the forgeries, four different scenarios are considered, namely: *i*) the forger only sees the written signature once and tries to imitate it right away (session 1), *ii*) the user sees the written signature and trains for a minute before making the forgery (session 2), *iii*) the donor is able to see the dynamics of the signing process 3 times, trains for a minute and then makes the forgery (session 3), and *iv*) the dynamics of the signature are shown as many times as the donor requests, he is allowed to train for a minute and then signes (session 4). Again both the on-line (SVC format) and off-line versions of the signature are captured using an

Modality	Samples	# Samples	Storage space (Mb)
Speech	10 short sentences	10	6.1
	4×4 PIN genuine	16	15.2
	3×4 PIN imitations	12	11.4
		38	**32.7**
Fingerprints	$4 \times 4 \times 4$ optical	64	10.2
	$4 \times 4 \times 4$ thermal	64	12.3
		128	**22.5**
Iris	$2 \times 4 \times 4$	**32**	**9.4**
Hand	$2 \times 4 \times 4$	**32**	**11.6**
Face	4×4 still faces	16	14.1
	1×4 talking faces videos	4	68.7
		20	**82.8**
Writing	1×4 lower-case text	4	2.4
	1×4 upper-case words	4	1.2
	1×4 number sequence	4	0.1
		12	**3.7**
Signature	4×4 genuine signatures	16	0.6
	3×4 skilled forgeries	12	0.4
		28	**1.0**
Keystroking	4×4 genuine name	16	0.02
	3×4 skilled forgeries	12	0.01
		28	**0.03**

Table 3.4: *Biometric data for each user in the BiosecurID database (400 users in total).*

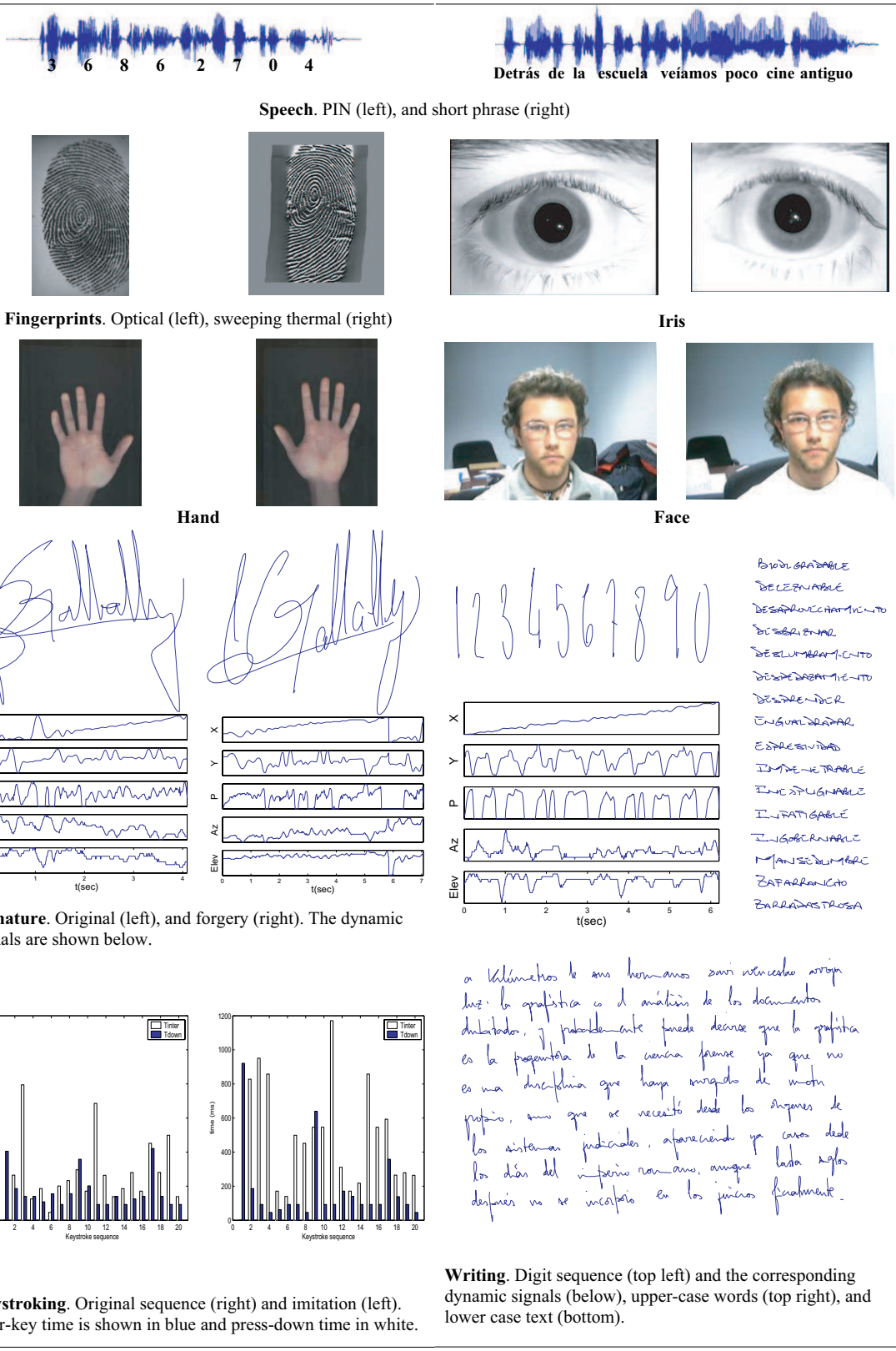


Figure 3.6: *Samples of the different traits present in the BiosecurID database.*

inking pen. This trait is compatible with the publicly available MCYT database [Ortega-Garcia *et al.*, 2003].

Keystroking. 4 case-insensitive repetitions of the donor's name and surname (2 in the middle of the session and two at the end) keystroked in a natural and continuous manner. No mistakes are permitted (i.e., pressing the backspace), if the user gets it wrong, he is asked to start the sequence again. The names of 3 different donors are also captured as forgeries (the same three donors as in the speech PIN imitations), again with no mistakes permitted when keying the name. Samples are stored in plain text files with the total number of keystrokes in the first line, an event (SCAN code + D=press/U=release) and the miliseconds elapsed from the last event in the subsequent lines.

Imitations in the speech, signature and keystroking traits are carried out in a cyclical way, i.e., all the users imitate the previous donors, and the first imitate the last subjects. Examples of typical images in BiosecurID database are depicted in Fig. 3.6 (different traits corresponding to different random subjects). Voice utterances are shown as waveforms, both the dynamic signals and the scanned images are shown for the signatures and the handwritten text, while keystroking samples appear as bar plots of the sequence of keystrokes (press-down and inter-key times).

3.4.5. Validation Process

Prior to the acquisition campaign and the validation process, the concepts *invalid sample* and *low quality sample* were defined as to be certain of which biometric data were acceptable and which had to be rejected.

- **Invalid sample.** Is a sample that does not comply with the specifications given in the acquisition protocol (e.g., index finger labelled as middle, utterance of a wrong PIN, forgery of a wrong signature, etc.)
- **Low quality sample.** Is a sample that will typically perform badly on an automatic recognition system (e.g., very dry fingerprint image, wet fingerprint image, blurred iris image, voice utterance with high background noise, bad illumination in face images, side pose in face images, excessive pressure on a hand sample etc.)

The main objective of the BiosecurID validation process was to reduce as much as possible the number of *invalid samples* within the database. The purpose of the procedure was in no case to reject *low quality samples*. Furthermore, the presence of low quality samples is a design feature of the database and a direct consequence of the non controlled scenario where it was collected. Far from being a disadvantage, poor quality biometric data is an added value to the database as it is one of the key issues that real-world applications have to deal with. In this sense, BiosecurID is a suitable benchmark to evaluate how systems will perform in a realistic scenario. In Fig. 3.7 some of the typical biometric data that can be found in the BiosecurID database, and some selected low quality samples are shown.

Figure 3.7: *Typical biometric data (left), and selected low quality samples (right) that can be found in the BiosecurID database.*

The validation process of the biometric data in the BiosecurID database was carried out in two successive stages:

- **Step 1.** During the acquisition process a human supervisor aided by a specially designed acquisition software (see Sect. 3.4.3), validated one by one the captured samples, reacquiring those which were not compliant with the acquisition protocol.
- **Step 2.** Although the database was thus carefully collected, the possibility of acquisition errors was still opened. In order to ensure that the database fulfils all the acquisition specifications, all collected biometric samples were once again manually verified by a human expert who either completed the missing data, corrected invalid samples, or removed incomplete users.

The rules followed to either complete, correct or remove users from the database were the following:

- If a user did not complete all the four sessions he is removed from the database.
- If a user did complete the four sessions, but in one or more of them an important part of her biometric data is missing or invalid (approximately more than 10% of all the genuine samples), tthen the user was removed from the database.
- If a user has a reduced number of missing or invalid genuine samples (approximately less than 10%), the samples are copied from valid samples of the same user. Therefore some identical samples may appear in the BiosecurID database.
- In the case of invalid or missing forgeries (PIN utterances, signature or keystroking), the expert verifying the database produced himself the missing or invalid samples.

In spite of the careful acquisition process and of all the post editing efforts, some acquisition errors are very difficult to find (e.g., errors in the naming of files) and will only be detected through the usage of the database. Thus, after the initial release it is likely that future updated versions of the database will appear.

3.4.6. Compatibility with other Databases

The design of the database is consistent with other available multimodal databases, which enables new experimental setups combining various databases. Thus, the devices and protocol used in the acquisition of some of the traits present in the BiosecurID database were chosen to be compatible with other existing databases, specifically:

- The **BioSec database**, with 250 subjects. Both databases present compatible characteristics (sensors and protocol) in the next traits: optical/thermal fingerprints, face, speech and iris. This way, combining both datasets, a 650 subjects multimodal database can be

	#Common Sub.	Fa	Fp	Ha	Hw	Ir	Ks	Sg	Sp
Biosecure PC (700 ap.)	29		×			×		×	
Biosecure Mobile (700 ap.)	29		×					×	
BioSec (250)	37	×	×			×			×
MyIDEA (104 ap.)	0		×					×	
MCYT (330)	0 ap.							×	

Table 3.5: *Summary of the main compatibilities of BiosecurID with other existing multimodal databases (in brackets appear the number of users of each database.)*

generated. Moreover, both databases (BioSec and BiosecurID) have 37 subjects in common, which allows to increase not only the number of users but also the number of sessions of the common donors, thus permitting real long term (2 year) temporal variability studies.

- The **Biosecure PC and mobile datasets**, with approximately 700 subjects in each dataset (400 subjects common to both of them). Similarly to the BioSec case, the Biosecure PC dataset is compatible with BiosecurID in optical/thermal fingerprints, iris, and signature. 29 of the subjects participated in both databases and so again long term variability and interoperability studies can be performed upon them.

Other multimodal databases such as MyIDEA (fingerprints, signature) or MCYT (signature) can also be combined with some portions of Biosecur-ID in order to increase the number of subjects as has been exposed with Biosec and Biosecure. However, in these cases no common subjects are available and so the number of sessions cannot be incremented. In Table 3.5 the main compatibilities of the BiosecurID database with other multimodal databases are summarized.

3.4.7. Potential Uses of the Database

Several potential uses of the database have already been pointed out throughout this paper. In this section some of the research lines that can be further developed upon this data set are summarized. It has to be emphasized that due to its unique characteristics in terms of size, acquisition environment and demographic distribution (age and gender), the BiosecurID database represents a good benchmark not only for the developing of new algorithms, but also for testing existing approaches in the challenging acquisition conditions present in BiosecurID. Some of the possible uses of the database are (in brackets we indicate the database features that make possible the different studies):

- Evaluation of potential attacks to unimodal, or real multibiometric systems (size, number of unimodal traits) [Galbally *et al.*, 2007, 2006].
- Research in any of the 8 available modalities or in multibiometric systems combining them (size, number of unimodal traits) [Jain *et al.*, 2008b].

- Evaluation of the effect of time on the systems performance (multisession, compatible with other databases): *i*) short term evaluation (samples within a session), *ii*) medium term evaluation (samples of different sessions), and *iii*) real long term evaluation (considering BiosecurID and Biosec common users). Research in biometric template adaptation and update [Marcialis *et al.*, 2008; Uludag *et al.*, 2003].

- Quality studies on different traits and its effect on multibiometric systems (realistic uncontrolled acquisition scenario, verification process with low quality samples not discarded) [Fierrez-Aguilar *et al.*, 2005c].

- Research on the effect of the users age on the recognition rates (balanced age distribution) [Modi *et al.*, 2007].

- Research and comparative studies of the systems performance depending on the gender (male/female) of the users (balanced gender distribution) [Moghaddam and Yang, 2002].

- Evaluation of the sensors interoperability in those traits acquired with several devices (fingerprint, speech), and its effect on multibiometric systems (multidevice, number of traits) [Grother *et al.*, 2008].

3.5. Chapter Summary and Conclusions

In this chapter we have outlined some best practices for performance evaluation in biometric authentication. We have also provided a description of the security evaluation protocol followed in this Thesis which can serve as guideline to carry out systematic and replicable vulnerability studies. Finally we have given an overview of the main existing multimodal biometric databases and we have described the most important one used in this Thesis: BiosecurID comprising samples from eight different biometric traits, and captured in four time separated acquisition sessions from 400 users in a real-like scenario.

This chapter includes novel contributions in the proposal of a systematic protocol for security evaluation of biometric systems, in the survey of the existing multimodal biometric databases, and in the description of the new corpus BiosecurID.

Chapter 4

New Methods for Vulnerability Assessment and Attack Protection

In this chapter we present three novel algorithmic methods which have been proposed during the development of the Thesis, and which will be used in the security evaluations carried out in the experimental part of the Dissertation (Chapters 5, 6, and 7.)

The presented algorithms are: *i*) a hill-climbing attack based on Bayesian adaptation which can be applied in a straight forward manner to different matchers and biometric traits, *ii*) a software-based liveness detection method for fingerprint recognition systems using quality measures (which presents the advantage over previously proposed schemes of needing just one image to determine whether it is real or fake), and *iii*) a complete scheme for the generation of totally synthetic on-line signatures based on the spectral information of the trajectory functions (unlike precedent approaches no real images are needed to produce the synthetic traits). All the three methods are validated on significant databases following systematic and replicable protocols, reaching remarkable results.

The hill-climbing attack will be used to carry out security evaluations of signature and face recognition systems in Chapters 6 and 7. The liveness detection approach is applied in Chapter 5 as a countermeasure against the direct attacks performed on the vulnerability evaluation of different fingerprint verification systems, while the synthetic signature generation method is used in Chapter 6 both to attack and improve the performance of a signature-based application.

The chapter is structured as follows. One section is dedicated to each of the novel methods, with the hill-climbing algorithm being presented in Sect. 4.1, the fingerprint liveness detection approach in Sect. 4.2, and the synthetic signature generation method in Sect. 4.3. These three sections share a common structure, with a brief introduction to the problem, the description of the algorithm, and finally the validation experiments, results and discussion. The chapter summary and conclusions are presented in Sect. 4.4.

This chapter assumes a basic understanding of the fundamentals of pattern recognition and classification [Duda *et al.*, 2001; Jain *et al.*, 2000; Theodoridis and Koutroumbas, 2006].

This chapter is based on the publications: Galbally *et al.* [2009a,e,f, 2007].

4.1. Hill-Climbing Attack Based on Bayesian Adaptation

As presented in Chapter 2, attacks on biometric systems can be broadly divided into: *i*) *direct attacks*, which are carried out at the sensor level using synthetic traits (e.g., printed iris images, gummy fingers); and *ii*) *indirect attacks*, which are carried out against the inner modules of the application and, therefore, the attacker needs to have some information about the system operation (e.g., matcher used, storage format).

Most of the works studying indirect attacks use some type of variant of the hill-climbing algorithm proposed by Soutar *et al.* [1999], which takes advantage of the score given by the matcher to iteratively change a synthetically created template until the similarity score exceeds a fixed decision threshold and the access to the system is granted. Some examples include hill-climbing attacks to a face-based system [Adler, 2004], or to PC and Match-on-Card minutiae-based fingerprint verification systems [Martinez-Diaz *et al.*, 2006; Uludag and Jain, 2004]. These hill-climbing approaches are all highly dependent of the technology used, only being usable for very specific types of matchers and for a given biometric trait.

In the present section, we propose a hill-climbing algorithm based on Bayesian adaptation [Duda *et al.*, 2001], inspired by the previously cited hill-climbing attacks and the adapted fusion approach developed by Fierrez-Aguilar *et al.* [2005a]. The contribution of this new approach lies in its generality: it can be applied in a straight forward manner for the security evaluation of any biometric system which uses fixed length feature vectors of real numbers and delivers real similarity (or dissimilarity) scores. The proposed attack uses the scores provided by the matcher to adapt a global distribution computed from a development set of users, to the local specificities of the client being attacked.

4.1.1. Hill-Climbing Algorithm

Problem statement. Consider the problem of finding a K-dimensional vector $\mathbf{y}^*$ which, compared to an unknown template $\mathcal{C}$ (in our case related to a specific client), produces a similarity score bigger than a certain threshold δ, according to some matching function J, i.e.: $J(\mathcal{C}, \mathbf{y}^*) > \delta$. The template can be another K-dimensional vector or a generative model of K-dimensional vectors.

Assumptions. Let us assume:

- That there exists a statistical model G (K-variate Gaussian with mean $\boldsymbol{\mu}_G$ and diagonal covariance matrix $\boldsymbol{\Sigma}_G$, with $\boldsymbol{\sigma}_G^2 = \text{diag}(\boldsymbol{\Sigma}_G)$), in our case related to a background set of users, overlapping to some extent with $\mathcal{C}$.
- That we have access to the evaluation of the matching function $J(\mathcal{C}, \mathbf{y})$ for several trials of $\mathbf{y}$.

Algorithm. The problem of finding $\mathbf{y}^*$ can be solved by adapting the global distribution G to the local specificities of template $\mathcal{C}$, through the following iterative strategy:

1. Take N samples $(\mathbf{y}_i)$ of the global distribution G, and compute the similarity scores $J(\mathcal{C}, \mathbf{y}_i)$, with $i = 1, \ldots, N$.

2. Select the M points (with $M < N$) which have generated highest scores.

3. Compute the local distribution $L(\boldsymbol{\mu}_L, \boldsymbol{\sigma}_L)$, also K-variate Gaussian, based on the M selected points.

4. Compute an adapted distribution $A(\boldsymbol{\mu}_A, \boldsymbol{\sigma}_A)$, also K-variate Gaussian, which trades off the general knowledge provided by $G(\boldsymbol{\mu}_G, \boldsymbol{\sigma}_G)$ and the local information given by $L(\boldsymbol{\mu}_L, \boldsymbol{\sigma}_L)$. This is achieved by adapting the sufficient statistics as follows [Fierrez-Aguilar *et al.*, 2005a]:

$$\boldsymbol{\mu}_A = \alpha\boldsymbol{\mu}_L + (1-\alpha)\boldsymbol{\mu}_G \tag{4.1}$$

$$\boldsymbol{\sigma}_A^2 = \alpha(\boldsymbol{\sigma}_L^2 + \boldsymbol{\mu}_L^2) + (1-\alpha)(\boldsymbol{\sigma}_G^2 + \boldsymbol{\mu}_G^2) - \boldsymbol{\mu}_A^2 \tag{4.2}$$

5. Redefine $G = A$ and return to step 1.

In Eq. (4.1) and (4.2), $\boldsymbol{\mu}^2$ is defined as $\boldsymbol{\mu}^2 = \mathrm{diag}(\boldsymbol{\mu}\boldsymbol{\mu}^T)$, and α is an adaptation coefficient in the range [0,1]. The algorithm finishes either when one of the N similarity scores computed in step 2 exceeds the given threshold δ, or when the maximum number of iterations is reached.

In the above algorithm there are two key concepts not to be confused, namely: *i*) number of *iterations* (n_{it}), which refers to the number of times that the statistical distribution G is adapted, and *ii*) number of *comparisons* (n_{comp}), which denotes the total number of matchings carried out through the algorithm. Both numbers are related through the parameter N, being $n_{comp} = N \cdot n_{it}$.

This last parameter (n_{comp}) corresponds to the efficiency of an attack defined in Sect. 3.2, and thus will be referred to as E_{ff} in the experimental chapters.

4.1.2. Validation Experimental Framework

The proposed hill-climbing algorithm has been successfully applied to attack a feature-based on-line signature verification system, and two different face recognition systems (one based on PCA and the other a parts-based system using GMMs). The detailed description of these security evaluations which serve as validation of the attacking approach can be found, respectively, in Chapters 6 and 7 of the present Dissertation.

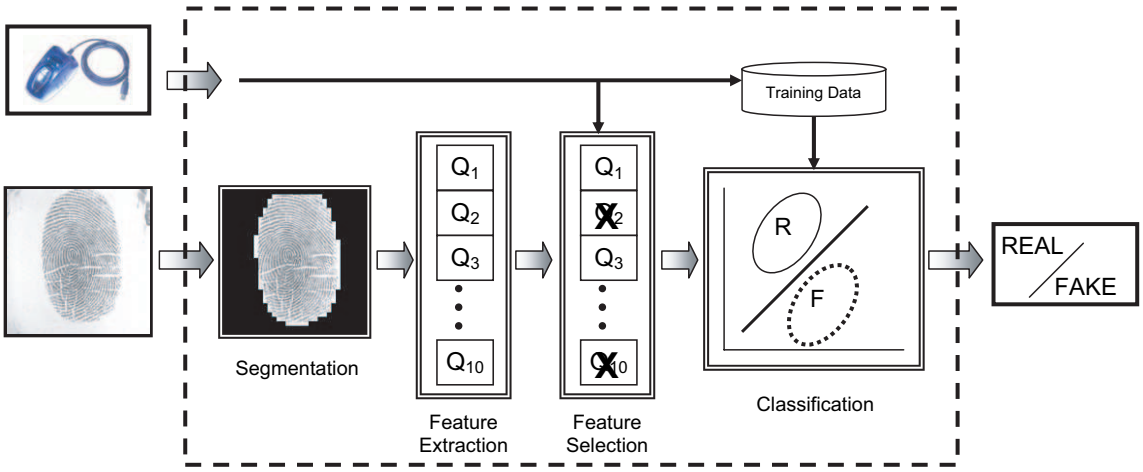


Figure 4.1: *General diagram of the fingerprint liveness detection approach presented in this work.*

4.2. Liveness Detection Based on Quality Measures

In the last recent years important research efforts have been conducted to study the vulnerabilities of biometric systems to direct attacks to the sensor (carried out using synthetic biometric traits such as gummy fingers or high quality iris printed images) [Matsumoto *et al.*, 2002; Ruiz-Albacete *et al.*, 2008], which have led to an enhancement of the security level offered by biometric systems through the proposal of specific countermeasures. In particular, different liveness detection methods have been presented. These algorithms are anti-spoofing techniques which use different physiological properties to distinguish between real and fake traits, thus improving the robustness of the system against direct attacks.

In this section we propose a new parameterization based on quality measures for a software-based solution in fingerprint liveness detection (i.e., features used to distinguish between real and fake fingers are extracted from the fingerprint image, and not from the finger itself). This novel strategy has the clear advantage over previously proposed methods of needing just one fingerprint image (i.e., the same fingerprint image used for access) to extract the necessary features in order to determine if the finger presented to the sensor is real or fake. This fact shortens the acquisition process and reduces the inconvenience for the final user.

The presented method has been validated on the database provided as development set in the Fingerprint Liveness Detection Competition LivDET 2009 LivDet [2009], comprising over 4,500 real and fake samples generated with different materials and captured with different sensors. The experimental validation results show its high potential as a liveness detection algorithm.

4.2.1. The Liveness Detection Approach

The problem of liveness detection can be seen as a two-class classification problem where an input fingerprint image has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate

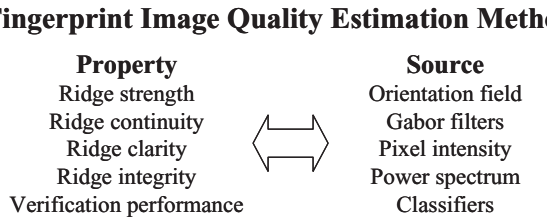


Figure 4.2: *Taxonomy of the different approaches for fingerprint image quality computation that have been described in the literature.*

classifier which gives the probability of the image vitality given the extracted set of features. In the present work we propose a novel parameterization using quality measures which is tested on a complete liveness detection system.

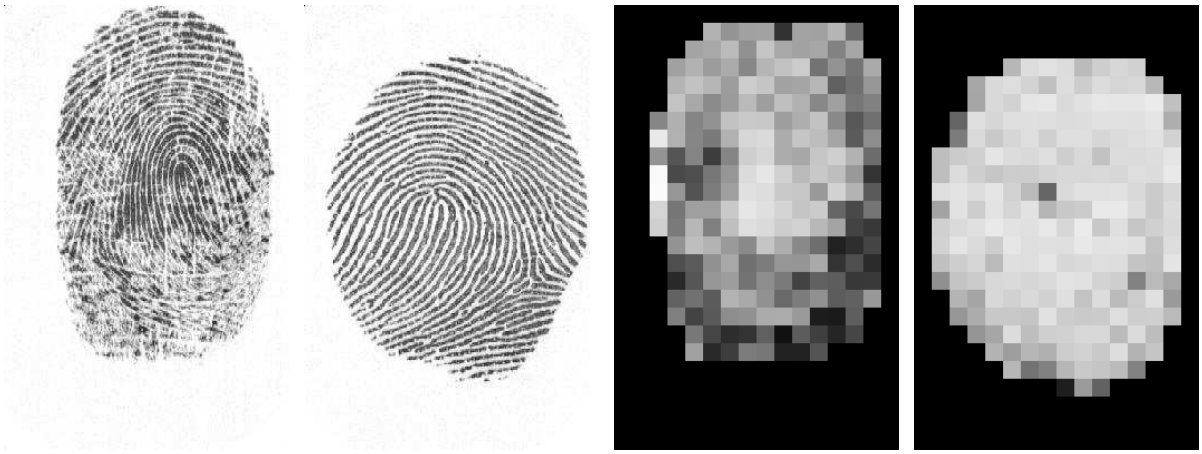
A general diagram of the liveness detection system presented in this work is shown in Fig. 4.1. Two inputs are given to the system: *i*) the fingerprint image to be classified, and *ii*) the sensor used in the acquisition process.

In the first step the fingerprint is segmented from the background, for this purpose, Gabor filters are used as proposed by Shen *et al.* [2001]. Once the useful information of the total image has been separated, ten different quality measures are extracted which will serve as the feature vector that will be used in the classification. Prior to the classification step, the best performing features are selected depending on the sensor that was used in the acquisition. Once the final feature vector has been generated the fingerprint is classified as real (generated by a living finger), or fake (coming from a gummy finger), using as training data of the classifier the dataset corresponding to the acquisition sensor.

4.2.1.1. Feature Extraction

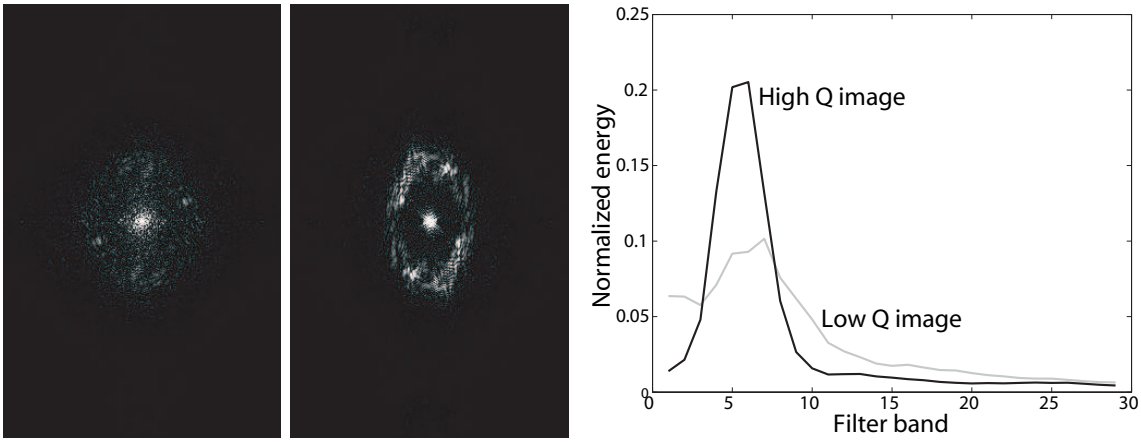
The parameterization proposed in the present work and applied to liveness detection comprises ten quality-based features. A number of approaches for fingerprint image quality computation have been described in the literature. A taxonomy is given by Alonso-Fernandez *et al.* [2008] (see Fig. 4.2). Image quality can be assessed by measuring one of the following properties: ridge strength or directionality, ridge continuity, ridge clarity, integrity of the ridge-valley structure, or estimated verification performance when using the image at hand. A number of sources of information are used to measure these properties: *i*) angle information provided by the direction field, *ii*) Gabor filters, which represent another implementation of the direction angle [Bigun, 2006a], *iii*) pixel intensity of the gray-scale image, *iv*) power spectrum, and *v*) Neural Networks. Fingerprint quality can be assessed either analyzing the image in a holistic manner, or combining the quality from local non-overlapped blocks of the image.

In the following, we give some details about the quality measures used in this paper. We have implemented several measures that make use of the above mentioned properties for quality assessment (a summary of the different quality measures is given at the end of the parameter description in Table 4.1):



(a) (b)

Figure 4.3: *Computation of the Orientation Certainty Level (OCL) for two fingerprints of different quality. Panel (a) are the input fingerprint images. Panel (b) are the block-wise values of the OCL; blocks with brighter color indicate higher quality in the region.*

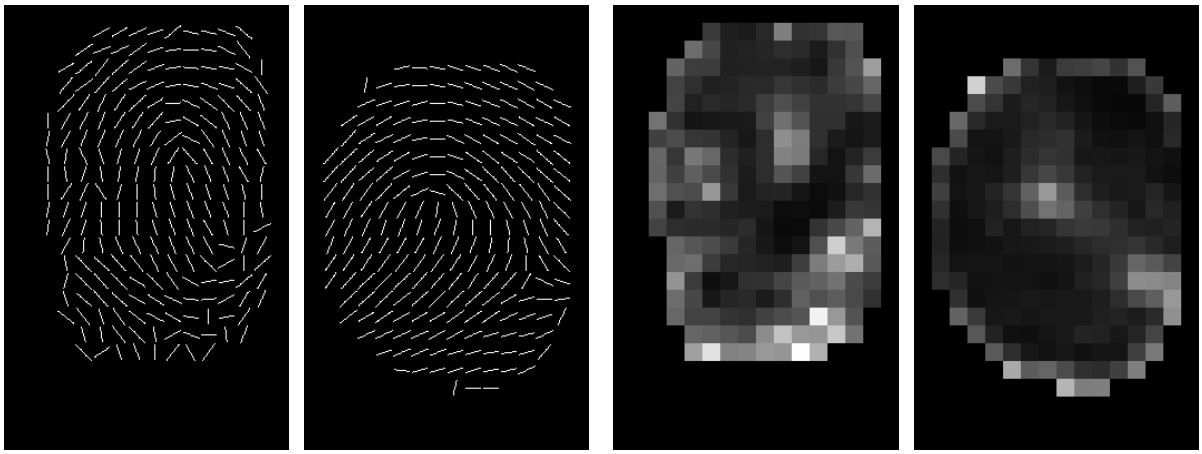


(a) Power spectrum (b) Energy concentration

Figure 4.4: *Computation of the energy concentration in the power spectrum for two fingerprints of different quality. Panel (a) are the power spectra of the images shown in Figure 4.3. Panel (b) shows the energy distributions in the region of interest. The quality values for the low and high quality image are* 0.35 *and* 0.88 *respectively.*

Ridge-strength measures

- **Orientation Certainty Level (Q_{OCL})** [Lim *et al.*, 2002], which measures the energy concentration along the dominant direction of ridges using the intensity gradient. It is computed as the ratio between the two eigenvalues of the covariance matrix of the gradient vector. A relative weight is given to each region of the image based on its distance from the centroid, since regions near the centroid are supposed to provide more reliable information [Chen *et al.*, 2005a]. An example of Orientation Certainty Level computation is shown in



(a) (b)

Figure 4.5: *Computation of the Local Orientation Quality (LOQ) for two fingerprints of different quality. Panel (a) are the direction fields of the images shown in Figure 4.3 (a). Panel (b) are the block-wise values of the average absolute difference of local orientation with the surrounding blocks; blocks with brighter color indicate higher difference value and thus, lower quality.*

Fig. 4.3 for two fingerprints of different quality.

- **Energy concentration in the power spectrum (Q_E)** [Chen *et al.*, 2005a], which is computed using ring-shaped bands. For this purpose, a set of bandpass filters is employed to extract the energy in each frequency band. High quality images will have the energy concentrated in few bands while poor ones will have a more diffused distribution. The energy concentration is measured using the entropy. An example of quality estimation using the global quality index Q_E is shown in Fig. 4.4 for two fingerprints of different quality.

Ridge-continuity measures

- **Local Orientation Quality (Q_{LOQ})** [Chen *et al.*, 2004], which is computed as the average absolute difference of direction angle with the surrounding image blocks, providing information about how smoothly direction angle changes from block to block. Quality of the whole image is finally computed by averaging all the Local Orientation Quality scores of the image. In high quality images, it is expected that ridge direction changes smoothly across the whole image. An example of Local Orientation Quality computation is shown in Fig. 4.5 for two fingerprints of different quality.

- **Continuity of the orientation field (Q_{COF})** [Lim *et al.*, 2002]. This method relies on the fact that, in good quality images, ridges and valleys must flow sharply and smoothly in a locally constant direction. The direction change along rows and columns of the image is examined. Abrupt direction changes between consecutive blocks are then accumulated

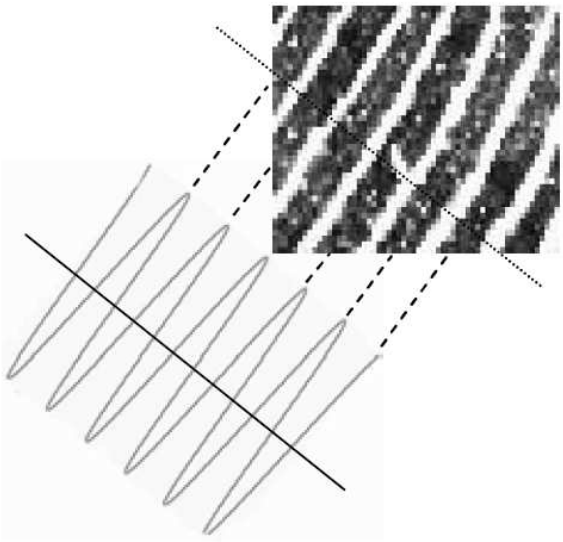


Figure 4.6: *Modeling of ridges and valleys as a sinusoid.*

and mapped into a quality score. As we can observe in Fig. 4.5, ridge direction changes smoothly across the whole image in case of high quality.

Ridge-clarity measures

- **Mean (Q_{MEAN})** and **standard deviation (Q_{STD})** values of the gray level image, computed from the segmented foreground only. These two features had already been considered for liveness detection by Coli *et al.* [2008].

- **Local Clarity Score (Q_{LCS1} and Q_{LCS2})** [Chen *et al.*, 2004]. The sinusoidal-shaped wave that models ridges and valleys is used to segment ridge and valley regions (see Fig. 4.6) [Hong *et al.*, 1998]. The clarity is then defined as the overlapping area of the gray level distributions of segmented ridges and valleys. For ridges/valleys with high clarity, both distributions should have a very small overlapping area. An example of quality estimation using the Local Clarity Score is shown in Fig. 4.7 for two fingerprint blocks of different quality. It should be noted that sometimes the sinusoidal-shaped wave cannot be extracted reliably, specially in bad quality regions of the image. The quality measure Q_{LCS1} discards these regions, therefore being an optimistic measure of quality. This is compensated with Q_{LCS2}, which does not discard these regions, but they are assigned the lowest quality level.

- **Amplitude and variance of the sinusoid that models ridges and valleys (Q_A and Q_{VAR})** [Hong *et al.*, 1998]. Based on these parameters, blocks are classified as *good* and *bad*. The quality of the fingerprint is then computed as the percentage of foreground blocks marked as *good*.

A summary of the different quality measures used as parameterization in the proposed live-

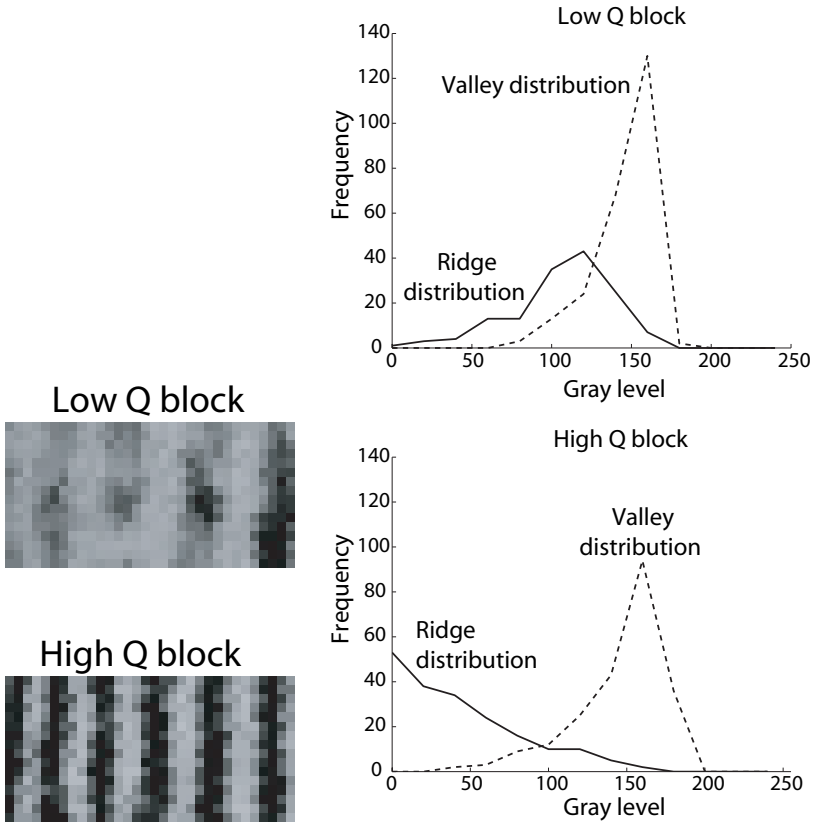


Figure 4.7: *Computation of the Local Clarity Score for two fingerprint blocks of different quality. Panel (a) shows the fingerprint blocks. Panel (b) shows the gray level distributions of the segmented ridges and valleys. The degree of overlapping for the low and high quality block is* 0.22 *and* 0.10*, respectively.*

ness detection approach and described above is given in Table 4.1.

4.2.1.2. Feature Selection

Due to the curse of dimensionality, it is possible that the best classifying results are not obtained using the set of ten proposed features, but a subset of them. As we are dealing with a ten dimensional problem there are $2^{10}-1 = 1,023$ possible feature subsets, which is a reasonably low number to apply exhaustive search as feature selection technique in order to find the best performing feature subset. This way we guarantee that we find the optimal set of features out of all the possible ones. The feature selection depends on the acquisition device (as shown in Fig. 4.1), as the optimal feature subsets might be different for different sensors.

4.2.1.3. Classifier

We have used Linear Discriminant Analysis (LDA) as classifier [Duda *et al.*, 2001]. In the experiments the leave-one-out technique has been used, where all the samples acquired with

Quality measure	Property measured	Source
Q_{OCL}	Ridge strength	Local angle
Q_E	Ridge strength	Power spectrum
Q_{LOQ}	Ridge continuity	Local angle
Q_{COF}	Ridge continuity	Local angle
Q_{MEAN}	Ridge clarity	Pixel intensity
Q_{STD}	Ridge clarity	Pixel intensity
Q_{LCS1}	Ridge clarity	Pixel intensity
Q_{LCS2}	Ridge clarity	Pixel intensity
Q_A	Ridge clarity	Pixel intensity
Q_{VAR}	Ridge clarity	Pixel intensity

Table 4.1: *Summary of the quality measures used in the parameterization applied to fingerprint liveness detection.*

the same sensor, except the one being classified, are used to fit the two normal distributions representing each of the classes. The sample being classified (which was left out of the training process) is then assigned to the most probable class.

4.2.2. Validation Experimental Framework

The proposed liveness detection approach is validated on the development set of the Fingerprint Liveness Detection Competition LivDET 2009 [LivDet, 2009]. The objective of the validation experiments is to estimate the efficiency of the presented method as a way to discriminate between images produced by real and fake fingers. To achieve this purpose, first we search for the optimal feature subsets (out of the proposed 10 feature set) for each of the three datasets comprised in the database. Then the classification performance of each of the optimal subsets is computed on each of the datasets in terms of the Average Classification Error which is defined as $ACE = (FLR + FFR)/2$, where the FLR (False Living Rate) represents the percentage of fake fingerprints misclassified as real, and the FFR (False Fake Rate) computes the percentage of real fingerprints assigned to the fake class.

4.2.2.1. Database

The database used in the experiments is the development set provided in the Fingerprint Liveness Detection Competition, LivDET 2009 LivDet [2009]. It comprises three datasets of real and fake fingerprints (generated with different materials) captured each of them with a different optical sensor:

- Biometrika FX2000 (569 dpi). This dataset comprises 520 real and 520 fake images. The latter were generated with gummy fingers made of silicone.

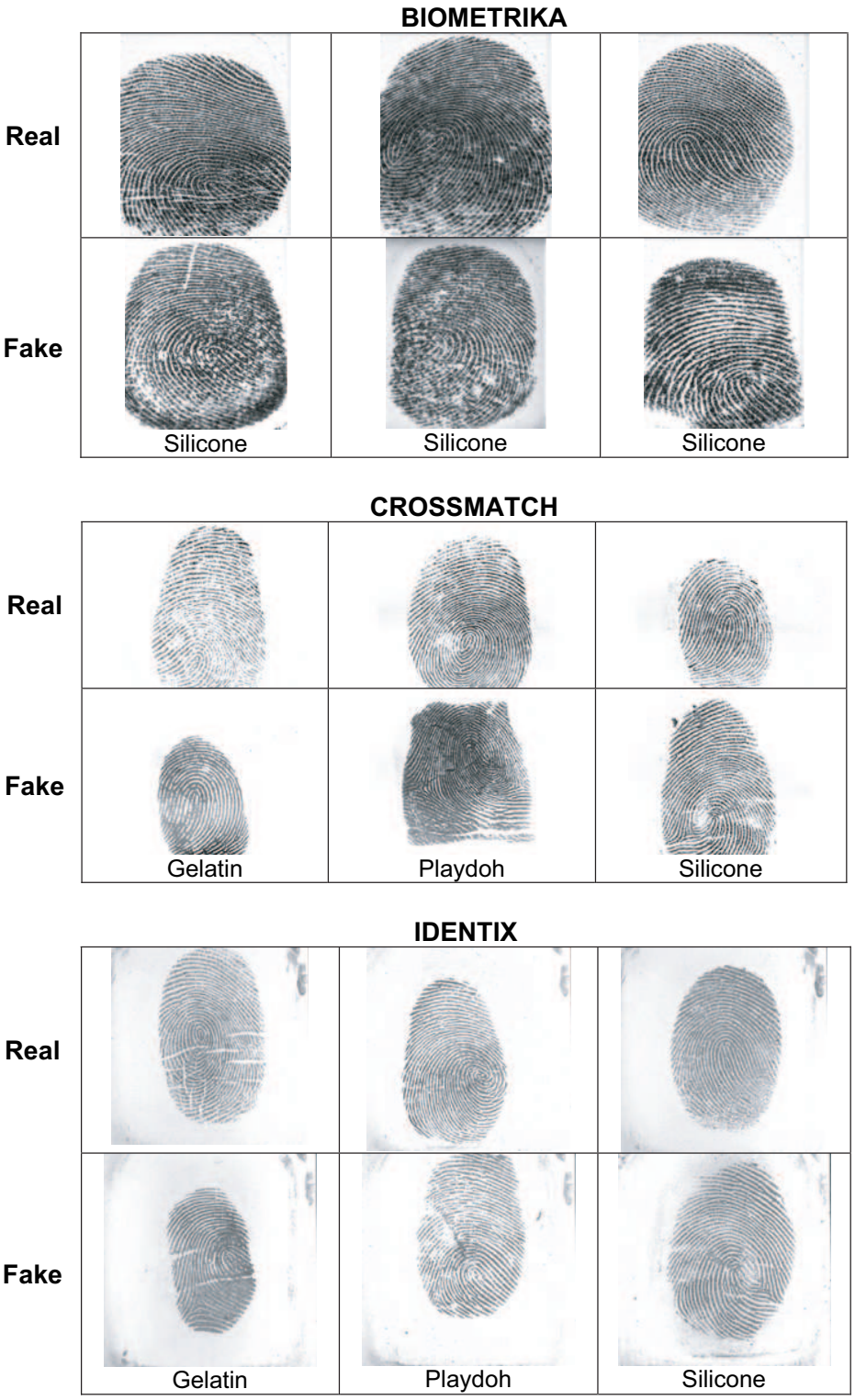


Figure 4.8: *Typical examples of real and fake fingerprint images that can be found in the database used in the experiments.*

- CrossMatch Verifier 300CL (500 dpi). This dataset comprises 1,000 real and 1,000 fake images. The latter were generated with gummy fingers made of silicone (310), gelatin (344), and playdoh (346).
- Identix DFR2100 (686 dpi). This dataset comprises 750 real and 750 fake images. The fake images were generated with gummy fingers made of silicone (250), gelatin (250), and playdoh (250).

The material with which the different fake images are made is known, however this information is not used in anyway by the liveness detection system as in a real case it would not be available to the application. Thus, as will be explained in the experiments, the feature selection is just made in terms of the sensor used in the acquisition.

In Fig. 4.8 we show some typical examples of the real and fake fingerprint images that can be found in the database (not necessarily belonging to the same subject). The fake fingerprints corresponding to the CrossMatch and Identix datasets were generated with each of the different materials. It can be noticed from the examples shown in Fig. 4.8 the difficulty of the classification problem, as even for a human expert it would not be easy to distinguish between the real and fake samples present at the database.

4.2.2.2. Results

Feature Selection Results

In order to find the optimal feature subsets, for each of the three datasets in the database, the classification performance of each of the 1,023 possible feature subsets was computed using the leave-one-out technique (i.e., all the samples in the dataset are used to train the classifier except the one being classified). The best feature subsets (for an increasing number of features N_f) found for each of the sensors are shown in Table 4.2, where a $\times$ means that the feature is included in the subset. The Average Classification Error for each of the best subsets is shown on the right (in percentage), and the optimal feature subset is highlighted in grey.

From the results shown in Table 4.2 we can see that the most discriminant features for the Biometrika dataset are those measuring the ridge strength. Also, one ridge continuity (Q_{LOQ}) and one ridge clarity (Q_{MEAN}) measure are shown to provide certain discriminative capabilities with this sensor. In the case of the CrossMatch sensor, on the other hand, the least useful features for liveness detection are the ridge continuity related, while the ridge strength and ridge clarity measures have a similar importance (only Q_{MEAN} clearly stands out). In the Identix dataset we can see that the best features are the ridge clarity related (specially Q_{STD}, Q_{LCS1}, and Q_{LCS2}), and, on the other hand, the ridge strength related are the least discriminant. The information extracted from Table 4.2 on the discriminant capabilities of the different parameters according to the ridge property measured is summarized in Table 4.3.

The evolution of the ACE produced by each of the best feature subsets (right column in Table 4.2) and for the three datasets is shown in Fig. 4.9, where the optimal error for each dataset

Best feature subsets for quality-based liveness detection: Biometrika Dataset											
	Ridge Strength		*Ridge Continuity*		*Ridge Clarity*						
N_f	$\mathbf{Q_{OCL}}$	$\mathbf{Q_E}$	$\mathbf{Q_{LOQ}}$	Q_{COF}	$\mathbf{Q_{MEAN}}$	Q_{STD}	Q_{LCS1}	Q_{LCS2}	Q_A	Q_{VAR}	ACE
1		×									21.83
2		×						×			13.37
3		×			×			×			7.60
4	×	×	×		×						4.71
5	×	×	×			×			×		2.60
6	×	×	×		×	×			×		2.12
7	×	×	×	×	×	×				×	1.73
8	×	×	×	×	×	×		×		×	1.83
9	×	×	×	×	×	×		×	×	×	2.02
10	×	×	×	×	×	×	×	×	×	×	2.31

Best feature subsets for quality-based liveness detection: CrossMatch Dataset											
	Ridge Strength		*Ridge Continuity*		*Ridge Clarity*						
N_f	Q_{OCL}	$\mathbf{Q_E}$	Q_{LOQ}	Q_{COF}	$\mathbf{Q_{MEAN}}$	Q_{STD}	Q_{LCS1}	$\mathbf{Q_{LCS2}}$	Q_A	Q_{VAR}	ACE
1					×						17.65
2					×					×	13.25
3					×		×		×		11.80
4		×			×			×		×	11.30
5		×			×	×		×		×	11.45
6	×	×			×	×	×	×			11.15
7	×	×	×		×	×	×	×			11.35
8	×	×		×	×	×	×	×	×		11.55
9	×	×	×	×	×	×	×	×		×	11.95
10	×	×	×	×	×	×	×	×	×	×	12.80

Best feature subsets for quality-based liveness detection: Identix Dataset											
	Ridge Strength		*Ridge Continuity*		*Ridge Clarity*						
N_f	Q_{OCL}	Q_E	Q_{LOQ}	Q_{COF}	Q_{MEAN}	$\mathbf{Q_{STD}}$	$\mathbf{Q_{LCS1}}$	$\mathbf{Q_{LCS2}}$	Q_A	Q_{VAR}	ACE
1					×						20.07
2			×			×					11.93
3						×	×	×			9.40
4				×		×	×	×			7.67
5	×		×			×	×	×			7.20
6				×		×	×	×	×	×	7.07
7		×	×			×	×	×	×	×	6.87
8		×		×	×	×	×	×	×	×	6.93
9	×	×	×	×	×	×	×	×		×	7.13
10	×	×	×	×	×	×	×	×	×	×	7.20

Table 4.2: *Best performing subsets with an increasing number of features. N_f stands for* number of features*, and the ACE is given in %. The symbol × means that the feature is considered in the subset. The optimal feature subset for each of the datasets is highlighted in grey. The best performing features are presented in* ***bold****.*

	Ridge Strength	Ridge Continuity	Ridge Clarity
Biometrika	High (Q_E, Q_{OCL})	Medium (Q_{LOQ})	Medium (Q_{MEAN})
CrossMatch	Medium (Q_E)	Low	High (Q_{MEAN}, Q_{LCS2})
Identix	Low	Medium	High (Q_{STD}, Q_{LCS1}, Q_{LCS2})

Table 4.3: *Summary for the three datasets of the parameters discriminant power according to the ridge property measured. The best performing features are specified in each case.*

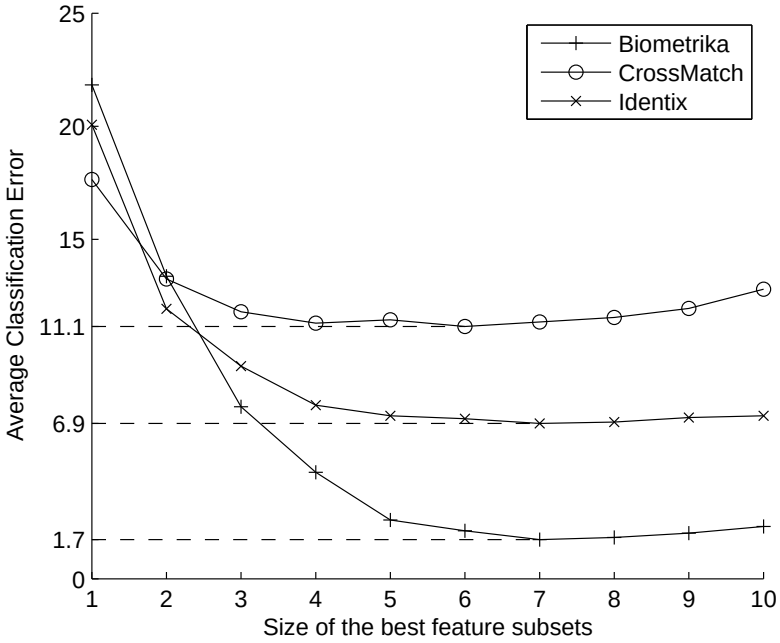


Figure 4.9: *Evolution of the ACE for the best feature subsets with an increasing number of features, and for the three datasets.*

is highlighted with a horizontal dashed line. In Fig. 4.9 we can see that the proposed parameterization is specially effective for liveness detection with the Biometrika sensor where the ACE rapidly decreases when new features are added, while for the other two sensors the improvement in the error classification rate is smaller (in particular in the case of the CrossMatch).

Optimal Feature Subsets

Considering only the optimal feature subsets found for each of the sensors (highlighted in grey in Table 4.2), we can see that the two most consistent features (that are included in the best subset for all the datasets) are Q_E and Q_{STD}. On the other hand, there is no feature that is not included at least in one of the optimal subsets which indicates that all the proposed features are relevant for fingerprint liveness detection.

	Best subset for Biometrika Q_{OCL}, Q_E, Q_{LOQ}, Q_{COF}, Q_{MEAN}, Q_{STD}, Q_{VAR}		
	FAR (%)	FRR (%)	ACE (%)
Biometrika	2.12	1.54	1.73
CrossMatch	12.48	12.32	12.40
Identix	6.40	10.67	8.53
TOTAL	7.00	8.17	7.58

(*a*) Performance of the best feature subset for the Biometrika dataset.

	Best subset for CrossMatch Q_{OCL}, Q_E, Q_{MEAN}, Q_{STD}, Q_{LCS1}, Q_{LCS2}		
	FAR (%)	FRR (%)	ACE (%)
Biometrika	6.73	2.50	4.62
CrossMatch	10.30	11.94	11.12
Identix	6.27	11.47	8.87
TOTAL	7.76	8.63	8.12

(*b*) Performance of the best feature subset for the CrossMatch dataset.

	Best subset for Identix Q_E, Q_{LOQ}, Q_{STD}, Q_{LCS1}, Q_{LCS2}, Q_A, Q_{VAR}		
	FAR (%)	FRR (%)	ACE (%)
Biometrika	6.92	0.96	3.94
CrossMatch	11.42	11.98	11.70
Identix	6.40	7.07	6.73
TOTAL	8.24	6.67	7.45

(*c*) Performance of the best feature subset for the Identix dataset.

Table 4.4: *Performance in terms of the Average Classification Error (ACE) of each optimal feature subset for the Biometrika (a), CrossMatch (b), and Identix (c) datasets. The best ACE for the different datasets is highlighted in grey.*

The classification performance of each of the optimal feature subsets was computed for the three datasets, again using the leave-one-out technique. Results for each of the subsets are given in Table 4.4 where the best result (the one corresponding to the optimal subset of a certain dataset, used to classify the images in that same dataset) is highlighted in grey.

From the results shown in Table 4.4 we can see that the optimal combination of features that generalizes best to all the sensors is the one corresponding to the Identix dataset as it produces the lowest total ACE (7.45%). However, all the optimal feature subsets have proven to be robust in the three datasets as the total ACE does not differ greatly.

The results also show that the new parameterization proposed performs best on the dataset captured with the Biometrika sensor where, for the optimal feature subset, an ACE of 1.73% is reached (over 98% of correctly classified samples). This result clearly improves the one presented by Coli *et al.* [2008] where, on a very similar dataset and using a parameterization based on different static and dynamic features (which need several images to be extracted), a best 17%

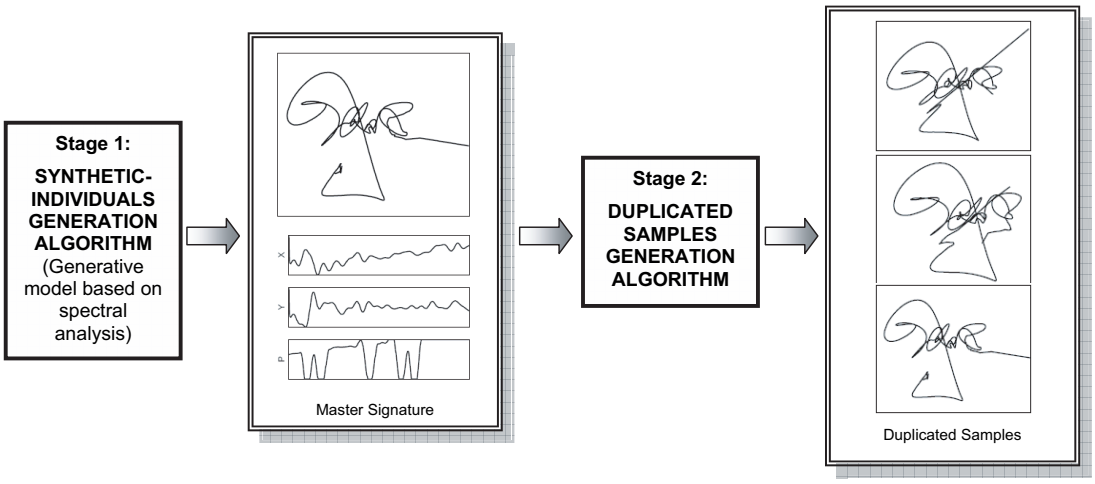


Figure 4.10: *General architecture of the synthetic signature generation algorithm proposed.*

classification error is reported.

On the other hand, the worst classification rate of our system is always generated on the CrossMatch dataset with a 11.12% of misclassified samples in the best case. An intermediate performance between the Biometrika and the CrossMatch datasets is reached for the Identix dataset in all cases.

Assuming that we can use for each of the datasets their own optimal feature subset (which is not a strong constraint as we should know the sensor used by the system), then the total ACE would be the average of the cells highlighted in grey in Table 4.4, and the system would present an optimal **ACE=6.56%**. This means that the system described in this work, using the new parameterization proposed, can correctly classify 93.44% of the fingerprint images available in the database, using just one single sample.

Also important to notice that the proposed liveness detection approach will affect the performance of the system where it is implemented under the normal operation scenario. In particular this countermeasure will increase the FRR of the system in a percentage equivalent, at the most, to the ACE. In particular, for the case considered in the validation experiments, 6.56% of the legitimate users would be rejected by the system due to an incorrect decision of the liveness detection method (i.e., considering real fingers as fake).

4.3. Synthetic On-Line Signature Generation Based on Spectral Analysis

This section studies the synthetic generation of the so called *occidental* signatures. In opposition to other types of signatures consisting of independent symbols, such as the *asian* signatures, the occidental signatures typically consist of handwritten concatenated text and some form of flourish.

As was introduced in Chapter 2 the different existing methods to generate synthetic biometric

data can be classified into: *i*) duplicated samples (i.e., multiple synthetic samples of one or more real impressions are generated this way) [Rabasse *et al.*, 2007; Richiardi, 2008], *ii*) combination of different real samples, usually used in the generation of synthetic handwriting (i.e., different characters of a given subject are combined to produce words) [Ballard *et al.*, 2007; Lin and Wang, 2007], and *iii*) synthetic-individuals, in this case a generative model is produced to obtain the synthetic traits and no real samples are needed to produce them [Cappelli, 2003; Zuo *et al.*, 2007].

In the present section we will describe a new model-based approach for realistic signature generation based on information obtained from the frequency domain, which does not need of any previously acquired real samples. The algorithm, as can be seen in Fig. 4.10, presents two different stages, in the first one a *master signature* corresponding to a synthetic individual is produced using a generative model based on spectral information (no real signatures are used in the process), in the second stage that master signature is used to generate different samples of that same synthetic user (following a generation scheme of duplicated samples).

The motivation to base our model on spectral analysis comes mainly from two facts. On the one hand, spectral analysis constitutes a general and powerful tool that enables the parameterization of complex time functions such as the ones found in online signature biometrics. This is for example patent in the work of Kholmatov and Yanikoglu [2008] who used it to devise a spectrum-based signature parameterization for their individuality study of the online signature biometrics. On the other hand, working with the spectrum of the signature functions permits us to exploit some similarities that we have heuristically found among different occidental handwritten signatures (this point will be further detailed in Sect. 4.3.1).

The validation methodology of the algorithm is based on qualitative and quantitative results which show the suitability of the technique and the high degree of similarity existing between the synthetic signatures generated and real signatures.

4.3.1. Generation of Synthetic Individuals

Although other signals such as the azimuth and elevation angles of the input pen might be taken into account, in this work we will consider that an online signature is defined by three time sequences $[x[n]\ y[n]\ p[n]]$ specifying each of them the x and y coordinates, and the pressure applied during the signing process at the time instants $n = 1, \ldots, N$ (here sampled at 100 Hz).

The algorithm proposed in the present contribution to generate synthetic signers comprises three successive steps, as can be seen in Fig. 4.11. A first step, carried out in the frequency domain, in which the synthetic Discrete Fourier Transform (DFT) of the trajectory signals x and y is generated using a parametrical model, obtained by spectral analysis of a development set of real signatures. In the second stage the resulting trajectory signals are used to place the penups of the pressure function. Finally, in the last stage, all the three signals are processed in the time domain in order to give the synthetic signatures a more realistic appearance. These three steps are described next.

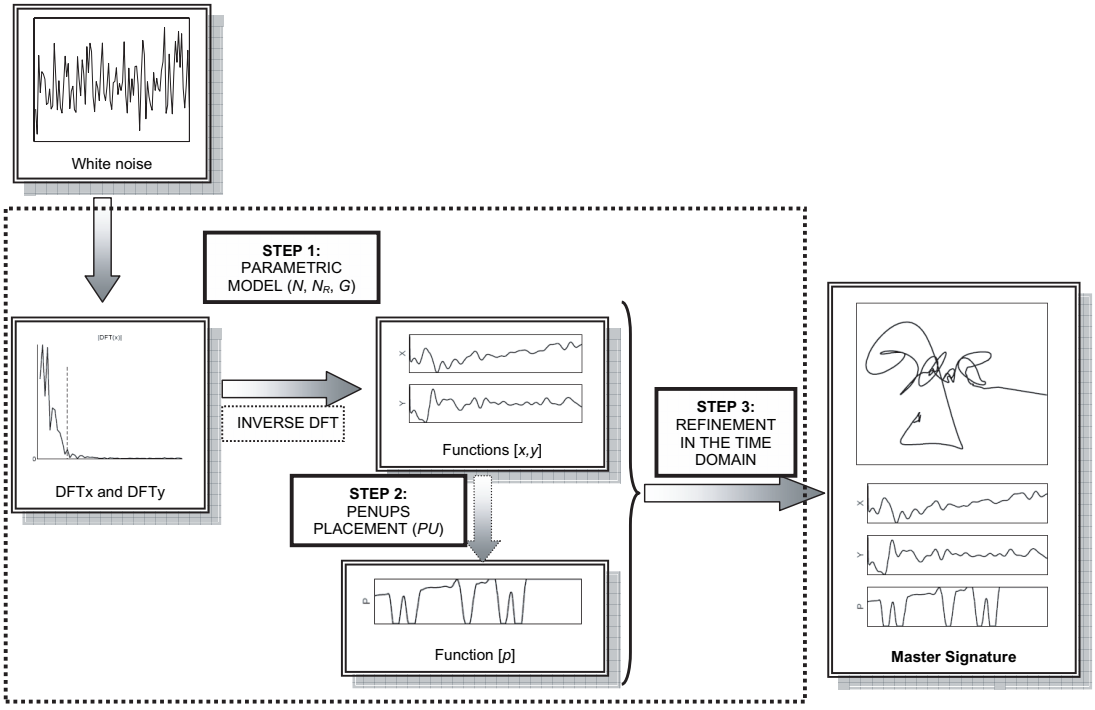


Figure 4.11: *General diagram of the synthetic individuals generation algorithm proposed.*

4.3.1.1. Signature Model in the Frequency Domain

In this step, a parametrical model is used to generate the DFT of the synthetic signature coordinate functions, which is based on a linear filter defined in the frequency domain.

The parametrical model proposed in the present contribution is based on the high degree of similarity existing among the trajectory signals of real signatures in the frequency domain. In Fig. 4.12 some examples of DFTs of the x and y signals are shown, where we can observe that the energy of the coefficients rapidly decreases in the initial harmonics and remains constant and practically negligible from that point (marked with a vertical dashed line in Fig. 4.12) to the end.

This common structure of the spectrum of x and y, allows us to determine a model defined by the next parameters:

- **Sequence Length** (N). It defines the number of samples of the three time functions x, y, and p. As will be explained in Sect. 4.3.3, it is computed according to the length distribution of the signatures comprised in the BiosecurID database [Fierrez *et al.*, 2009].

- **Number of Relevant Spectral Coefficients** (N_R). It defines the number of coefficients which have a significant power (i.e., those which appear before the dashed line in Fig. 4.12). This parameter is computed as a percentage of N, $N_R = \delta N$, where δ follows a uniform distribution between $\delta^{\min} > 0$ and $\delta^{\max} < 1$.

- **Power Ratio** (G). Computed as the quotient between the power of the relevant spectral

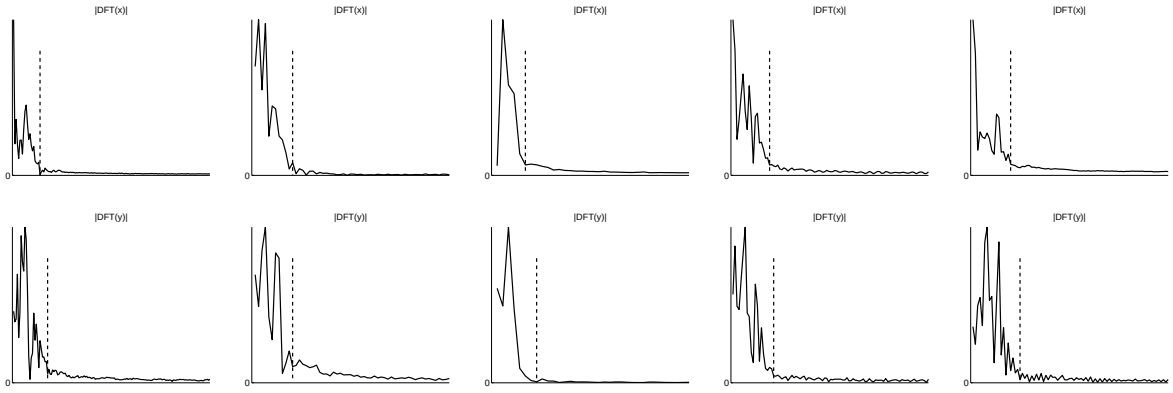


Figure 4.12: *DFT amplitude examples of the trajectory functions* x *(top) and* y *(bottom), of 5 real signatures (from left to right).*

coefficients, and that of the last spectral coefficients (i.e., in Fig. 4.12 those after the dashed line), $G = P_R/P_I$. The value of G is taken from a uniform distribution, $G \in [G^{\min}, G^{\max}]$.

In order to generate a synthetic signature, the DFT of each of the trajectory signals is generated colouring white noise with the described parametrical model. This approach implies two simplifications: *i*) that all Fourier coefficients are independent, and *ii*) that both coordinate functions x and y are independent.

Once the synthetic DFT of both trajectory signals has been generated, we compute the Inverse DFT (IDFT) in order to obtain the coordinate functions x and y in the time domain.

4.3.1.2. The Pressure Function

The two main features defining the pressure function of a signature are:

- **Number of Penups** (PU). A penup is a zero pressure segment of the signature (it occurs when the pen is lifted from the paper during the signing process). The number of penups PU was extracted from the BiosecurID database, and applied to the synthetic signatures according to their length N (i.e., a longer signature presents a higher probability of having a large number of penups).

- **Placing of the Penups**. From an heuristical analysis of the y and p signals of real signatures we can conclude that most penups occur close to a singular point (maximum or minimum) of the y function.

With these two premises, the penups are located through the pressure function and some maximum points (between penups) are determined randomly. In a successive step all these singular points (penups and maxima) are joined using a cubic spline interpolation algorithm. Once this initial p waveform is generated, it is processed in order to avoid undesired effects:

- Many online signature acquisition devices consider 1024 integer pressure levels, so each point of the synthetic p function is rounded to the nearest integer value, and those which exceed 1024 are set to this maximum value. The same way, those points lower than 0 are set to the penup value.

- A signature pressure signal cannot start or end with a penup. If this is the case the function is artificially changed so that the starting and ending points are non-zero elements.

- Due to the biomechanical properties of the human writing movements, penups cannot be shorter than a certain number of points (around 15 for a 100 Hz sampling rate). The pressure function is accordingly modified in order to avoid unrealistic penups.

4.3.1.3. Signature Refinement in the Time Domain

Several actions are undertaken at this point to give the signature a more realistic appearance:

- Both trajectory functions are smoothed using a 10-point moving average in order to avoid possible high frequency noise.

- The x function of most left-to-right written signatures presents a general growing tendency fluctuating around a straight of fixed slope (see x function of the first real signature in Fig. 4.14). This behaviour is artificially produced in this step of the algorithm.

- In many cases, real signatures present a big fluctuation of their values at the end of the x and y signals, which in most cases can be identified with a round-like flourish (see x and y functions of the first real signature in Fig. 4.14). This final waveform is also artificially added to some signatures in this part of the algorithm.

- Additionally, translation, rotation and scaling transformations can be applied at this point if considered necessary.

4.3.2. Generation of Duplicated Samples

Lets consider the signing process as follows. A clean dynamic signature $[x(t), y(t), p(t)]$, unique for each subject, is transmitted through an unknown channel h where it is distorted, in this way generating the various genuine impressions corresponding to the natural variability of the subject at hand (see Fig. 4.13). Under this framework, the generation of multiple samples from a given clean signature is straightforward given by the distortion parameters.

In the present work we consider three different stages to model the distortions introduced by the channel h in the signature time signals: i) noise addition according to a particular Signal to Noise Ratio (SNR), ii) resampling/downsampling of the original signal by a factor M, and iii) amplification/attenuation of the signal in terms of a parameter α. Next we describe each of the three distortion stages.

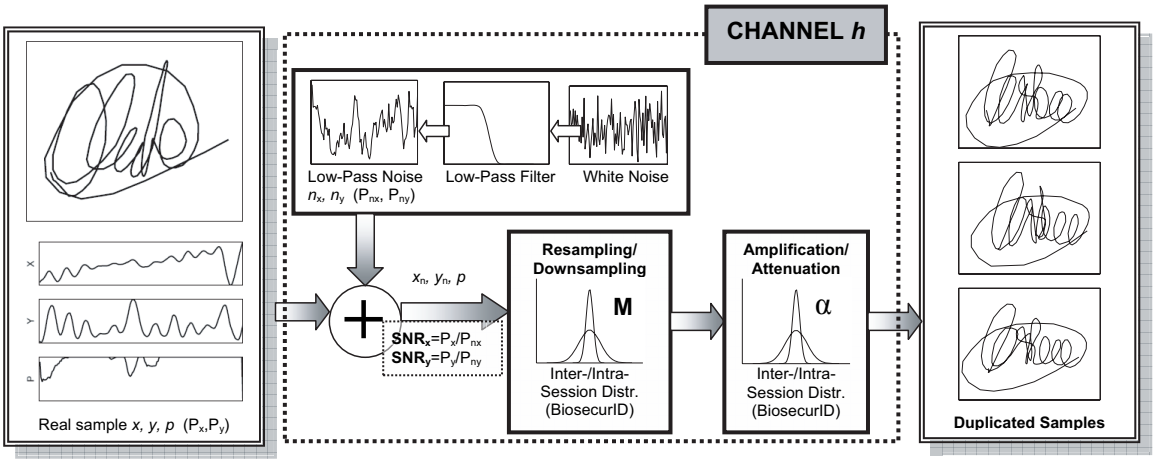


Figure 4.13: *General architecture of the algorithm for generating duplicated samples.*

- **Noise addition** (SNR). Low-pass noise n_x and n_y is added to the trajectory functions x and y so that the resulting signals x_n and y_n present a particular SNR_x and SNR_y (defined as the quotient between the function's power P_x, and the noise power P_{nx}, i.e., $\text{SNR}_x = P_x/P_{nx}$). The SNR should vary depending on whether we want to generate samples from the same or from different sessions (intra- and inter-session SNRs, respectively). In our experiments we assume that the noise is uncorrelated with the signature signals.

  In this step of the algorithm no distortion is introduced in the pressure (p) signal which remains unaltered.

- **Resampling/Downsampling** (M). This is equivalent to a duration expansion or contraction of the signals (the same length increase or decrease is applied to all three functions). Considering T as the duration of a signature (the same for the trajectory and pressure signals), the duration of the contracted/expanded new signature is computed as: $T_M = (1 + M)T$.

  The value of the resampling/downsampling factor M is taken from a different uniform distribution depending on whether we want to produce intrasession ($M \in [-M^{\text{intra}}, M^{\text{intra}}]$) or intersession ($M \in [-M^{\text{inter}}, M^{\text{inter}}]$) variability, being in general $|M^{\text{intra}}| < |M^{\text{inter}}|$.

- **Amplification/Attenuation** (α). An affine scaling is finally applied to all three signals according to a parameter α (which varies for each time function) [Munich and Perona, 2003]. Analogously to the resampling parameter M, the amplification factor α follows a uniform distribution between $[-\alpha_x^{\text{intra}}, -\alpha_x^{\text{intra}}]$ for intrasession samples, and between $[-\alpha_x^{\text{inter}}, -\alpha_x^{\text{inter}}]$ for intersession samples (similarly for functions y and p). For a given value of the parameter α_x, the scaled function x_α is computed as $x_\alpha = (1 + \alpha_x)x$.

4.3.3. Validation Experimental Framework

The validation experiments are carried out using two independent databases as development and test sets. The efficiency of the algorithm is estimated both from a qualitative (visual appearance of the synthetic signatures), and quantitative point of view. For the quantitative validation, two different experiments are carried out, one comparing the information present in the synthetic and real signatures using global parameters, and the other comparing the performance of both real and synthetic samples on an automatic signature recognition system.

4.3.3.1. Database

In order to avoid biased results, two totally different datasets were used as development (to estimate the generation model parameters) and test sets (where results on the efficiency of the algorithm are obtained).

For the estimation of the algorithm parameters (N, N_R, G, and PU for the generation of synthetic individuals, and SNR, M, and α for the generation of multiple samples) we used part of the signature data in the BiosecurID multimodal database [Fierrez *et al.*, 2009]. BiosecurID, which was introduced in Chapter 3, comprises eight different biometric traits of 400 users and was captured in four acquisition sessions over a six month time span (which makes it a very efficient tool to estimate the inter and intrasession variability). The signature subset comprises for each user, 16 original samples (four samples per session), and 12 forgeries carried out with an increasing degree of skill over the sessions (both the off-line and on-line information of each signature is available). In the present work, the imitations were discarded and only the $400 \times 16 = 6,400$ genuine dynamic signatures were used as development set. The values obtained on this dataset for each of the parameters defining our generation model of synthetic individuals were:

- Parameter N. It follows the length distribution of the development set.
- Parameter N_R. The values that define the uniform distribution from which this parameter is extracted are, $[\delta^{\min}, \delta^{\max}] = [0.15, 0.26]$, with $N_R = \delta N$.
- Parameter G. The ratio between the power of the relevant and non relevant coefficients follows a uniform distribution defined by $G^{\min} = 8$ and $G^{\min} = 19$.
- Parameter PU. It follows the penups distribution of the development set according to the signature length N (i.e., longer signatures present a higher probability of having a bigger number of penups.)

The values of the parameters defining the duplicated samples generation model, obtained on the development dataset were:

- Parameter SNR. Based on the assumption of uncorrelated signature signals and noise, we estimate the SNR averaging the noise (computed between pairs of genuine signatures

avoiding repetitions) across users. Thus, the global SNR of signal x of a specific user ($\mathrm{SNR}_x^{\mathrm{U}}$) is estimated as:

$$\mathrm{SNR}_x^{\mathrm{U}} = \frac{1}{\mathrm{C}(N_{gs},2)} \sum_{k=1}^{N_{gs}} \frac{P_x^i}{|P_x^i - P_x^j|} \quad \text{for} \quad j > i,$$

where N_{gs} represents the number of considered genuine signatures from the user, and $\mathrm{C}(N_{gs},2)$ is the number of possible combinations of the N_{gs} signatures taken in pairs: $\mathrm{C}(N_{gs},2) = N_{gs}!/2!(N_{gs}-2)!$.

The final SNR_x distribution is estimated using the 400 $\mathrm{SNR}_x^{\mathrm{U}}$ measures obtained from BiosecurID.

Parameter SNR_y is computed similarly, being in both cases the genuine pairs of signatures (N_{gs}) either from the same or different acquisition sessions (intra-session and inter-session SNR models, respectively).

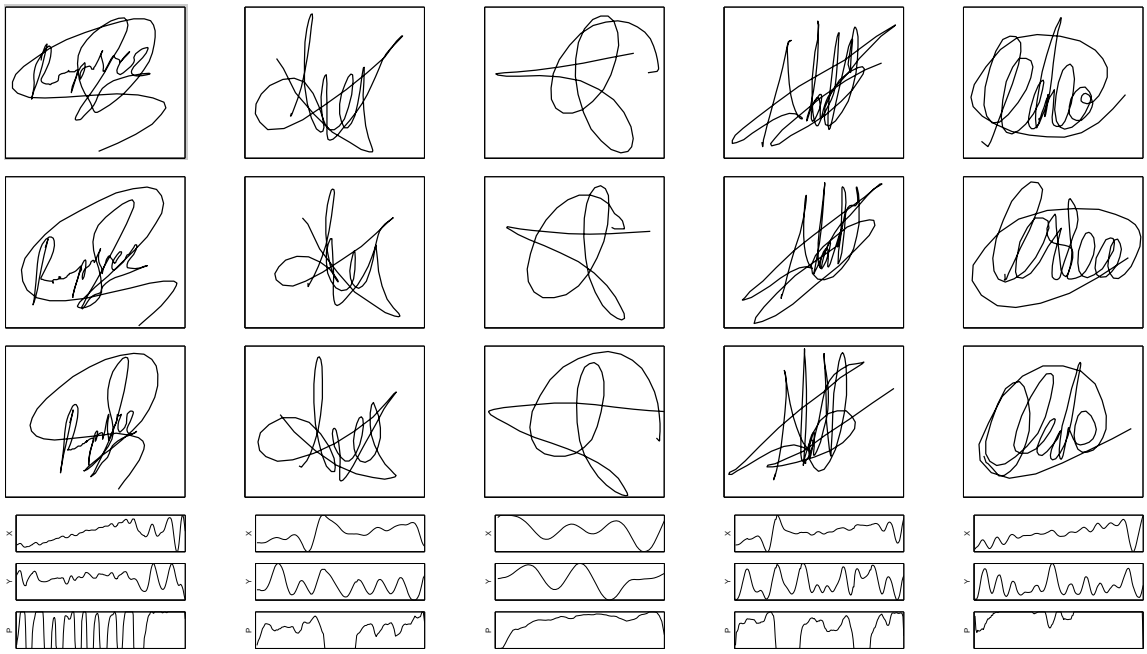
The results show that the power of the noise added in the x coordinate to produce intersession samples P_{nx}^{inter} has to be around 8% higher than in the case of intrasession repetitions P_{ny}^{intra} (i.e., $P_{nx}^{\mathrm{inter}} = 1.08 P_{nx}^{\mathrm{intra}}$). In the case of the noise affecting the y coordinate function, the variability between samples captured in the same and different sessions is slightly higher: $P_{ny}^{\mathrm{inter}} = 1.11 P_{ny}^{\mathrm{intra}}$.

- Parameter M. The value of the intrasession duration variability found in the development set is defined by $M^{intra} = 0.1$, while the intersession variability follows a uniform distribution characterized by $M^{\mathrm{inter}} = 0.14$.

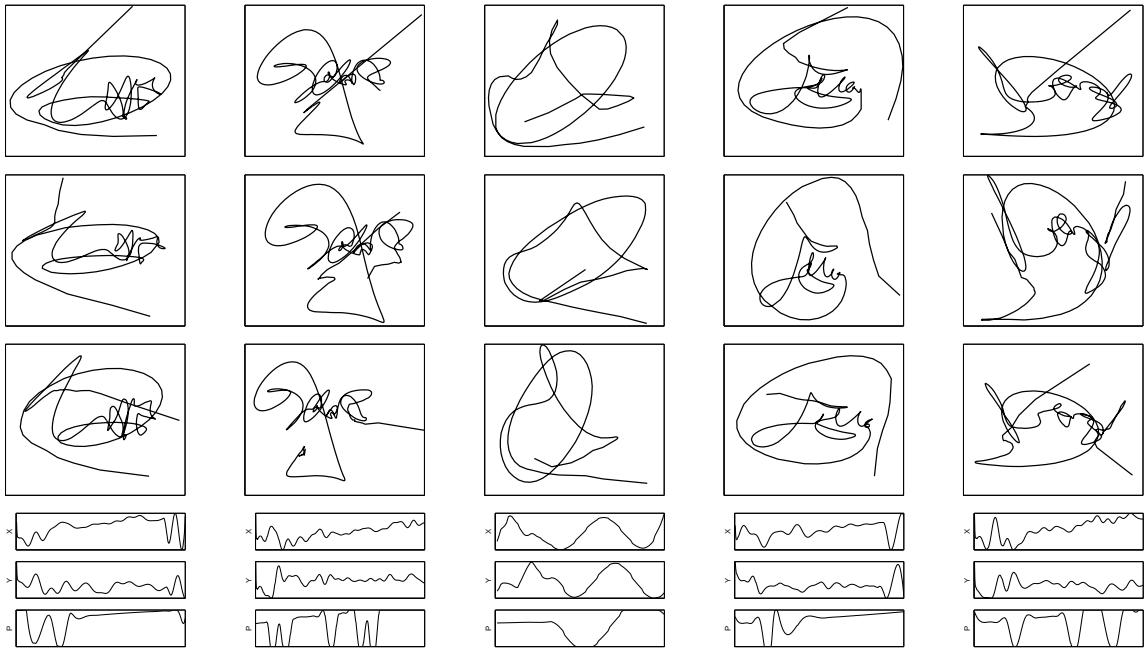
- Parameter α. The values that define the uniform distributions from which this parameter is extracted are (for the three time functions x, y, and p):
  $[\alpha_x^{\mathrm{intra}}, \alpha_x^{\mathrm{inter}}] = [0.06, 0.08]$,
  $[\alpha_y^{\mathrm{intra}}, \alpha_y^{\mathrm{inter}}] = [0.08, 0.11]$,
  $[\alpha_p^{\mathrm{intra}}, \alpha_p^{\mathrm{inter}}] = [0.05, 0.06]$.

As test set, the dynamic signature data of the MCYT database (comprising signature and fingerprint information of 330 users) was used [Ortega-Garcia *et al.*, 2003]. The signature dataset (presented in Chapter 3) is formed by 25 original samples and 25 skilled forgeries per user (captured in five different acquisition sets). These data are used in the two validation experiments described in Sect. 4.3.3.2.

In Fig. 4.14 three samples of five real (top) and synthetic (bottom) signers are shown. The real signers were taken from the test set (MCYT database), and the synthetic subjects were produced using the proposed generation method with the parameter values estimated from the development set (BiosecurID database). The trajectory and pressure signals of the first sample appear below. We can observe that, although no recognizable characters can be distinguished in the synthetic signatures, their aspect and that of their time functions is quite similar to the real signatures appearance.



Real signatures extracted from the MCYT database.



Synthetic signatures produced with the described model-based generation algorithm.

Figure 4.14: *Examples of real (top) and synthetic (bottom) signatures. Three samples of 5 different real and synthetic signers are shown together with the time sequences $x[n]$, $y[n]$, and $p[n]$ corresponding to the first sample.*

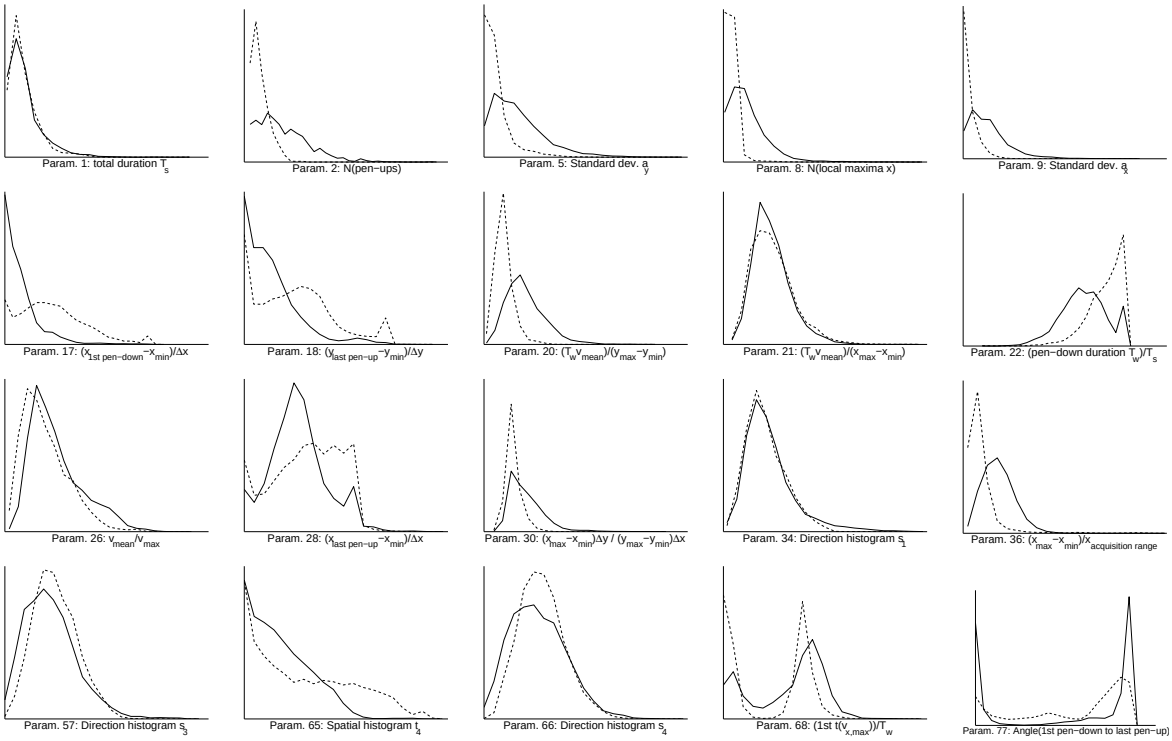


Figure 4.15: *Histograms of real (solid lines) and synthetic (dashed lines) signatures, corresponding to the best performing 20-parameter set found by Galbally et al. [2008b] for signature verification. The parameter numeration followed by Fierrez-Aguilar et al. [2005b] is used, where a complete set of 100 parameters from which the best 20 were selected was introduced and discussed.*

4.3.3.2. Results

In addition to the observable similarity between the real and synthetic signatures appearance (patent in Fig. 4.14), two other experiments have been carried out in order to assess the suitability of the proposed synthetic signature generation algorithm. For that purpose a database (following the MCYT structure) of 330 synthetic signers and 25 samples per signer was generated (from now on the SSiGGeDB). The first 5 samples of each signature were generated according to the intrasession variability present in real signatures, while the remaining 20 present a higher variance in order to imitate samples acquired in different sessions.

Validation Experiment 1: Global Features Comparison

As a first approximation to evaluate the goodness of the synthetic generation algorithm, we studied to what extent the synthetic signatures in SSiGGeDB are similar to the real signatures in MCYT according to a set of discriminative features. For that purpose, the comprehensive set of 100 global features described by Fierrez-Aguilar *et al.* [2005b] was extracted from each signature in MCYT and in SSiGGeDB, which comprises many of the features of the most popular works on feature-based signature verification [Fierrez and Ortega-Garcia, 2008]. From that 100-feature set we selected the best performing 20-parameter subset in a signature verification task

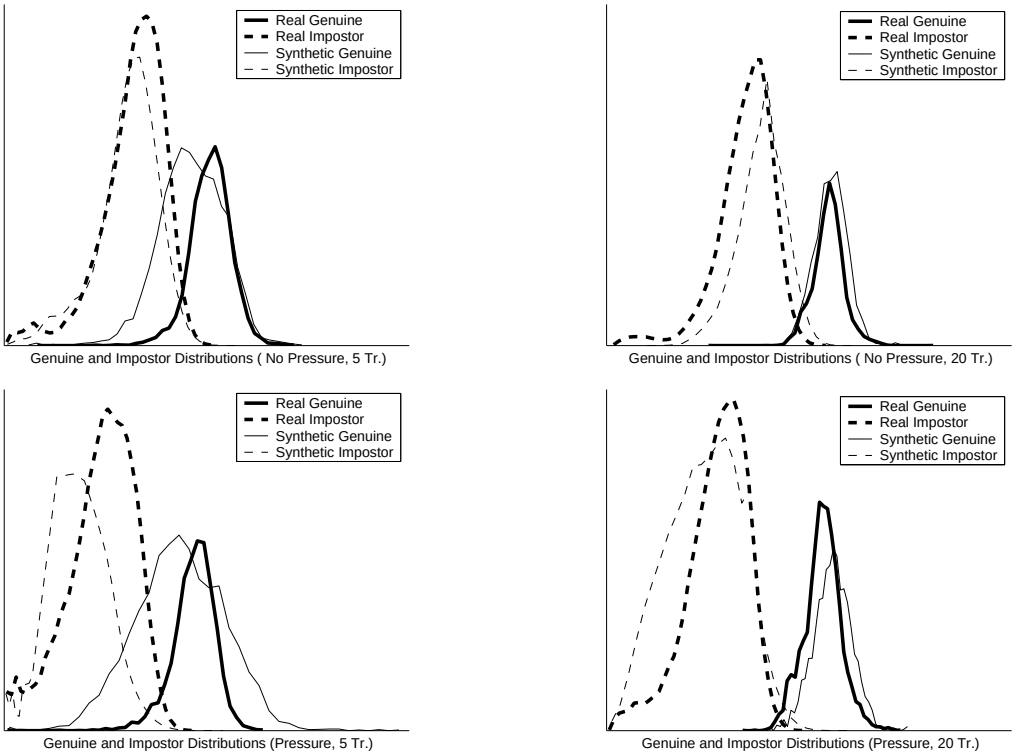


Figure 4.16: *Score distributions of real and synthetic signatures for the different scenarios considered: with and without taking into account the pressure information and for 5 and 20 training signatures.*

(using the SFFS feature selection algorithm) [Galbally *et al.*, 2008b]. The resulting individual distributions of real and synthetic signatures are shown in Fig. 4.15, where we can observe the clear similarity between them, being in some cases (parameters 1, 21, 26, 34, and 57) practically identical.

From this result we can conclude that the most discriminant features (for verification purposes) that characterize the signature trait, are present in a very similar manner both in the real and synthetic signatures generated according to the proposed algorithm.

Validation Experiment 2: Evaluation on a Recognition System

The performance of the synthetic signatures has been also evaluated using an HMM-based signature recognition system [Fierrez *et al.*, 2007a]. A 12-state and 4-mixture HMM configuration was used, with no user-dependent or score-dependent normalization of the scores. For both performance evaluations (using real and synthetic signatures) four different scenarios were considered in order to see if the behaviour of the synthetic signatures is comparable to those of the real samples, and thus can be used in the evaluation of signature verification systems:

- Number of training signatures: the performance of the system was evaluated using either 5 or 20 training signatures to compute the model of each user.

	EER (%)			
	No Pressure		Pressure	
	5 Tr.	20 Tr.	5 Tr.	20 Tr.
Real	4.63	1.24	3.74	0.47
Synthetic	10.41	4.17	5.83	2.03

Table 4.5: *Performance comparison on an HMM-based signature verification system on real and synthetic signatures. 5 Tr. and 20 Tr. indicate the number of training signatures used.*

- Pressure information: the system was evaluated with and without considering the pressure information of the signatures. The scenario with no pressure information was taken into account as not all the on-line signature acquisition devices capture this information.

In all cases the data corpus was divided into training and test sets, where the training set comprises either 5 or 20 signatures and the test set consists of the remaining samples (this way either 330×20 or 330×5 genuine scores are produced). In order to compute the impostor scores, the trained model of each user is compared with one signature (chosen randomly) of the remaining users, thus resulting in 330×329 impostor scores.

The genuine and impostor sets of scores were computed both for real (MCYT) and synthetic signatures (SSiGGeDB), for the different scenarios considered: with and without taking into account the pressure information, and for 5 and 20 training signatures. The score distributions for all these sets of scores are shown in Fig. 4.16, where we can observe that, specially for the scenarios with 5 training signatures, the genuine score distribution of synthetic signatures (solid thin line) presents a bigger dispersion than that of the real signatures (solid thick line).

With those sets of scores, the EER of the system was computed and the results are shown in Table 4.5. Several observations can be made: *i*) the system performance on real signatures is better than with synthetic individuals, representing the latter ones a reasonable upper bound of the real performance, *ii*) in both cases (real and synthetic) there is a similar decrease in the EER when the number of training signatures increases from 5 to 20, and *iii*) for both type of signatures the inclusion of the pressure information improves the EER in a similar way.

From the two reported validation experiments we can infer that the discriminative information present in the synthetic signatures and in the real signatures, does not vary significantly. This fact makes the presented algorithm suitable to be used for the performance evaluation of automatic signature verification systems.

4.4. Chapter Summary and Conclusions

In this chapter we have introduced three novel algorithmic methods which will be used in the security evaluations described in the experimental part of the Dissertation. The presented algorithms include a hill-climbing attack based on Bayesian adaptation which can be applied in

a straight forward manner to different matchers and biometric traits, a software-based liveness detection method using quality measures for fingerprint recognition systems, and a complete scheme for the generation of totally synthetic on-line signatures (both synthetic individuals and duplicated samples). All the three methods were validated on significant databases following systematic and replicable protocols, reaching remarkable results.

Regarding the Bayesian-based hill-climbing attack, it has been successfully used to attack an on-line signature and two face verification systems, thus proving its ability to adapt to different matchers working with fixed length feature vectors and returning real similarity scores. The details and results of these vulnerability evaluations are given in Chapters 6 and 7 respectively.

The novel fingerprint parameterization for liveness detection based on quality measures has been tested on the development set of the recent LivDET competition LivDet [2009]. This challenging database comprises over 4,500 real and fake fingerprint images (generated with different synthetic materials), acquired with three optical sensors. The novel approach has proven to be robust to the multi-sensor scenario, correctly classifying (real or fake) over 93% of the fingerprint images.

The proposed approach is part of the software-based solutions as it distinguishes between images produced by real and fake fingers based only on the acquired sample, and not on other physiological measures (e.g., odor, heartbeat, skin impedance) captured by special hardware devices added to the sensor (i.e., hardware-based solutions that increase the cost of the sensors, and are more intrusive to the user). Unlike previously presented methods, the proposed technique classifies each image in terms of features extracted from just that image, and not from different samples of the fingerprint. This way the acquisition process is faster and more convenient to the final user who does not need to keep his finger on the sensor for a few seconds, or place it several times.

Liveness detection solutions such as the one presented in this Chapter are of great importance in the biometric field as they help to prevent direct attacks (i.e., those carried out with synthetic traits which makes them very difficult to be detected), thus enhancing the level of security offered to the user. The proposed approach is used in Chapter 5 as countermeasure against the different direct attacks considered in the fingerprint security evaluation with results that improve those reached in the validation experiments.

The proposed new algorithm to generate synthetic handwritten signatures based on the spectral analysis of the signature trajectory functions presents the clear advantage over previously reported methods of not needing any real samples to generate new synthetic individuals. The reported validation results show that the synthetically generated signatures, in addition to presenting a very realistic appearance, possess very similar characteristics to those that enable the recognition of real signatures. The proposed algorithm can be used as an efficient tool for the evaluation of automatic signature verification systems, as it can rapidly and easily generate large amounts of realistic data (instead of the costly and time-consuming real biometric databases).

In addition to evaluation tasks, the proposed synthetic generation method can also be useful as a development tool in other biometric applications where the data scarcity is a key issue. In

particular it can be used to:

- Carry out vulnerability assessment studies against attacks that need many real samples to be successful (e.g., brute-force attacks).
- Generate multiple samples of given users in order to overcome the shortage of data in verification and identification enrollment.
- Generate data from multiple signers for signature recognition approaches using data-driven machine learning, where large amounts of data to train the classifier are needed.
- Study in depth the nature, properties and limitations of the signature signal in order to identify individuals (e.g., individuality studies), to increase the robustness of the current recognition systems, or to obtain more robust signatures against forgeries.

In particular, in Chapter 6 the proposed generation method will be analyzed as a threat to on-line signature verification systems (carrying out a brute-force attack with synthetic signatures), and as a way to improve the performance of those same systems by increasing the amount of enrollment data, thus minimizing the effects of the studied attack.

Novel contributions of this chapter are the matcher-independent hill-climbing attack algorithm based on Bayesian adaptation, the quality-based parameterization used for liveness detection, and the generation algorithm of synthetic individuals based on the spectral information of on-line signatures.

Chapter 5

Security Evaluation of Fingerprint-Based Authentication Systems

This chapter studies the vulnerabilities of fingerprint-based recognition systems to direct and indirect attacks, and different approaches to countermeasure these security threats are evaluated.

As indicated in Chapter 2, the security threats of a biometric system can be broadly divided into *direct* [Galbally *et al.*, 2006] and *indirect attacks* [Uludag and Jain, 2004], being the first those carried out using a fake biometric trait, and the latter those directed to some of the system inner modules. The main difference between the two attack categories is that in the direct approach no information about the internal functioning of the system is needed, the only requisite is to have access to the sensor. Thus, it would be desirable for a potential attacker to be able to transform an indirect attack into a direct one as the requirements to carry it out would be largely simplified.

The order in which the attacks are analyzed in the Chapter has been selected on the basis of the amount of information about the system needed by the attacker to execute them: we start with a direct attack starting from latent fingerprints where no special information about the system is required, we continue with a direct attack where we need access to the user template, and we conclude with a hill-climbing indirect attack that requires to know the template format, and access to the input of the matcher and to the score returned by the system.

As already commented above, two type of direct attacks are evaluated in this chapter: those starting from a latent fingerprint, which had already been considered in the literature [Matsumoto *et al.*, 2002; Van der Putte and Keuning, 2000], and those performed with gummy fingers generated from standard ISO minutiae templates, which had never been carried out before and that present the ability to convert an indirect attack carried out with fingerprint images to a direct attack executed with fake fingers. The study includes some interesting findings

regarding the relation between the quality of the images used in the attacks and the success rate (SR) reached by them. The novel liveness detection approach based on quality measures presented in Sect. 4.2, is used to countermeasure these attacks and its efficiency to reduce the risks arisen from them is evaluated.

An evaluation of the robustness of fingerprint recognition systems to a hill-climbing algorithm (indirect attack to the input of the matcher) is also performed. We study the impact in the final success rate of the attack of different algorithm parameters, and score quantization is proposed and evaluated as a way to countermeasure this type of security breach.

The chapter is structured as follows. One section is dedicated to each of the three different vulnerability evaluations: *i*) direct attacks performed with gummy fingers generated from latent fingerprints (Sect. 5.1), *ii*) direct attacks starting from standard ISO templates (Sect. 5.2), and *iii*) indirect attacks following a hill-climbing approach (Sect. 5.3). Each of these sections share a common structure where the attacking method is first described, then the recognition systems being evaluated are presented, followed by the database and experimental protocol, and finally the results of the evaluation are given and analyzed. In the last section of the chapter we present different countermeasures for the studied attacks (Sect. 5.4). Finally, the chapter summary and conclusions are given in Sect. 5.5.

This chapter is based on the publications: Galbally *et al.* [2009a,b, 2008a, 2006]; Martinez-Diaz *et al.* [2006].

5.1. Direct Attacks Starting from a Latent Fingerprint

We will perform a systematic and replicable evaluation of the vulnerabilities of two fingerprint-based recognition systems to direct attacks carried out with gummy fingers generated from latent fingerprints. The minutiae-based NFIS2 system by the American NIST (which is a *de facto* standard reference system used in many fingerprint-related research contributions), and a proprietary ridge-based system are used in the experiments. Fingerprint recognition systems using ridge pattern information present, in general, a lower performance under normal operation conditions than those working on minutiae, and are usually used to complement the latter. However, in this case we consider both technologies separately in order to give insight and understanding of their behaviour and vulnerabilities in different attacking scenarios.

For this evaluation two general attack scenarios have been considered, namely: *i*) with a cooperative user, and *ii*) without the cooperation of the user. A database of real and fake fingerprints was specifically created for each of these two scenarios, using three different sensors each belonging to one of the main technologies existing in the market: two flat (optical and capacitive), and one sweep sensor (thermal). The two different fingerprint recognition systems are tested on these two databases and we present the results considering the normal operation mode (i.e., enrollment and test are carried out with real fingerprints) as reference, and two different attacks, namely: *i*) enrollment and test are performed with fake fingerprints (attack 1), and *ii*) enrollment is carried out with real fingerprints while the test is done with the corresponding

fake imitations (attack 2).

Previous related works have already studied direct attacks to fingerprint verification systems [Matsumoto *et al.*, 2002; Thalheim and Krissler, 2002; Van der Putte and Keuning, 2000], but usually with very limited datasets, thus resulting in statistically insignificant results. The contributions of the present work over previous approaches, which are mainly our vulnerability assessment methodology and various experimental findings, are based on a large set of data from diverse subjects and acquisition conditions. In particular, we show a strong correlation between the image quality of fake fingerprints and the robustness against direct attacks of the fingerprint verification systems. The results reported are therefore relevant to devise proper countermeasures against the considered attacks depending on the system at hand.

5.1.1. Generation Process of the Gummy Fingers

For each of the attack scenarios considered, with and without cooperation of the user, a database of real and fake fingers was created for the experiments. The generation process of the gummy imitations differs for each of the two scenarios:

- **With cooperation**. In this context the legitimate user is asked to place his finger on a moldable and stable material in order to obtain the negative of the fingerprint. In a posterior step the gummy finger is recovered from the negative mold using modeling silicone. The different steps of the whole generation process are depicted and described in Fig. 5.1.

- **Without cooperation**. In this case we recover a latent fingerprint that the user has unnoticedly left behind (on a CD in our experiments). The latent fingerprint is lifted using a specialized fingerprint development toolkit and then digitalized with a scanner. The scanned image is then enhanced through image processing and finally printed on a PCB (negative of the fingerprint) from which the gummy finger is generated. The main steps of this non-cooperative process, first introduced by Van der Putte and Keuning [2000], are depicted in Fig. 5.2.

5.1.2. Fingerprint Verification Systems

Two different fingerprint verification systems, one minutiae-based and one ridge-based, are used in the experiments:

- The minutiae-based NIST Fingerprint Image Software 2 (NFIS2) [Garris *et al.*, 2004]. It is a PC-based fingerprint processing and recognition system formed of independent software modules. The feature extractor generates a text file containing the location, orientation and quality of each minutia from the fingerprint. The matcher uses this file to generate the score. The matching algorithm is rotation and translation invariant since it computes only relative distances and orientations.

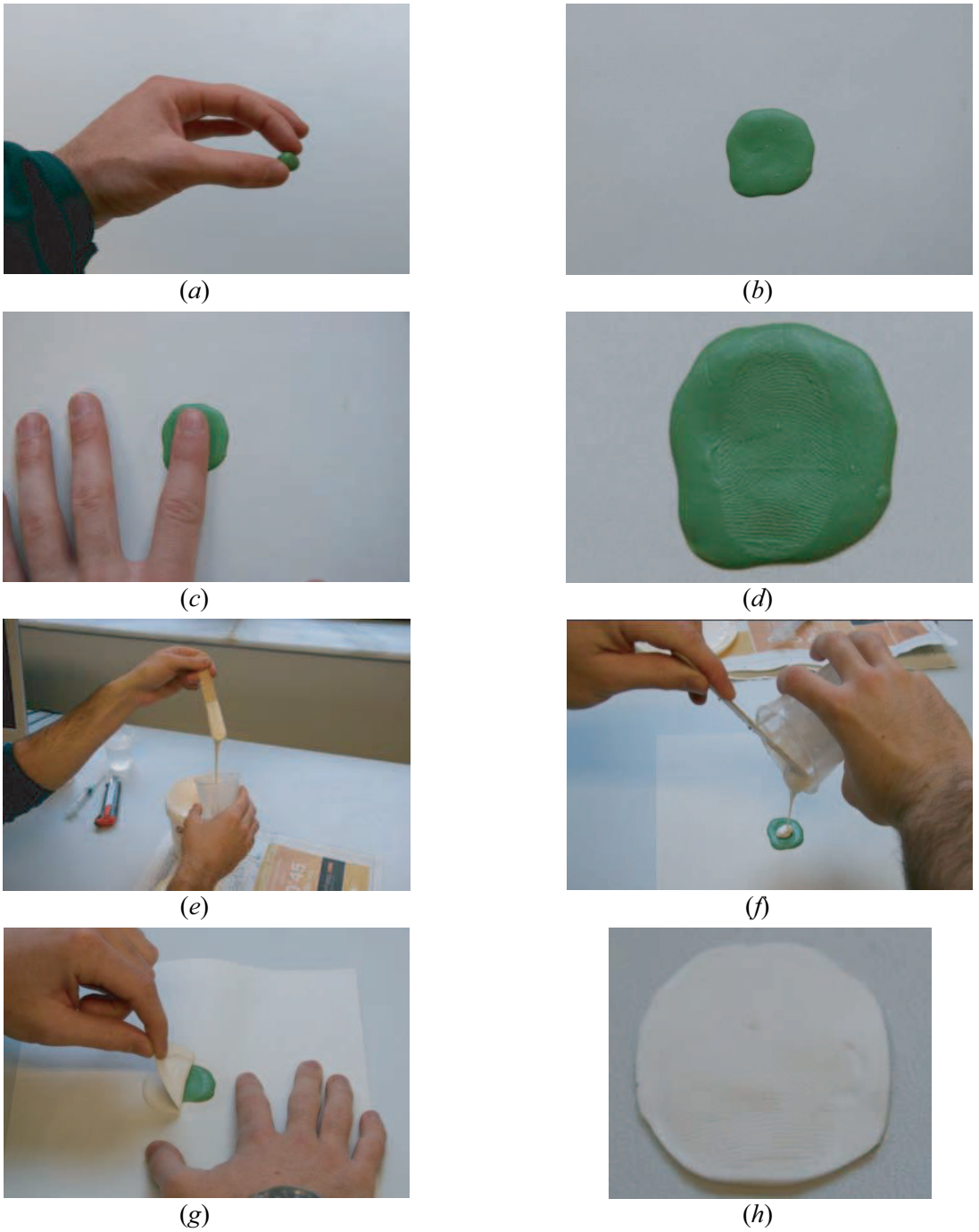


Figure 5.1: *Process followed to generate fake fingerprints with the cooperation of the user: select the amount of moldable material (a), spread it on a piece of paper (b), place the finger on it and press (c), negative of the fingerprint (d). Mix the silicone and the catalyst (e), pour it on the negative (f), wait for it to harden and lift it (g), fake fingerprint (h).*

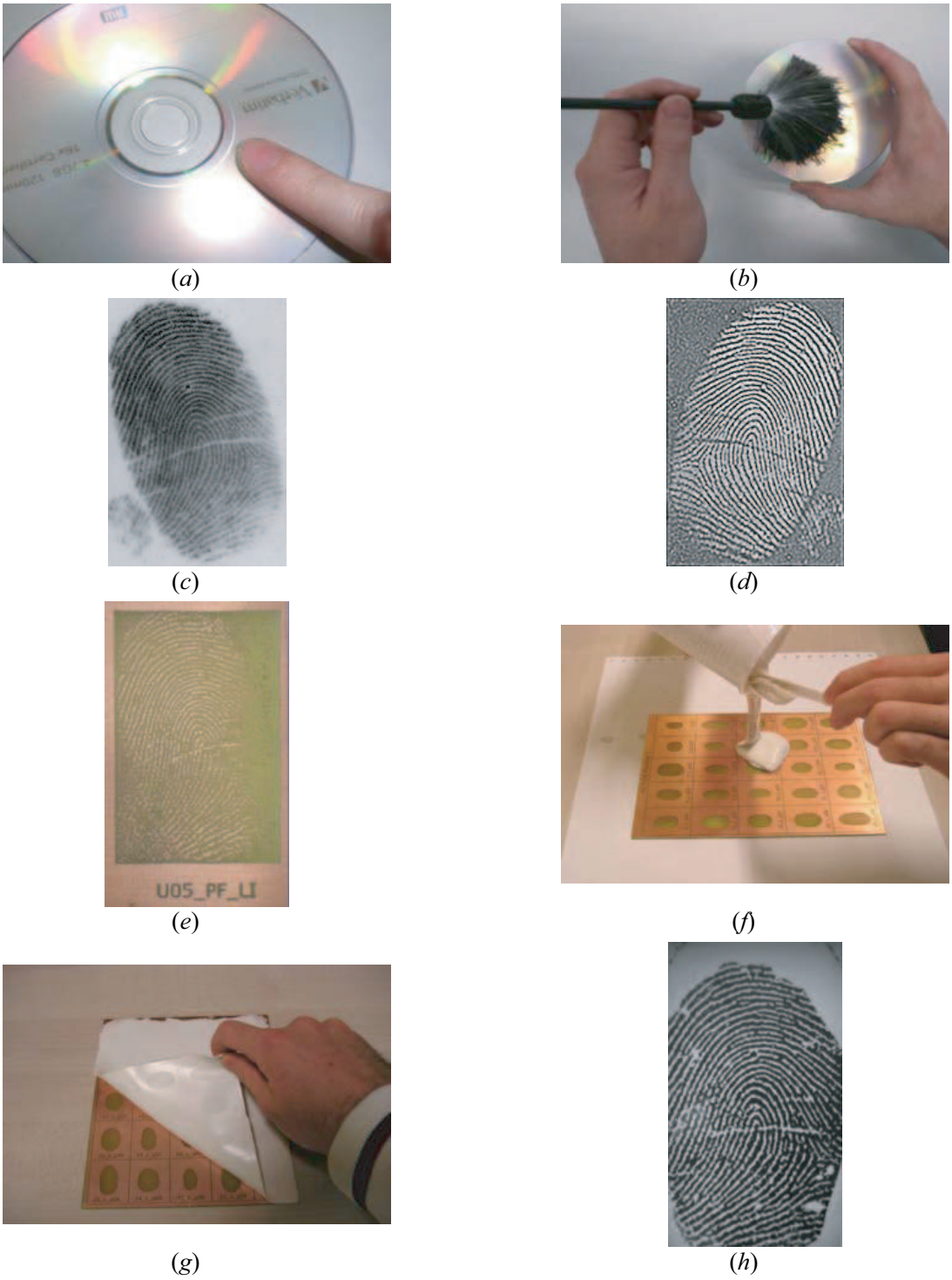


Figure 5.2: *Process followed to generate fake fingerprints without the cooperation of the user: latent fingerprint left on a CD (a), lift the latent fingerprint (b), scan the lifted fingerprint (c), enhance the scanned image (d), print fingerprint on PCB (e), pour the silicone and catalyst mixture on the PCB (f), wait for it to harden and lift it (g), fake fingerprint image acquired with the resulting gummy finger on an optical sensor (h).*

- A basic ridge-based fingerprint verification system [Fierrez-Aguilar *et al.*, 2006]. Most of the actual fingerprint verification systems are minutiae-based as this is the basis of the fingerprint comparison made by fingerprint examiners. However, although minutiae may carry most of the fingerprint discriminant information, under certain circumstances (e.g. bad quality images) the extraction of a reliable minutiae map could be quite challenging. In this cases the use of some complementary recognition system, for example based on the ridge pattern, can improve the global performance of the system [Fronthaler *et al.*, 2008]. The system tested in this work uses 8 Gabor filters (each rotated 27.5° with respect to the previous one) to capture the ridge pattern. The 8 resulting images are tesselated in a rectangular grid and the variance of the filter responses in each cell are used to generate the feature vector. No rotation alignment is applied to the input images so it is quite sensitive to fingerprint rotation. For more details we refer the reader to [Fierrez-Aguilar *et al.*, 2006].

5.1.3. Database and Experimental Protocol

Experiments are carried out on a database comprising the index and middle fingers of both hands of 17 users ($17 \times 4 = 68$ different fingers). For each real finger, two fake imitations were generated following each of the procedures explained before (i.e., with and without the user's cooperation). Four samples of each fingerprint (fake and real) were captured in one acquisition session with: *i*) flat optical sensor Biometrika Fx2000 (512 dpi), *ii*) sweeping thermal sensor by Yubee with Atmel's Fingerchip (500 dpi), and *iii*) flat capacitive sensor by Precise Biometrics model Precise 100 SC (500 dpi). Thus, the database comprises 68 fingers $\times 4$ samples $\times 3$ sensors $= 816$ real image samples and as many fake images for each scenario (with and without cooperation). In order to ensure inter- and intra-class variability, samples of the same finger were not captured consecutively, following the methodology for biometric database acquisition developed in the project BioSec [Fierrez *et al.*, 2007b]. As will be described in Sect. 5.1.4, the quality of the images was estimated using three quality measures (each of them taking into account different properties of the fingerprint). Some good and bad quality samples of the database are depicted in Figs. 5.3 and 5.4 respectively.

Two different attack scenarios are considered in the experiments and compared to the normal operation mode of the system:

- **Normal Operation Mode (NOM)**: both the enrollment and the test are carried out with real fingerprints. This is used as the reference scenario. In this context the FAR (False Acceptance Rate) of the system is defined as the number of times an impostor using his own finger gains access to the system as a genuine user, which can be understood as the robustness of the system against a zero-effort attack. The same way, the FRR (False Rejection Rate) denotes the number of times a genuine user is rejected by the system.

- **Attack 1**: both the enrollment and the test are carried out with fake fingerprints. In this case the attacker enrols to the system with the fake fingerprint of the genuine user and

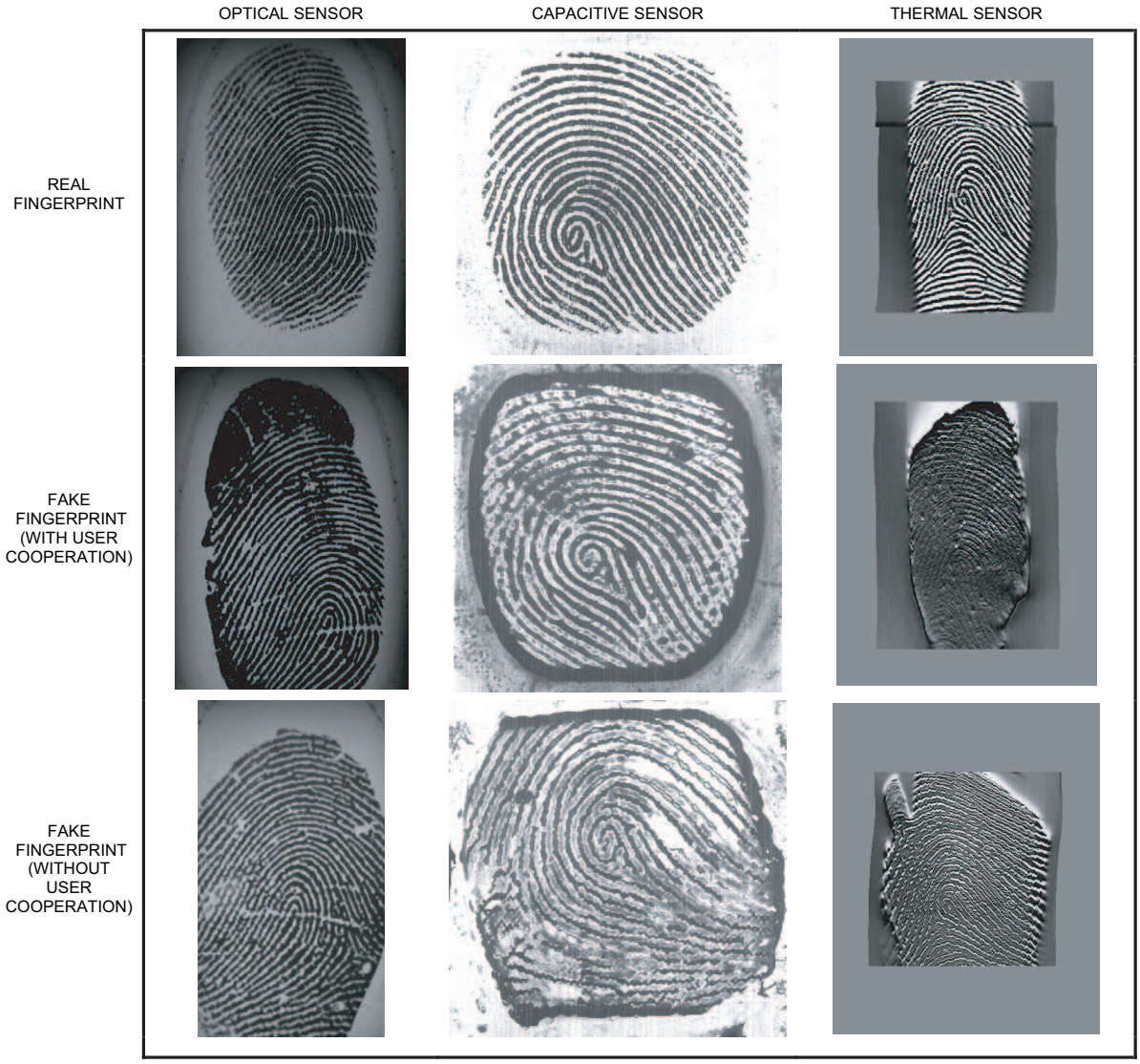


Figure 5.3: *Examples of good quality images of the database used in the direct attacks evaluation (available at http://atvs.ii.uam.es). Real images acquired with the optical, capacitive, and thermal sensor, are shown in the top row. Their respective fake images generated with cooperation are shown in the middle row, and without cooperation in the bottom row.*

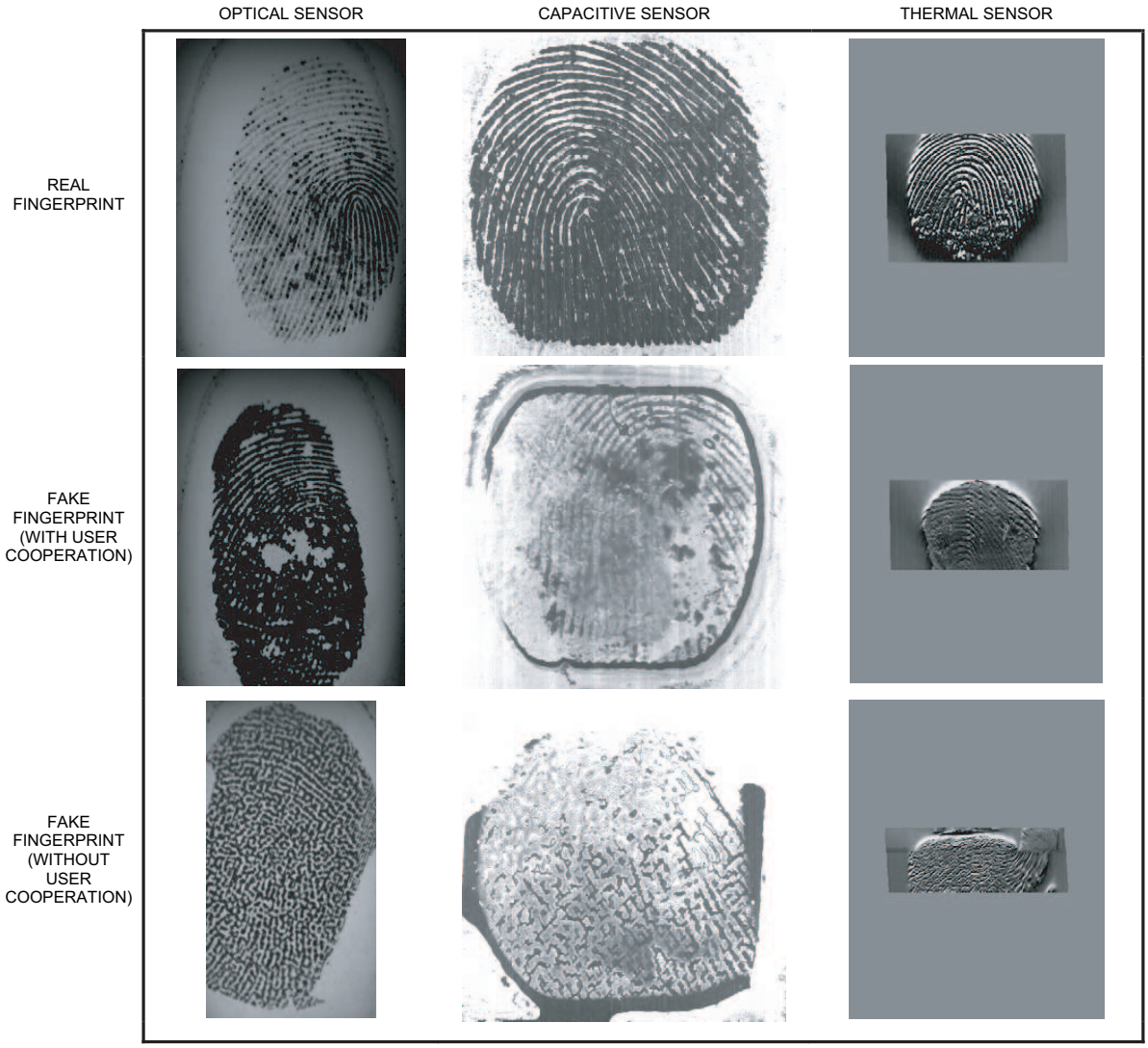


Figure 5.4: *Examples of bad quality images of the database used in the direct attacks evaluation (available at http://atvs.ii.uam.es). Real images acquired with the optical, capacitive, and thermal sensor, are shown in the top row. Their respective fake images generated with cooperation are shown in the middle row, and without cooperation in the bottom row.*

then tries to access the application with that same fake fingerprint. In this scenario an attack is unsuccessful (i.e., the system repels the attack) when an impostor enrols to the system using the gummy fingerprint of a genuine user, and subsequently he is not able to access the system using that same fake fingerprint. Thus, the Success Rate of the attack in this scenario can be computed as: SR = 1 − FNMR, where FNMR is the False Non-Match Rate.

In order to compute the performance of the system in the normal operation mode, the following sets of scores are generated: *i*) for genuine tests all the 4 real samples of each user are matched against each other avoiding symmetric matchings ($(4 \times 3)/2 = 6$ scores per user), which leads to $6 \times 68 = 408$ genuine scores, and *ii*) for impostor tests each of the four samples of every user are matched with all the samples of the remaining users in the database avoiding symmetric matchings, resulting in $(67 \times 4 \times 4 \times 68)/2 = 36,448$ impostor scores.

Similarly, in order to compute the FNMR in attack 1, all the 4 fake samples of each user are compared with each other avoiding symmetric matchings, resulting in a total 408 scores for each scenario (cooperative and non-cooperative).

- **Attack 2**: the enrollment is achieved using real fingerprints, and tests are carried out with fake fingerprints. In this case the genuine user enrolls with her fingerprint and the attacker tries to access the application with the corresponding gummy fingerprint. A successful attack is accomplished when the system confuses a fake fingerprint with its corresponding genuine fingerprint, i.e., SR = FMR where the FMR is the False Match Rate.

In this last scenario, only the impostor scores are computed matching all 4 original samples of each user with all 4 fake samples which results in $16 \times 68 = 1,088$ impostor scores for each scenario considered.

This experimental protocol was followed independently for the three sensors and the two kinds of fake fingerprints (cooperative and non-cooperative users).

In Fig. 5.5 the DET curves of the two evaluated systems are shown for all the three sensors used in the experiments. The top two rows correspond to attacks carried out with fake fingerprints generated with the cooperation of the user, and the bottom rows without his cooperation. These results will be furthered analyzed in Sect. 5.1.4.2 and Sect. 5.1.4.3.

5.1.4. Results

In addition to the evaluation of the attacks performance, we analyze the quality of the database samples comparing real and fake images. Then we study the success rates (SR) of the two attack scenarios compared to the performance at the normal operation mode, taking into account the quality-related findings reached in the quality analysis (see Sect. 3.2 for definition of SR).

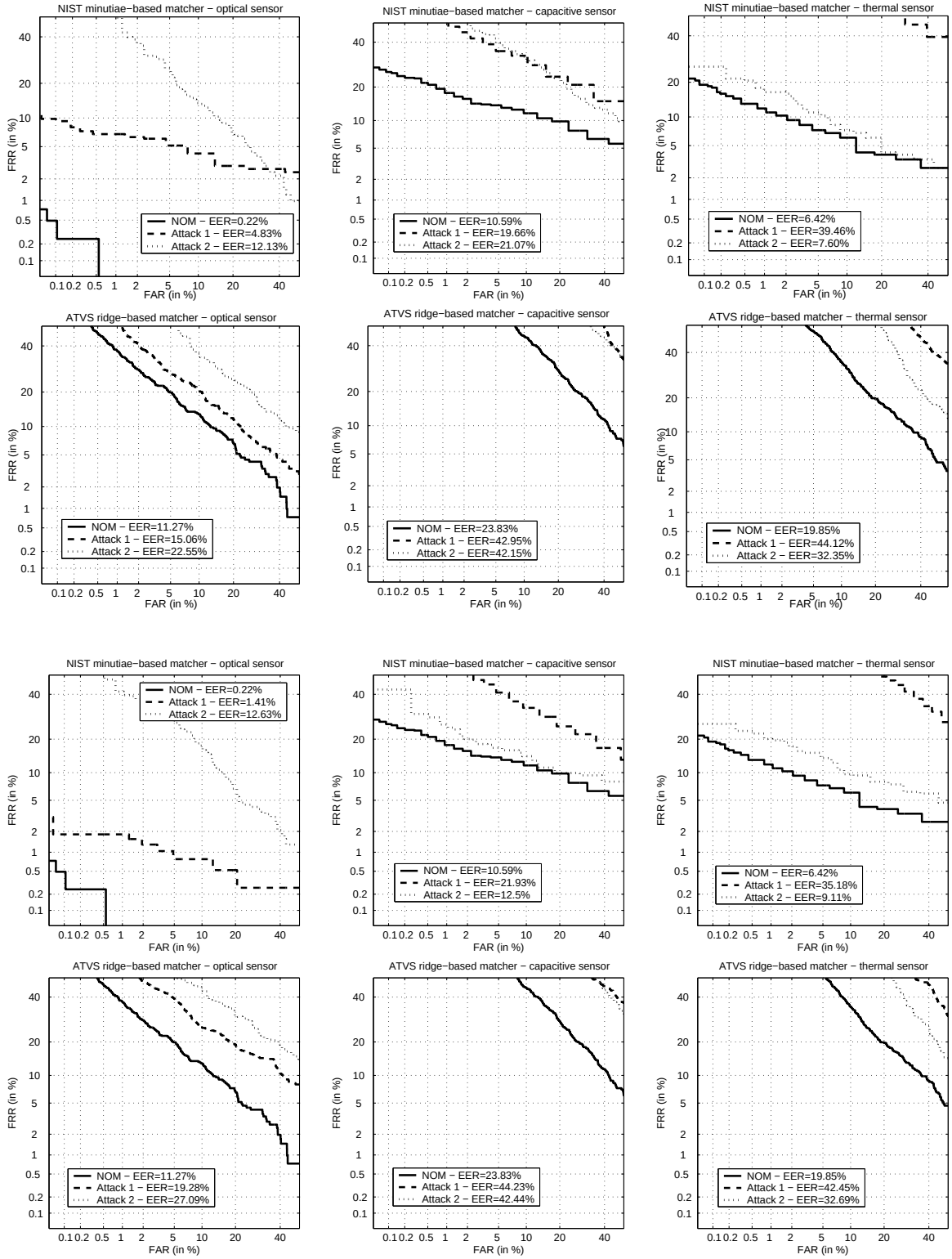


Figure 5.5: *DET curves of the minutiae- and ridge-based systems for the three sensors used in the experiments (left to right: optical, capacitive and thermal). The top two rows correspond to attacks with cooperative users and the bottom rows with non-cooperative users.*

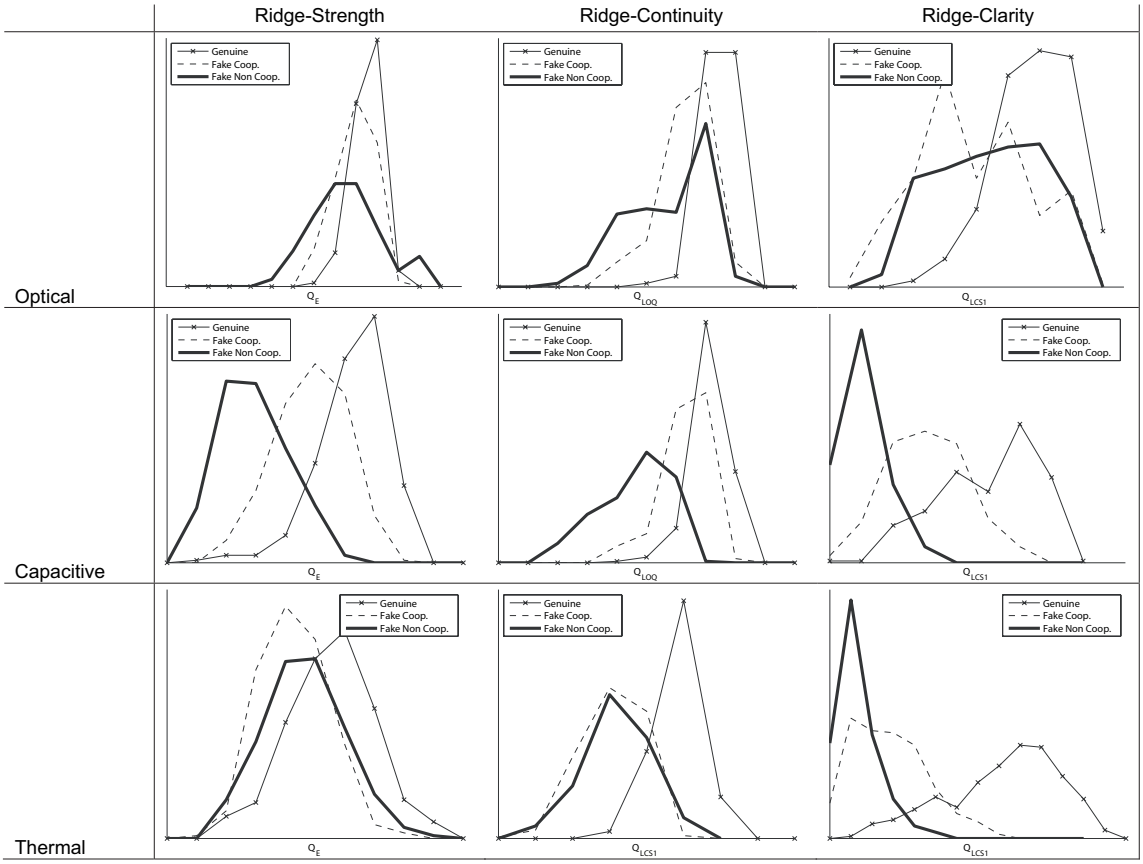


Figure 5.6: *Quality distributions (for the three measures considered) of the image databases (genuine, fake with cooperation, and fake without cooperation), captured with the optical sensor, capacitive sensor, and thermal sweeping sensor.*

5.1.4.1. Quality Analysis

Different quality measures were computed on the three datasets used in the evaluation (original, and fake with and without cooperation), for the three sensors used in the acquisition.

As explained in Sect. 4.2, image quality can be assessed by measuring one or more of the following properties [Alonso-Fernandez *et al.*, 2008]: ridge strength or directionality, ridge clarity, ridge continuity, integrity of the ridge-valley structure, and estimated verification performance when using the image at hand. Different quality measures (computing three of the previous fingerprint properties) have been implemented to estimate the quality of the images comprised in each of the datasets:

- **Ridge-strength measures**. Energy concentration in the power spectrum (Q_E) [Chen *et al.*, 2005a; Fierrez-Aguilar *et al.*, 2006]. It is computed using a set of bandpass filters in order to extract the energy in each frequency band.

- **Ridge-continuity measures**. Local Orientation Quality (Q_{LOQ}) [Chen *et al.*, 2004], which is computed as the average absolute difference of direction angle with the surround-

ing image blocks, providing information about how smoothly direction angle changes from block to block.

- **Ridge-clarity measures**. Local Clarity Score (Q_{LCS1}) [Chen *et al.*, 2004]. The sinusoidal-shaped wave that models ridges and valleys [Hong *et al.*, 1998] is used to segment ridge and valley regions. The clarity is then defined as the overlapping area of the gray level distributions of segmented ridges and valleys. The sinusoidal-shaped wave cannot be extracted reliably, specially in bad quality regions of the image.

In Fig. 5.6 we show, for each of the sensors and for the different quality measures considered, the quality distributions of the image databases used in the experiments. We can see that, as expected, the quality of the real samples (solid line) in all sensors is higher than that of the fake samples (dashed and thick solid lines). The quality of the fake images acquired with the optical sensor is acceptable (the distributions are close to that of the genuine images), while the fake images of the thermal and capacitive sensors are of a lower quality compared to that of the original images.

These differences in the fake fingerprints quality is due to the three technologies used. The optical sensor is based on refraction effects of the light which take place in a similar way both in the skin and in the silicone of the gummy fingers, which leads to good fake images. On the other hand, the thermal sensor measures the difference in temperature between ridges and valleys which is nonexistent in the silicone, so, although the gummy fingers were heated up before being placed on the sensor, the resulting images are of poor quality. Similarly, the capacitive sensor is based on electrical measures, thus the silicone fingers had to be damped with a conductive substance in order to acquire the samples, which lead to low quality images.

Although the non-cooperative process to generate gummy fingers takes more steps (where the original fingerprint information might be degraded) than the cooperative procedure, the quality of the final fake images between both fake generation procedures only decreases significantly when acquired with the capacitive sensor (both distributions are clearly separated). With the optical the quality is just slightly worse for the non-cooperative process, while in the thermal sensor non-cooperative samples present a quality level which is fully comparable to those generated with the cooperation of the user. These observations are consistent regardless of the property considered by the quality measures (ridge-strength, ridge-continuity, or ridge-clarity). As will be shown in the next sections, these quality-related findings have a strong influence in the performance of the attacks evaluated.

5.1.4.2. NFIS2 System Evaluation

In Table 5.1 (a) we show the Success Rate (SR) of the direct attacks against the NIST minutiae-based system at three different operating points. The decision threshold is fixed to reach a FAR = $\{0.1, 1, 10\}$ in the normal operation mode (NOM), and then the success rate of the two proposed attacks in analyzed in the two attack scenarios (with and without cooperation) for the three acquisition sensors.

	NOM		Attack 1		Attack 2	
	FAR (%)	FRR (%)	SR (%)		SR (%)	
			Coop	NoCoop	Coop	NoCoop
Optical	0.1	0.25	91	90	65	41
	1	0	93	94	69	49
	10	0	96	98	78	61
Capacitive	0.1	25	30	21	15	1
	1	16	44	39	24	2
	10	11	66	58	42	9
Thermal	0.1	18	7	35	0.5	0.5
	1	11	10	59	5	5
	10	6	45	78	15	22

(*a*) Performance of the attacks on the NIST minutiae-based system.

	NOM		Attack 1		Attack 2	
	FAR (%)	FRR (%)	SR (%)		SR (%)	
			Coop	NoCoop	Coop	NoCoop
Optical	0.1	61	55	13	1	0.5
	1	36	76	37	9	3
	10	13	94	74	37	27
Capacitive	0.1	96	38	42	4	8
	1	78	75	78	11	19
	10	35	87	92	40	57
Thermal	0.1	95	49	64	2	1
	1	82	86	92	11	8
	10	45	93	98	31	28

(*b*) Performance of the attacks on the ridge-based system.

Table 5.1: *Evaluation of the NIST and ridge-based systems to direct attacks with (Coop) and without (NoCoop) the cooperation of the user. NOM refers to the system Normal Operation Mode and SR to the Success Rate of the attack. Attack 1 and 2 correspond to the attacks defined in Sect. 5.1.3 (enrollment/test with fakes/fakes for attack 1, and genuine/fakes for attack 2).*

Attacks with cooperation

When the optical sensor is used, due to the good quality samples acquired, the SR increases to reach over 65% in all of the operating points considered for attack 2 (the intruder tries to access the system with the gummy finger of a correctly enrolled user). On the other hand, the fake images captured with the thermal sensor show very little discriminant capacity, which leads to a very similar performance of the system against random impostors (FAR in NOM) and the SR of attack 2 for all the operating points studied. When the capacitive sensor is used, the system shows more resistance to the attacks than with the optical sensor, but it is more vulnerable than when the thermal technology is deployed (as corresponds to the intermediate quality level of the fake samples captured). The same effect can be observed in attack 1: as the quality of the fake samples increases (from the thermal to the optical sensor) the system

becomes more vulnerable to the attacks.

Attacks without cooperation

In this scenario the samples captured with the thermal sensor present a higher quality than those acquired with the capacitive sensor and thus the SR of the attacks is lower in the latter case. We can also see that the performance of the attacks carried out using the optical sensor is lower when considering non-cooperative samples (compared to the samples generated with the cooperation of the user), as corresponds to a lower quality of the images.

On this basis, we can conclude that there exists a clear correlation between the quality of the fake fingerprint samples and the robustness against direct attacks of the NIST verification system: the better the image quality of the captured fake fingerprints, the higher the success rate of the attacks.

5.1.4.3. Ridge Based System Evaluation

In Table 5.1 (*b*) we show the Success Rates of the attacks (SR) for the ridge-based system in an analog way to those presented in Table 5.1 (*a*) for the NIST system.

Attacks with cooperation

In this case the difference between the robustness against random impostors (FAR in NOM) and the SR of attack 2 when using the optical sensor is significantly smaller than in the minutiae-based system. In addition, there are no noticeable differences in the success rate of the attacks between the three sensors used.

Attacks without cooperation

We observe that the SR is specially high for attack 1 with the thermal sensor, while specially low for attack 2 with the optical sensor. Also, as has been observed in the attacks with cooperation, the difference in the attacks performance between the three sensors is much lower than in the NFIS2 system.

Thus, we can conclude that the ridge-based system is more robust to variations in the fingerprints quality, and less vulnerable to direct attacks with good quality fake images than the minutiae-based system from NIST.

5.2. Direct Attacks Starting from an ISO Minutiae Template

The studies presented by Hill [2001], Ross *et al.* [2007], and Cappelli *et al.* [2007b], showed that, contrary to a common belief, a minutiae-based fingerprint template contains enough information to reconstruct a digital image similar to the original fingerprint, and such an image may be used to break a biometric system. In those studies the reconstructed digital images were compared to the original fingerprints, thus simulating indirect attacks carried out by injecting the reconstructed images into the feature extractor.

In the present contribution we perform a systematic and replicable evaluation of a more dangerous security threat: transforming such an indirect attack into a direct attack executed with gummy fingers made from the reconstructed images. The success chances of such attack are evaluated on a standard and publicly available fingerprint database [Fierrez *et al.*, 2007b], using a competitive matching algorithm working with ISO/IEC 19794-2 templates [ISO/IEC 19794-2, 2005].

The vulnerability threats shown in this study are of special relevance for applications working with fingerprint template standards such as the PIV program [NIST, 2005] (using ANSI-INCITS 378-2004 templates without encryption on smart cards), or the ILO Seafarers' Identity Document [ILO, 2006] (using ISO/IEC 19794-2 templates printed in clear on plastic cards as 2D barcodes).

5.2.1. Generation Process of the Gummy Fingers

The fake finger reconstruction approach comprises two phases: in the former, a fingerprint image is generated according to the technique proposed by Cappelli *et al.* [2007a,b], in the latter, the fingerprint image is used to make a fake fingertip.

5.2.1.1. From the Template to the Image

The image reconstruction approach exploits the information stored in the template to reconstruct a realistic image by estimating several aspects of the original unknown fingerprint through four processing steps (Fig. 5.7). The attacking scenario considered in this work supposes that only the mandatory information stored in a Fingerprint Minutiae Record of the ISO template is available [ISO/IEC 19794-2, 2005]; hence, the reconstruction approach only makes use of the following data: the image size, its resolution, and the list of minutiae, each defined as a quadruple $\{t, x, y, \theta\}$ that indicates its type ($t\epsilon$\{termination, bifurcation, other\}), position (x, y), and direction (θ).

The four reconstruction steps (Fig. 5.7) are here briefly summarized (the reader should refer to [Cappelli *et al.*, 2007b] for a more detailed description)

1. The fingerprint area is estimated according to the elliptical model proposed by Cappelli [2003], minimizing the area that encloses all the minutiae in the template.

2. The orientation image is estimated, starting from the direction of each minutia, by optimizing the parameters of the orientation model proposed by Vizcaya and Gerhardt [1996]. Then a local adjustment is performed to better approximate the orientations in the minutiae neighbourhoods.

3. The fingerprint pattern is generated by positioning minutiae prototypes and iteratively growing the pattern, starting from the orientation image and the frequency image (denoting the local ridge-line frequency). The local frequency is initially assumed constant over the whole fingerprint (according to an input parameter υ [Cappelli *et al.*, 2006a, 2007b]), and then refined in step 4 for a further execution of step 3. The minutiae prototype positioning

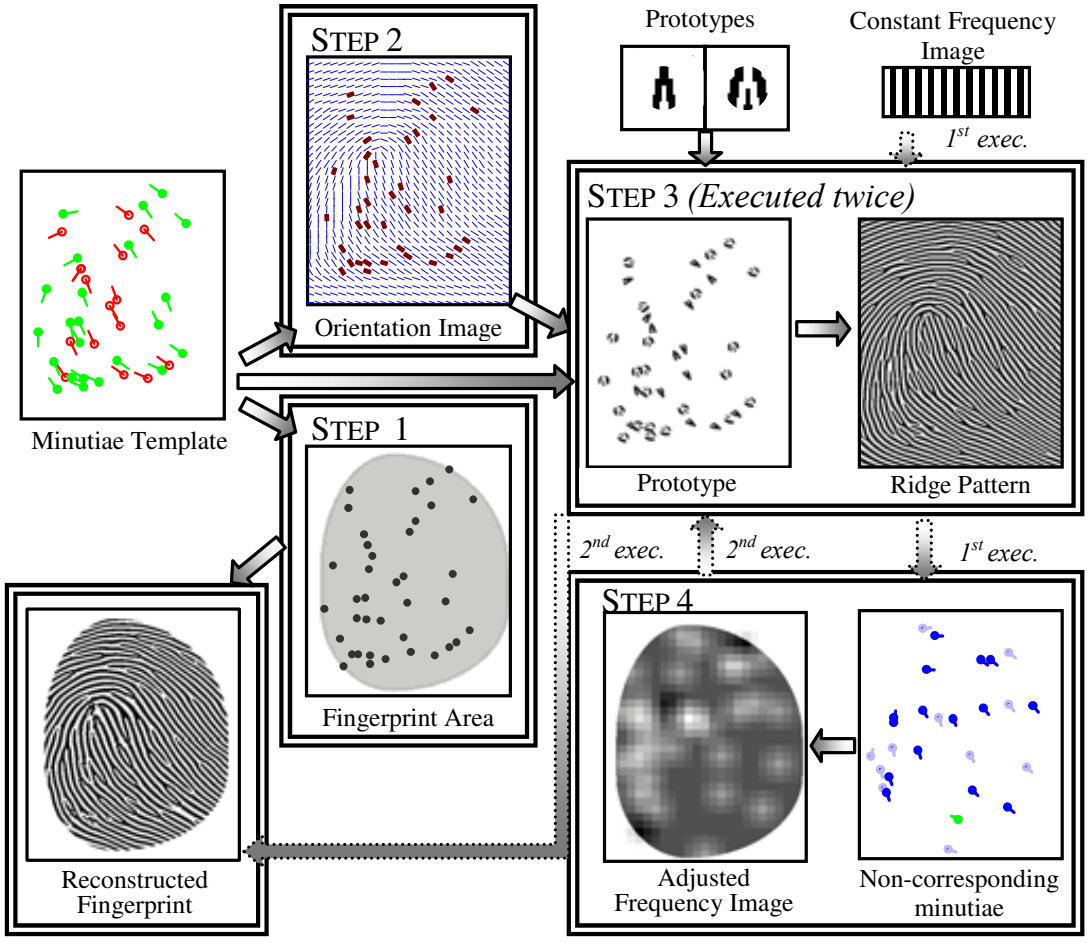


Figure 5.7: *Steps followed to reconstruct the fingerprint image from the ISO minutiae template.*

consists in placing on an empty image a small prototype for each minutia, properly scaled and rotated. The iterative pattern growing iteratively modifies the image by applying at each pixel a Gabor filter adjusted according to the local frequency and orientation until the whole image has been covered [Cappelli *et al.*, 2007b].

4. A more realistic frequency image (than the constant one) is estimated by comparing the minutiae in the image generated by the first execution of step 3 with the original template. The frequency image is locally adjusted as follows: the frequency is decreased in the neighborhood of any false minutia and increased in the regions where true minutiae are not present. Then step 3 is repeated using the new frequency image as input, usually resulting in a generated image with a lower number of non-corresponding minutiae.

Cappelli *et al.* [2007b] included the addition of noise in the final rendering of the image to make it more realistic. In the present work, both fake fingerprints made from noisy images and from "perfect" ridge patterns have been evaluated (see Sect. 5.2.4.1).

5.2.1.2. From the Image to the Fake Finger

The technique used to go from the two dimensional reconstructed fingerprint image to the three dimensional fake finger is similar to the non-cooperative method to generate gummy fingers described in Sect. 5.1.1. Once the fingerprint image has been reconstructed from the ISO template, the colours are inverted (i.e., ridges are now valleys and viceversa) and the inverted image is printed on a slide which will serve as a mask to create a Printed Circuit Board (PCB) where the circuit lines are the valleys of the original fingerprint. Once the PCB has been generated the steps to be carried out are analogue to steps *e* to *f* shown in Fig. 5.2. The whole process to go from the reconstructed fingerprint image to the gummy fingertip is depicted in Fig. 5.8.

Four examples of real images and their corresponding reconstructed and fake samples are shown in Fig. 5.9. The quality of the different datasets (estimated in Sect. 5.2.4.3) is also shown.

5.2.2. Fingerprint Verification Systems

The described reconstruction process is used to carry out a vulnerability evaluation of an ISO minutiae-based matcher against direct attacks executed with fake fingers generated from ISO templates. Previous to the vulnerability evaluation a development experiment is carried out on a totally different scenario (sensor, database, and systems tested), in order to acquire some general information about the attack potential and to adjust parameters. Thus, although the main objective of the experimental framework is to evaluate the vulnerability of an ISO matcher to the proposed attack, several other systems are used in the development experiment in order to fix the parameters of the image reconstruction algorithm:

- **Development experiment**. The experiments are carried out on the eight fingerprint matchers used in [Cappelli *et al.*, 2007b] and [Cappelli *et al.*, 2007a]. These systems are state-of-the-art commercial fingerprint recognition algorithms and, to the best of our knowledge, all of them (whose implementation details are industrial secrets) use minutiae as the main feature; on the other hand it is likely that they also exploit other features to improve the performance.

- **ISO matcher evaluation**. The ISO matcher used in the evaluation is a proprietary highly competitive system. The only available information about its internal functioning is that it works on pure ISO templates (only minutiae information is used). Thus, in the evaluation it is treated as a black box (only inputs and outputs are known) ensuring that the results are objective and unbiased[1].

5.2.3. Database and Experimental Protocol

As presented in the previous section, a development experiment is carried out previous to the vulnerability evaluation of the ISO matcher. The main objectives pursued by this preliminary

[1]The names of the commercial systems tested are not disclosed here to avoid any form of undesired publicity

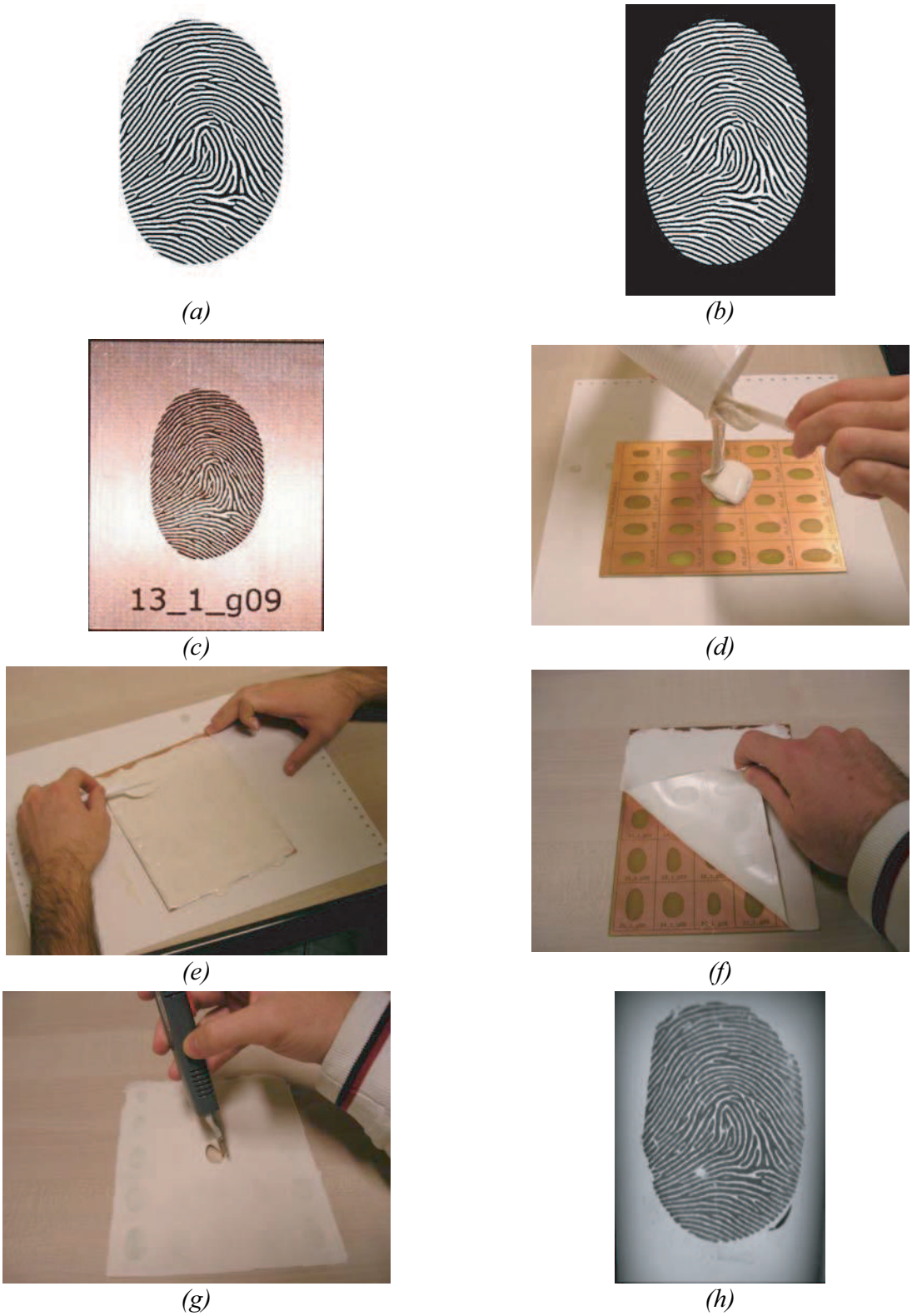


Figure 5.8: *Process followed to generate the fake fingerprint: reconstructed image (a), negative of the reconstructed image (b), fingerprint on the PCB (c), pour the silicone and catalyst mixture on the PCB (d), spread the mixture over the PCB (e), detach when it hardens (f), cut out each fake finger (g), final fake fingerprint acquired (h).*

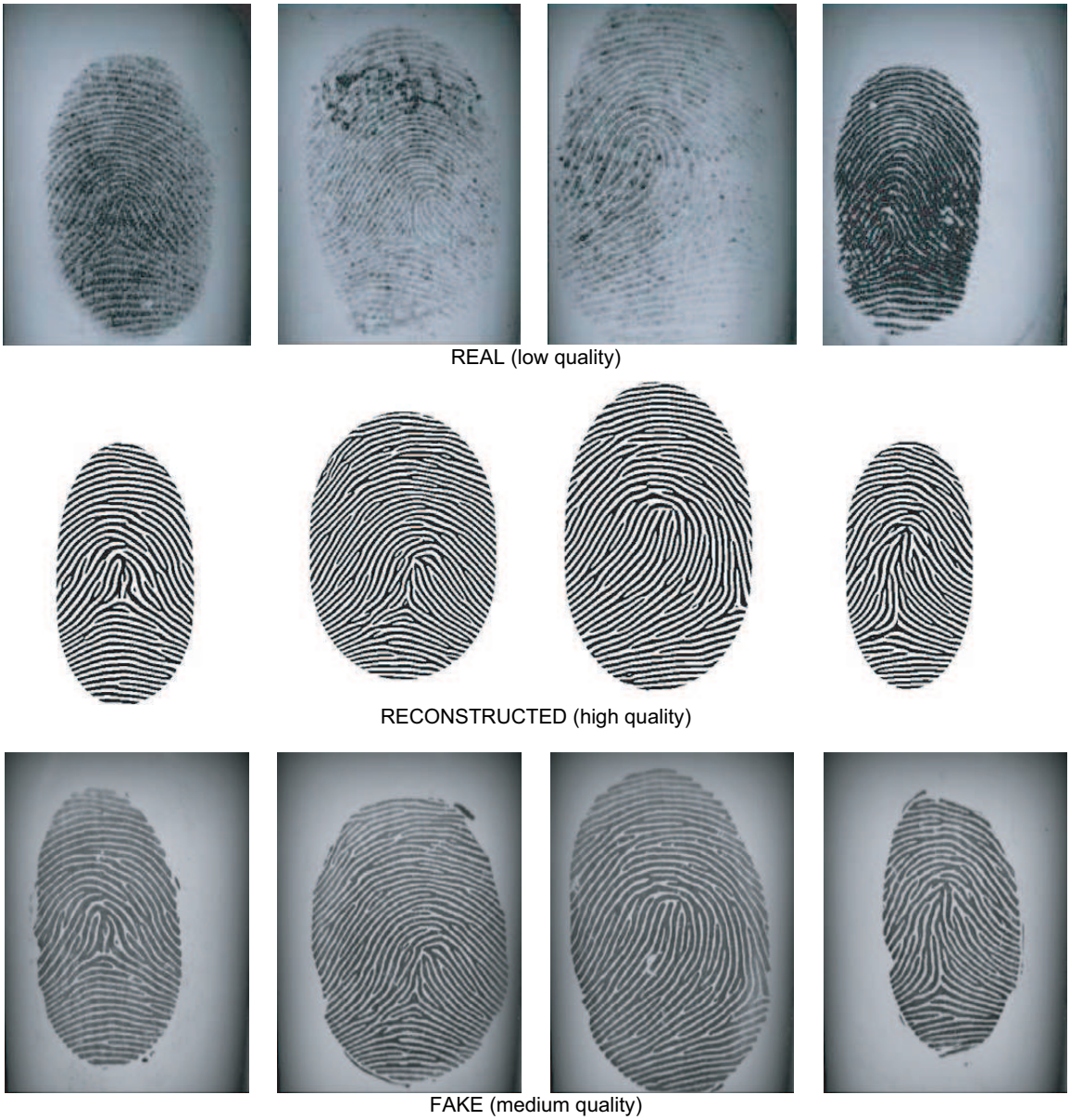


Figure 5.9: *Typical examples of images that can be found in each of the datasets (real, reconstructed, and fake) used in the evaluation. The quality level corresponding to each of the datasets is also shown.*

experiment are namely, *i*) fix the parameters of the image reconstruction algorithm for the ISO matcher evaluation, *ii*) verify the feasibility of the whole attacking approach, and *iii*) decide which of the configurations, with or without noise, produces better results. For this reason it is carried out on a totally different scenario (sensor, database, and protocol) to the final ISO matcher evaluation. Thus, the database and experimental protocol followed in the development experiment and in the vulnerability evaluation are:

- **Development experiment**. The evaluation of the ISO matcher is carried out over the FVC2006 DB2 database [Fierrez *et al.*, 2007b], captured with the optical Biometrika

Figure 5.10: *Original fingerprints (left). Reconstructed images without noise (row 1) and with noise (row 3) for decreasing ridge frequencies. The respective final fake fingerprints without noise (row 2), and with noise (row 4).*

FX3000 sensor. Thus, in order to have an independent training scenario (for the tuning of the algorithm parameters, objective *i*) this preliminary experimentation was executed over the FVC2002 DB1 captured with the optical CrossMatch sensor [Maio *et al.*, 2002a], also used by Cappelli *et al.* [2007b]. This way the final evaluation results are ensured to be totally unbiased, and at the same time there are previous experimental results with which to compare the performance of the attack in these preliminary tests (objective *iii*) [Cappelli *et al.*, 2007b].

Ten different fingerprint ISO templates were selected from the original database (FVC2002 DB1), and three images, each with a different ridge frequency (period of 7, 8, and 9 pixels, respectively), were reconstructed from each of the templates. In addition, two scenarios (with and without random noise) were considered, so that in the end a total $10 \times 3 \times 2 = 60$ fingerprint images were printed in the PCBs, and therefore 60 silicone fingers were finally produced. One sample of each of the 60 fake fingers is captured with the CrossMatch sensor, thus resulting in a final database of 60 impostor images. In Fig. 5.10 we show

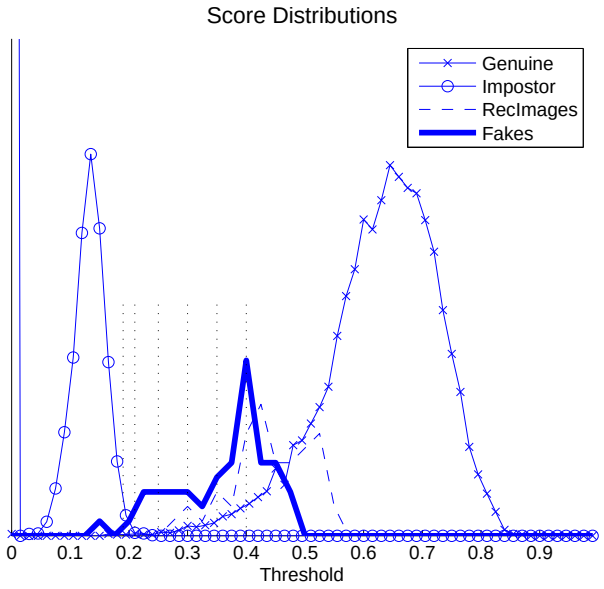


Figure 5.11: *Matching score distributions and selected thresholds (dotted lines).*

for the configuration without noise (two top rows), and with noise (two bottom rows), an original fingerprint (left), together with the three reconstructed images at different ridge frequencies and their respective final impostor images.

Three different thresholds were computed for each of the eight matchers tested as in [Cappelli *et al.*, 2007b], corresponding to: FAR=1%, FAR=0.1%, and FAR=0%. For each of the thresholds, we consider that an attack has been successful if any of the three impostor images (corresponding to the three different ridge frequencies taken into account) produces a matching score higher than the threshold.

- **ISO matcher evaluation**. The experiments are carried out on the FVC2006 DB2 database [Fierrez *et al.*, 2007b], captured with the Biometrika Fx3000 optical sensor and comprising 12 samples from 140 different fingers (a total of 1,680 images).

  In order to set the different operating points in which to evaluate the system robustness, genuine and impostor sets of scores are computed following the FVC2006 protocol, i.e.: *i*) for genuine tests all the 12 samples of each user are compared with each other avoiding symmetric comparisons ($(12 \times 11)/2 = 66$ scores per user), this results in $66 \times 140 = 9,240$ genuine scores, and *ii*) for impostor tests the first sample of every user is compared with the first sample of the remaining users in the database (again avoiding symmetric comparisons), resulting in $(140 \times 139)/2 = 9,730$ impostor scores. The genuine and impostor score distributions are depicted in Fig. 5.11 (crosses and circles, respectively).

  These sets of matching scores are used to compute the system threshold (μ) for: FAR=1% ($\mu = 0.19$), FAR=0.1% ($\mu = 0.21$), and FAR=0% ($\mu = 0.25$). The last two thresholds correspond to the typical operating points of a medium/high-security application (see

[ANSI-NIST, 2001]); however, in order to evaluate the matcher robustness for higher levels of security, the operating points $\mu = 0.30$, $\mu = 0.35$, and $\mu = 0.40$ (all with zero FAR) have been also considered. All the six operating points are shown with a vertical dotted line in Fig. 5.11.

Three images (each with a different ridge frequency, as in the preliminary experiment) are reconstructed from the ISO templates corresponding to the first fingerprint of each of the first 50 users in FVC2006 DB2 database. Each of the three reconstructed images were matched with the respective genuine fingerprint. The matching score distribution for the best performing frequency images is depicted in Fig. 5.11 (dashed line).

Due to practical restrictions concerning the PCBs manufacture, only one of the reconstructed images (corresponding to the best performing frequency) from each ISO template has been converted into a gummy finger. In spite of this strategy, the results obtained in the evaluation are in no case optimistically biased, as they are always lower bound to those that would be achieved in a real attack scenario (where the intruder would try to access de system with the fake fingers corresponding to the three ridge frequencies). One sample of each of the 50 fake fingers is acquired with the Biometrika FX3000 sensor and matched to its corresponding genuine fingerprint, resulting in a score distribution which is depicted in Fig. 5.11 with a thick solid line.

5.2.4. Results

In this section we present the results obtained by the described attacking approach in the development experiment, and in the vulnerability evaluation of the ISO matcher. In an analogue way to the evaluation of the direct attacks starting from a latent fingerprint, we also carry out a quality-based analysis of the attack which gives some further understanding of the studied security threat.

5.2.4.1. Development Experiment

All the attacks performed (to the ten real fingerprints selected) for the three operating points considered were able to spoof each of the eight systems tested. Although all the attacks carried out in both scenarios (with and without noise) were successful, the results show that the average matching score obtained in the noisy-images scenario is about 14% lower than that reached in the scenario without noise.

Thus, although the number of fake fingers generated is not enough to obtain statistically significant results about the vulnerability of the different systems to the attack, this preliminary experimentation does match the three objectives proposed. We can conclude from the results that the configuration chosen for the reconstruction algorithm (objective *i*) is very effective against all the matchers tested, proving that the attacking approach is totally feasible (objective *ii*). Furthermore, as expected, the attack presents a better performance when using the fake fingerprints created without noise (objective *iii*).

Threshold	FAR	FRR	1-FRR	RIASR	DASR
$\mu = 0.19$	1%	0.08%	99.92%	100%	**98%**
$\mu = 0.21$	0.1%	0.12%	99.88%	100%	**96%**
$\mu = 0.25$	0%	0.17%	99.83%	100%	**90%**
$\mu = 0.30$	0%	0.41%	99.59%	98%	**78%**
$\mu = 0.35$	0%	1.03%	98.97%	92%	**68%**
$\mu = 0.40$	0%	2.06%	97.94%	82%	**50%**

Table 5.2: *Results of the ISO matcher evaluation. RIASR stands for Reconstructed Images Attack Success Rate, and DASR for Direct Attack Success Rate.*

5.2.4.2. ISO Matcher Evaluation

The results of the ISO matcher evaluation are presented in Table 5.2. The performance of the matcher (in terms of FAR and FRR) in each of the thresholds considered (marked with a vertical doted line in Fig. 5.11) is recorded in columns 2 to 4. With these performance results, the matcher would have ranked among the top five algorithms competing in FVC2006 (out of 42 that entered the open category). The fact that FVC2006 algorithms typically exploit minutiae information complemented with other ridge pattern data while the evaluated matcher works only on pure ISO minutiae templates, proves it to be highly competitive.

In column five of Table 5.2 we show, for each considered operating point, the percentage of times (out of the total 50 mentioned in the experimental protocol) any of the three frequency images produced a score higher than the fixed threshold. Finally, the percentage of successful attacks (out of the total 50) for each of the thresholds considered is recorded in the last column of Table 5.2.

In Fig. 5.11 we can observe that both score distributions (reconstructed images and fake fingerprints) are clearly tilted towards the genuine score distribution, which results in the high attack success rates shown in the last two columns of Table 5.2. Fig. 5.11 also highlights a difference between the matching scores achieved with the reconstructed images and those obtained with the fake fingerprints (whose distribution is centered more to the left). This decrease in the value of the matching scores results in a reduction in the number of successful attacks for all the operating points considered (see Table 5.2). This loss of efficiency of the attack will be further discussed in Sect. 5.2.4.3 based on different quality measures.

From the results shown in Table 5.2 we can conclude that, although a top performing algorithm has been tested, the system is highly vulnerable to the attack approach presented in the paper, and even for a very high security configuration (with over 2% of FRR) an eventual attacker would be able to enter the system in half of the attempts. This rate increases to over 75% for more realistic operating points (FRR<0.5%).

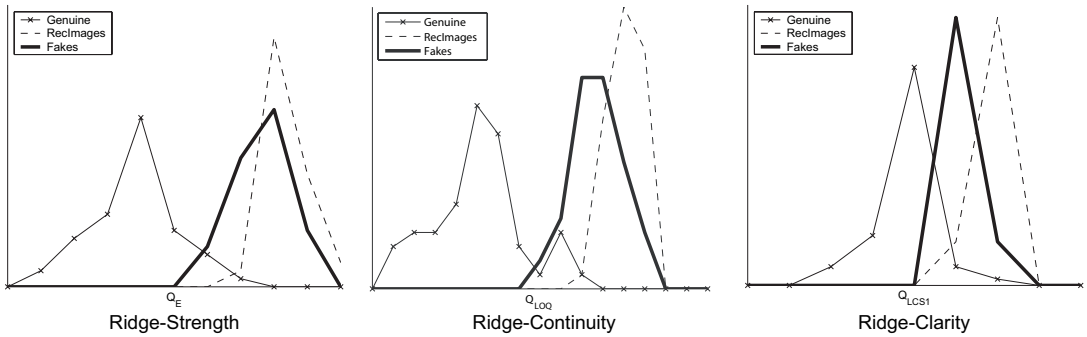


Figure 5.12: *Distributions corresponding to the original (solid with crosses), reconstructed (dashed), and fake (thick solid) datasets, for the three quality measures computed.*

5.2.4.3. Quality Analysis

In order to find an explanation to the decrease in the mean value of the scores observed in Fig. 5.11 (images acquired from the fake gummy fingers compared to the reconstructed fingerprint images), a quality analysis of the samples comprised in the experimental database is performed following an analogue protocol to the one used in the evaluation of the direct attacks starting from a latent fingerprint. The same three quality measures presented in Sect. 5.1.4.1 and estimating different fingerprint properties (ridge-strength, ridge-continuity, and ridge-clarity), were computed on each of the three datasets used in the attack evaluation (original, reconstructed, and fake fingerprint images).

In Fig. 5.12 we show the quality distributions of the images belonging to each of the three datasets (original genuine fingerprint images, reconstructed, and fake), for the three quality measures computed. We can observe that, regardless of the image property measured, the lowest quality corresponds to the original fingerprint images, the highest to the reconstructed images, and an intermediate quality level is presented by the fake fingerprint samples.

This is an expected result as the reconstructed images represent perfectly clean fingerprints (with no noise or distortions), while the manufacturing process introduces some noise in the gummy fingers generated from these images (which entails a slight decrease of the images quality). On the other hand, real fingerprints present a high degree of degradation (dry or wet fingers, marks or scars, dirt, etc.) which produces lower quality levels. These three quality levels can be observed in Fig. 5.9 where four real fingerprints used in the experiments (top row), together with their associated reconstructed images (middle row), and the fake samples (bottom row) are shown.

It has already been proven in several works that lower quality samples imply lower performance [Alonso-Fernandez *et al.*, 2008; Fierrez-Aguilar *et al.*, 2006], so the decrease in the quality level between the reconstructed images and the fake samples (observed in Fig. 5.12), explains that the scores reached by the latter are in general lower than those produced by the clean reconstructed images. Hence, this quality decrease is directly linked to the loss of efficiency of the attack detected in Table 5.2 (between the case in which it is carried out with the clean

reconstructed images, and the case in which the gummy fingers are used).

5.3. Indirect Hill-Climbing Attacks

In this section, we study the feasibility of indirect attacks towards two fingerprint verification systems. The indirect attacks implemented for the evaluation are known as hill-climbing attacks [Uludag and Jain, 2004], and are directed to the input of the matcher. The attacks are implemented on both the NIST minutia-based system and a Match-on-Card (MoC) system.

Match-on-Devices represent a hot topic in biometrics, of which a representative example is Match-on-Card for fingerprint recognition. In Match-on-Card systems, the user information, fingerprint template and matching algorithm are stored in a smart card [Bergman, 2008]. Smart cards have integrated circuits or microprocessors that may allow the encryption and protection of stored information and the execution of moderately complex algorithms [Bistarelli *et al.*, 2006; Mueller and Martini, 2006; Sanchez-Reillo *et al.*, 2003]. They allow users to easily carry with them a full biometric verification system. Corroborating the increasing interest in Match-on-Card systems, in the Fingerprint Verification Competition (FVC) 2004 [Cappelli *et al.*, 2006b], a special evaluation track was introduced for the case of matching systems with reduced memory and time restrictions. In the 2006 competition, [FVC, 2006], the need for introducing new specific Match-on-Card and Match-on-Device categories was stated. Furthermore, the American National Institute of Standards and Technology (NIST) is currently performing the Minutiae Interoperability Exchange (MINEX) II public evaluation of Match-on-Card systems [Grother *et al.*, 2008]. The objective of this evaluation is to certify fingerprint Match-on-Card algorithms, required by the US government Personal Identity Verification program for the identification and authentication of Federal employees and contractors. The common approach in these and other related benchmarks in fingerprint recognition is to evaluate competing systems with regard to the verification error rates and other performance measures [Wilson *et al.*, 2004b]. In the present study, we stress the importance of also evaluating the robustness of fingerprint systems against possible attacks.

No attacks of the type evaluated in this work have been tested in real operating conditions like the ones considered in the present study to the extent of our knowledge.

5.3.1. Hill-Climbing Algorithm

The hill-climbing attacks studied in this work are implemented as follows. The attacks assume that the user template is stored in the system as a set of minutiae. Minutiae are defined by their position (x, y) and orientation α.

At the beginning of the attack a set of 100 synthetic random minutiae templates is generated. Synthetic templates are divided in 9×9 pixels cells. Each cell can only contain one minutiae, this way we avoid generating minutiae which are closer than the inter-ridge distance. Next, the following steps are followed:

1. The 100 synthetic minutiae templates are initially sent to the matcher to be compared with the attacked fingerprint.

2. Out of the 100 synthetic templates, the one that produces the highest score is stored.

3. The saved template is iteratively modified by means of:

   a) Changing an existing minutia by moving it to an adjacent cell or by changing its orientation.

   b) Adding a minutia.

   c) Replacing a minutia.

   d) Deleting a minutia from the template.

4. The four types of iteration mentioned above are executed one at a time and changes are only saved if they cause an improvement in the score.

5. The algorithm stops either when the decision threshold (μ) or the maximum number of iterations allowed is reached.

The performance of these attacks is compared to the one of brute force attacks, in terms of the required attempts to reach the decision threshold. As was already stated in 3.2, assuming that we have access to an unlimited collection of different fingerprints, the theoretical number of attempts that a brute force attack would need against a verification system is equal to the inverse of the False Acceptance Rate ($E_{ff-bf} = 1/FAR$).

In the indirect attacks evaluation we study the impact of several parameters, such as the number of initial minutiae or the effectiveness of each type of iteration (a, b, c and d). The effects of the usage of a Region of Interest (ROI) for the placement of synthetic minutiae (i.e. in the generation of the 100 synthetic template set and in step 3 of the algorithm) are also studied. The ROI is defined as the area of the fingerprint images in which most minutiae are found and is obtained heuristically from a fingerprint database as shown in Fig. 5.13 (right). It can be hypothesized that the generation of synthetic features only in the ROI should improve the algorithm effectiveness, reducing the number of iterations needed.

5.3.2. Fingerprint Verification Systems

The vulnerabilities to hill-climbing attacks are studied on two different minutiae-based fingerprint verification systems, one running on a PC and one embedded in a smart card (Match-on-Card):

- The minutiae-based NIST Fingerprint Image Software 2 (NFIS2) [Garris *et al.*, 2004]. This is the same system used in the vulnerability evaluation of direct attacks carried out with gummy fingers generated from latent fingerprints (see Sect. 5.1.2).

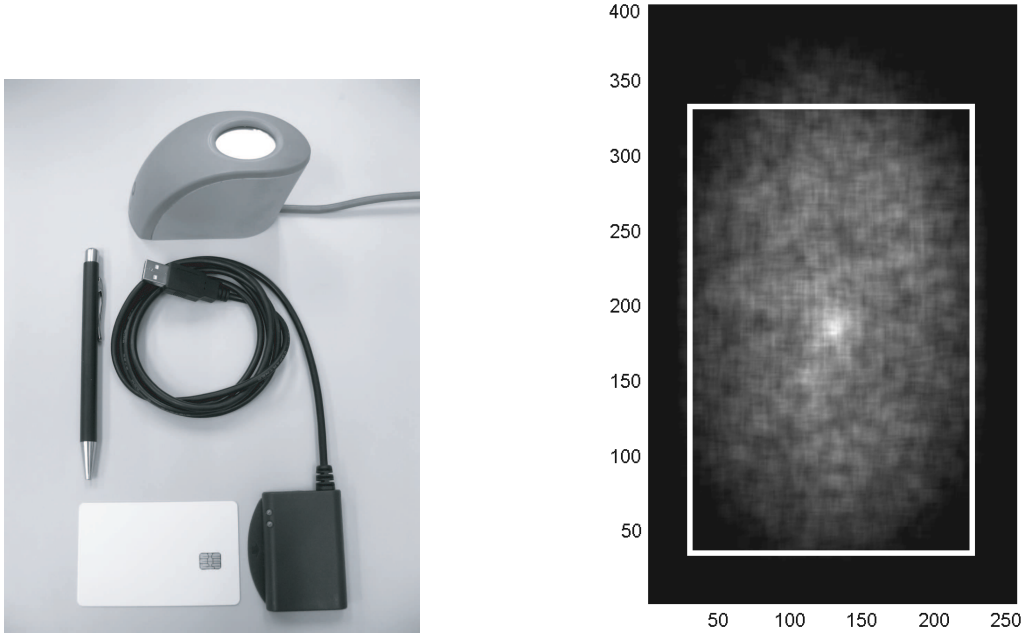


Figure 5.13: *(Left) Top: fingerprint sensor used for acquiring the fingerprints in our experiments. Bottom: MoC system used in our experiments. (Right) Histogram of minutiae locations, and Region of Interest (ROI).*

- A prototype Match-on-Card system. The system is a prototype from a Match-on-Card vendor, developed in 2006. It is a minutiae-based system with the matching algorithm fully embedded in a smart card. This is a good method to protect the privacy of users (their templates do not leave the card), while providing reasonable performance with current technology. In the experiments the NIST software is used in the feature extraction process and the resulting templates are transformed to the MoC system format and sent to the smart card. Except for basic information about the input-output interface of the smart card, the specificities of the matching algorithm are unknown in our analysis, being thus a realistic attack scenario. The MoC system evaluated in our experiments is shown in Fig. 5.13 (left).

5.3.3. Database and Experimental Protocol

The hill-climbing attacks have been studied using a subcorpus of the MCYT_Fingerprint dataset [Ortega-Garcia *et al.*, 2003] (for a brief description of the database see Sect. 3.3). The subcorpus comprises 10 impressions of the right and left index fingers of 75 users ($75 \times 2 \times 10 = 1,500$ images), captured electronically with an optical sensor UareU from Digital Persona (500 dpi, 256×400 images). Six of the samples of each finger were acquired with a high control level (small rotation or displacement of the finger core from the center of the sensor was permitted), another two with a medium control level, and the remaining two with low control level (see Figs. 5.15–5.18 for example fingerprint images).

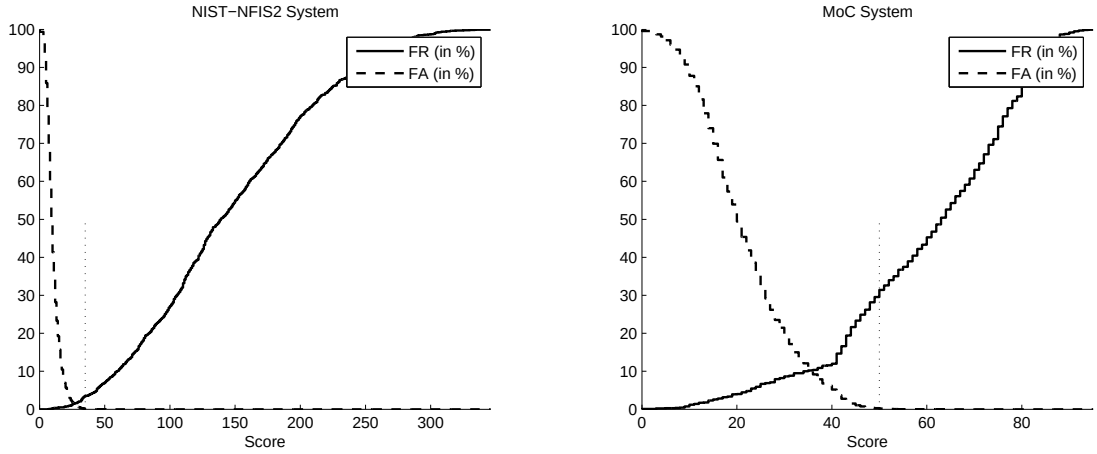


Figure 5.14: *FAR and FRR curves for the NIST (left) and MoC systems (right). The vertical doted lines show the operating point where the systems are evaluated.*

In Fig. 5.13 (right) we depict the two dimensional histogram of all the minutiae locations in the subcorpus, together with a rectangle that was heuristically obtained and which contains the majority of the minutiae. This rectangle defines the Region of Interest (ROI) and will be used in the experiments as described in Sect. 5.3.1 to improve the success rate of the attacks.

The 1,500 images available in the subcorpus were also used for evaluating the verification error rates of the two studied systems. We use one of the low control samples as a template and the other 9 samples from the same finger as probes to test genuine matches, leading to $150 \times 9 = 1,350$ genuine user scores. Impostor scores are obtained comparing each template to one sample from each other finger of the subcorpus, thus resulting in $150 \times 149 = 22,350$ impostor scores. These sets of genuine and impostor scores are used to compute the FAR and FRR curves of both systems depicted in Fig. 5.14.

Using one of the impressions of high control level for each fingerprint, the 150 different fingerprints considered in the database were attacked following the algorithm described in Sect. 5.3.1.

For the NFIS2 system, a decision threshold (μ) of 35 for the match score is fixed (marked with a dote line in 5.14), leading to a 0.10% FAR and a 3.33% FRR. This means that a brute force attack would need in average 1/FAR = 1,000 attempts to be successful. For the Match-on-Card system a decision threshold (μ) of 50 is selected (marked with a dote line in 5.14), resulting in a FAR of 0.16% and a FRR of 28.73%. In this case a brute force attack would need around 630 attempts to break the system. The brute force attack number of iterations (1,000 and 630 respectively) will be considered in the experiments in order to evaluate the success rate and speed of the attacks. An attack is considered as successful if it needs less iterations than the ones a brute force would theoretically need. We establish a maximum of 5,000 and 2,000 iterations for the NFIS2 and the MoC system respectively. If the decision threshold is not reached within these limits of iterations, the algorithm ends.

Different configurations are tested, varying the number of initial synthetic minutiae, modify-

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 1,000 it. (%)	SR before 5,000 it. (%)
			a	b	c	d		
No	a, b, c, d	38	1.87	5.16	6.13	0.90	1.3	42.7
Yes	a, b, c, d	38	2.41	4.93	5.60	1.35	4.7	56.7

(a) Hill-climbing statistics using all iterations with and without ROI.

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 1,000 it. (%)	SR before 5,000 (%)
			a	b	c	d		
Yes	a, b, c, d	38	2.41	4.93	5.60	1.35	4.7	56.7
Yes	a, b, c	38	3.18	7.70	7.91	-	18.7	96.7
Yes	b, c	38	-	9.25	9.76	-	26.7	95.3

(b) Hill-climbing statistics deleting low performing iterations.

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 1,000 it. (%)	SR before 5,000 it (%)
			a	b	c	d		
Yes	b, c	25	-	10.85	8.95	-	18.7	90.7
Yes	b, c	38	-	9.25	9.76	-	26.7	95.3
Yes	b, c	55	-	5.68	13.67	-	8.0	88.0

(c) Hill-climbing statistics using different amounts of initial minutiae.

Table 5.3: *Hill-climbing results on NFIS2. The Success Rate (SR) of the attack is given in percentage out of the total 150 accounts attacked.*

ing the iterations of the algorithm or using the previously described ROI. Following the defined protocol, 150 different accounts are attacked for each possible configuration.

5.3.4. Results

5.3.4.1. NFIS2 System Evaluation

In the first experiment, the effect of using a ROI is studied. In Table 5.3 (a) the effect of the ROI when it is included in the configuration of the attack can be seen. The SR of the hill-climbing attacks that need less iterations than an eventual brute force attack raises from 1.3% to 4.7% when no synthetic minutiae are allowed to be placed outside the ROI. The number of successful attacks before the maximum number of attempts is reached increases from 42.7% to 56.7%. This first experiment (Table 5.3 (a)) also shows that not all the iterations (changing, adding, replacing or deleting a minutia) have the same probability of improving the matching score.

A second experiment is performed to analyze the effectiveness of each type of iteration, defined in Sect. 5.3.1. In Table 5.3 (b) the effect of eliminating the least effective iterations is studied. The results show that iterations a and d (changing and deleting a minutiae respectively) have barely any impact in the success rate of the attacks. Actually, when they are not performed,

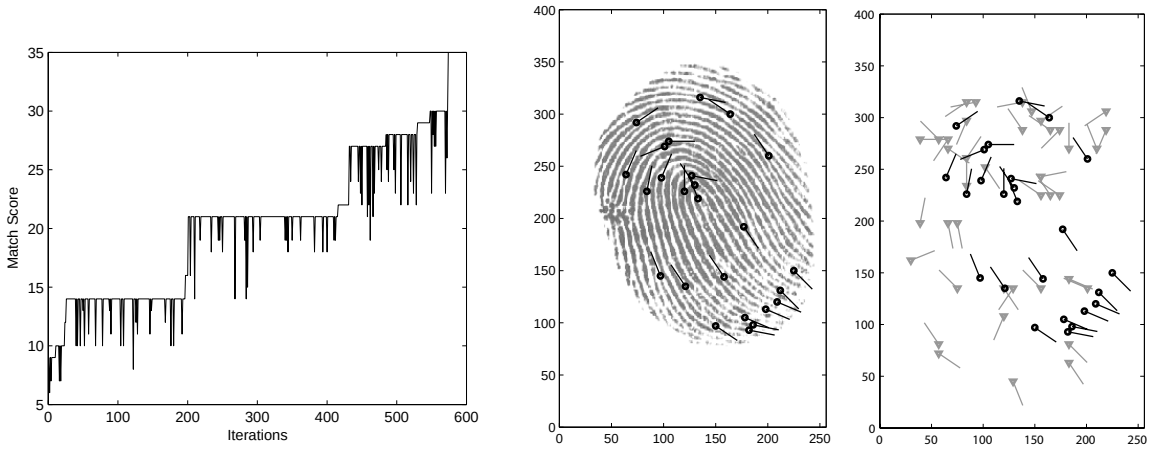


Figure 5.15: *(a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) that achieve a higher score than the decision point on NFIS2 in a relatively short attack.*

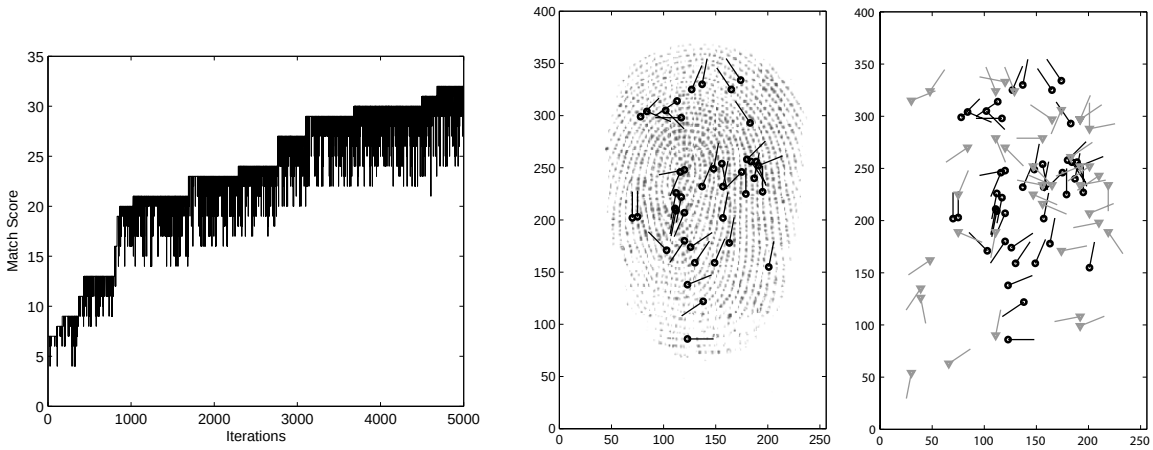


Figure 5.16: *(a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) after 5,000 iterations on NFIS2 in an unsuccessful attack.*

the SR of the attack increases from 56.7% to 95.3%.

In the third experiment we use the best configuration so far, i.e., taking into account the ROI and performing iterations b and c, to analyze the impact of the initial number of minutiae in the synthetic fingerprints. The NFIS2 system extracts an average of 38 minutiae points from the fingerprints in the database considered. We can see in Table 5.3 (c) that the success rate of the attacks improves when the initial number of minutiae approaches 38.

In Fig. 5.15 we show the minutiae maps and the evolution of the matching score in a successful

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 630 it. (%)	SR before 2,000 it. (%)
			a	b	c	d		
Yes	b, c	10	-	7.70	5.30	-	43.3	88.7
Yes	b, c	25	-	5.53	10.08	-	82.0	97.3
Yes	b, c	38	-	3.55	13.27	-	52.0	92.7

(a) Hill-climbing statistics using different amounts of initial minutiae.

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 630 it. (%)	SR before 2,000 it. (%)
			a	b	c	d		
Yes	a, b, c, d	25	1.22	4.60	5.71	4.68	34.7	88.0
Yes	b, c, d	25	-	5.24	5.98	5.03	52.7	92.0
Yes	b, c	25	-	5.53	10.08	-	82.0	97.3

(b) Hill-climbing statistics deleting low performing iterations.

ROI	Iterations	Initial Minutiae	Score Raise Probability (%)				SR before 630 it. (%)	SR before 2,000 it. (%)
			a	b	c	d		
Yes	b, c	25	-	5.53	10.08	-	82.0	97.3
No	b, c	25	-	6.13	9.15	-	60.7	98.7

(c) Hill-climbing statistics with and without rectangular ROI.

Table 5.4: *Hill-climbing results on the Match-on-Card system. The Success Rate (SR) of the attack is given in percentage out of the total 150 accounts attacked.*

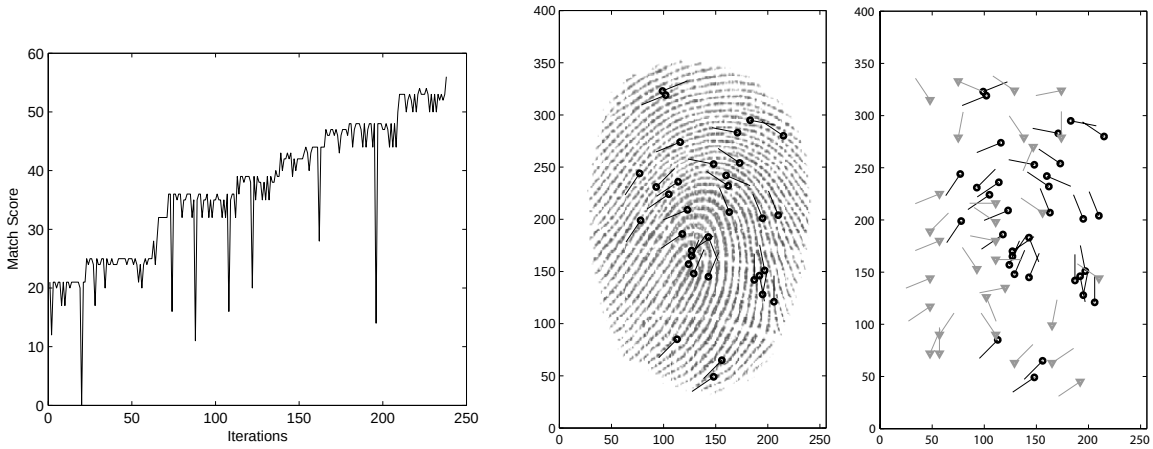
attack against the NIST system. Fig. 5.16 shows the same data for an unsuccessful attack. In the first case around 580 iterations are needed to reach the desired matching score (35), while in the failed attack the maximum allowed number of iterations is reached before the algorithm reaches the positive verification score.

5.3.4.2. MoC System Evaluation

The experiments for the MoC system follow an inverse order than the ones for the NIST system. Based on the best configuration of the attack for the NFIS2 system, we first study the influence of the initial number of minutiae over the final success rate in the MoC system. In this case we find that better results are achieved using 25 initial minutiae, instead of the 38 used in the NFIS2 system. In Table 5.4 (a) we can see that the number of fingerprints cracked before a brute force attack increases from 52.0% to 82.0% when the initial number of minutiae is reduced from 38 to 25.

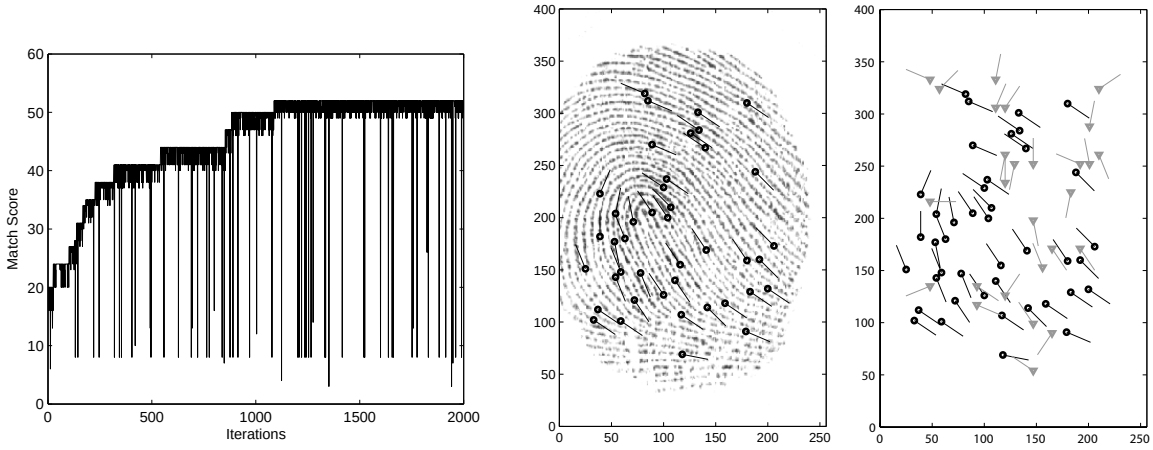
The contribution of each type of iteration is then analyzed. In Table 5.4 (b) the effect of each of the iterations over the match score can be observed. As happened in the NFIS2 system, the most effective iterations are b and c, so a and d can be again discarded.

In the last experiment we focus on the impact of the ROI over the number of successful



(a) (b) (c)

Figure 5.17: *(a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) that achieve a higher score than the decision point on the MoC system in a relatively short attack.*



(a) (b) (c)

Figure 5.18: *(a) Score progression, (b) original fingerprint minutiae, and (c) original minutiae (black circles) vs. synthetic minutiae (grey triangles) after 2000 iterations on the MoC system in an unsuccessful attack.*

attacks. As can be seen in Table 5.4 (c) when no minutiae are allowed to be placed outside the ROI, the number of fingerprints cracked before a brute force attack increases from 60.7% to 82%. No significant improvement can be observed in the use of the ROI when the maximum number of iterations is reached.

In Figs. 5.17 and 5.18 the minutiae maps and the evolution of the matching score in a successful and an unsuccessful attack are respectively depicted for the MoC system. In the first

case the desired matching score of 55 is reached in around 240 iterations, while in the failed attack the maximum number of iterations is reached before the algorithm gets to the positive verification matching score.

The results show that the performance of hill-climbing attacks is heavily dependent upon the system under attack and the iterations that are performed. Attacks with reduced number of minutiae are highly successful against the MoC system, while their performance against NFIS2 is very poor, even when using the same minutiae feature extractor from NIST. This is probably due to the limitations of the matcher embedded in the smart card.

It may be derived from the results that, at least in the case of NFIS2, hill-climbing attacks are less effective than brute force attacks. This statement must be taken with care, as hill-climbing attacks require much less resources than the ones needed by a brute force attack. In fact, to perform an efficient brute force attack, the attacker must have a database of more than a thousand different real fingerprint templates which is not straightforward to obtain, whereas there is no need for real templates in the case of a hill-climbing attack.

5.4. Attack Protection

The vulnerability evaluation results to direct and indirect attacks presented in the previous sections, prove the need of providing fingerprint recognition systems with the necessary countermeasures to prevent the attacks. In this section we propose two ways of minimizing the effects of direct and indirect attacks: liveness detection and score quantization.

5.4.1. Countermeasuring Direct Attacks: Liveness Detection

The liveness detection approach based on quality measures described in Sect. 4.2 is used to countermeasure the direct attacks evaluated in Sects. 5.1 and 5.2 (starting from a latent fingerprint, and from an ISO template). The aim of the experiments is to find the efficiency of the vitality detection method classifying the images (real or fake) of the different datasets used in the direct attacks evaluations.

The evaluation protocol followed is analogue to the method used in the validation of the vitality detection method. In order to find the optimal parameter subsets (out of the 10-feature parameterization proposed) exhaustive search is applied to each of the datasets of the direct attacks evaluations, using the leave-one-out technique (i.e., all the samples in the dataset are used to train the classifier except the one being classified). In Tables 5.5 and 5.6 we present the optimal feature subsets found to countermeasure the direct attacks starting from a latent fingerprint, and from an ISO template. The classification performance (real or fake) of the method is given in terms of the Average Classification Error (ACE), which is defined as $ACE = (FLR + FFR)/2$, where the FLR (False Living Rate) represents the percentage of fake fingerprints misclassified as real, and the FFR (False Fake Rate) computes the percentage of real fingerprints assigned to the fake class.

		Liveness detection of gummy fingers generated from a latent fingerprint										
		Ridge Strength		*Ridge Continuity*		*Ridge Clarity*						
		Q_{OCL}	Q_E	Q_{LOQ}	Q_{COF}	Q_{MEAN}	Q_{STD}	Q_{LCS1}	Q_{LCS2}	Q_A	Q_{VAR}	ACE
Opt.	C	×	×	×	×	×	×		×		×	1.88
	NC	×	×		×		×	×	×		×	0.55
Cap.	C	×	×			×	×			×	×	0.37
	NC	×			×	×	×		×	×	×	0
Ther.	C			×	×	×	×			×	×	2.60
	NC	×		×	×		×			×	×	0.84

Table 5.5: *Optimal performing subsets for quality-based vitality detection of gummy fingers generated from a latent fingerprint. The datasets correspond to those used in the vulnerability evaluation described in Sect. 5.1.3, where C stands for fake fingers generated with the Cooperation of the user, and NC following the Non-Cooperative process. The symbol × means that the feature is considered in the subset. The ACE appears in percentage.*

	Liveness detection of gummy fingers generated from an ISO template										
	Ridge Strength		*Ridge Continuity*		*Ridge Clarity*						
	Q_{OCL}	Q_E	Q_{LOQ}	Q_{COF}	Q_{MEAN}	Q_{STD}	Q_{LCS1}	Q_{LCS2}	Q_A	Q_{VAR}	ACE
Opt.	×	×	×	×	×	×				×	0

Table 5.6: *Optimal performing subset for quality-based vitality detection of gummy fingers generated from an ISO minutiae template (see Sect. 5.2.3). The symbol × means that the feature is considered in the subset. The ACE appears in percentage.*

In Table 5.5, where the results for the gummy fingers generated from a latent fingerprint are presented, we can see that for the images captured with the three sensors (optical, capacitive and thermal), the liveness detection approach is more effective detecting fake fingerprints generated without the cooperation of the user (NC). This result is consistent with the quality analysis presented in Sect. 5.1.4.1, where we could see that the quality distribution of non-cooperative fake fingerprints was more separated from the real fingerprints distribution, than that of the images produced by gummy fingers generated with the cooperation of the user. Thus, non-cooperative fake images are easier to classify and less errors are made.

Although the liveness detection method presents a high performance for the three sensing technologies tested (an average 1.07% ACE is reached for all the datasets), it is specially effective on the capacitive sensor where all the non-cooperative fake images were correctly classified. Again, this results reinforces the observations made in Sect. 5.1.4.1 where the quality distributions corresponding to the capacitive sensor were the most separated ones (and so the easiest to be classified).

Results of the liveness detection method performance on the dataset used for the vulnerability evaluation of direct attacks carried out using gummy fingers generated from ISO templates are shown in Table 5.6. All the 50 real and fake images comprised in the test set were correctly classified. The quality analysis performed in Sect. 5.2.4.3 already suggested this excellent result, as the distributions (real and fake fingerprints) shown in Fig. 5.12 are very well differentiated.

Reaching a 0% classification error in some of the datasets does not imply that the proposed approach is the definitive solution to countermeasure direct attacks. Depending on the size of the database, on the materials used to generate the gummy fingers, or on the acquisition sensor, the performance of the proposed liveness detection system will change (as has been shown). However, the results obtained on the different scenarios, show the high efficiency as liveness detection method of the proposed quality-based approach and its great potential as a way to minimize the risks entailed by direct attacks.

It is interesting to notice as well, that the databases used for the validation of the liveness detection algorithm and for the direct attacks vulnerability evaluations are completely different in terms of size, materials and process used to generate the gummy fingers, acquisition protocols, etc. However, the Biometrika FX3000 sensor was used in the acquisition of part of the three databases, and for those particular datasets (the ones captured with the Biometrika device) the subset of features presenting the lowest ACE is the same. This fact suggests that the optimal feature subset (out of the 10 feature parameterization proposed) for a given dataset is mainly dependent on the acquisition device and not on other factors such as the material or the manufacturing process of the fake fingers. This parameter consistency can be of great help when designing efficient strategies to protect automatic fingerprint recognition systems from direct attacks.

As was already pointed out in Sect. 4.2.2, it has to be remarked that in either cases, direct attacks carried out from a latent fingerprint or from an ISO template, the implementation of the liveness detection approach would have very little impact (if any) on the performance of the systems under the normal operation scenario, just increasing its FRR in 1.07% for the worst case.

5.4.2. Countermeasuring Indirect Attacks: Score Quantization

The BioAPI consortium [BioAPI, 2009] recommends that biometric algorithms emit only quantized matching scores in order to prevent eventual hill-climbing attacks. Such quantization means that small changes in the randomly generated templates will normally not result in a modification of the matching score so that the attack does not have the necessary feedback from the system to be carried out successfully.

The fingerprint verification systems put to test against the hill-climbing attack (NIST and MoC) produce integer quantized scores, in the ranges observed in the FAR and FRR curves depicted in Fig. 5.14. Such a quantization has proven not enough in order to act as countermeasure against the hill-climbing attacks.

In our experiments, the four types of iterations described (a, b, c and d) may increase or decrease the match score during a hill-climbing attack, as seen in Figs. 5.15-5.18. It is found that ca. 30% of the total number of iterations produce a score increase. The distribution of the score increase magnitudes during the iterations from the 150 attacks to the MoC system in one of the previous experiments is shown in Fig. 5.19. As can be seen, in most cases (more than 33% of the score increases), the score increases 1 unit. The score is increased in more than 5

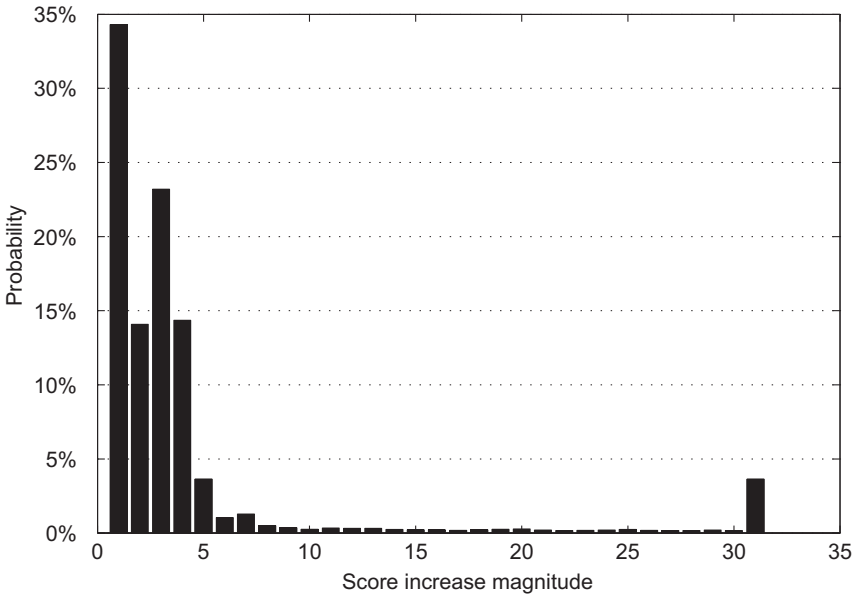


Figure 5.19: *Distribution of magnitudes corresponding to score increases during an experiment with the MoC system (150 attacks). Match scores are quantized as integer numbers.*

points in less than 15% of the cases. It must be taken into account that only score increases are shown in the histogram, as many iterations produce score decreases.

Further experiments are carried out where the similarity scores are forced to follow a 2 and 5 unit quantization step (i.e., only multiples of 2 and 5 are permitted). Taking into account the distribution shown in Fig. 5.19, it is expected that this quantization procedure may protect the system against the proposed attacks since most iterations produce score variations which are lower than these quantization steps. In Table 5.7 we show the performance of the best configuration of the hill-climbing attack against the NIST system (a) and the MoC system (b) for different quantization steps (QS).

The experiments show that score quantization is an effective measure in order to prevent the studied hill-climbing attack, as the performance of the algorithm drops drastically for just a 2 quantization step in the two systems tested (2% and 4% SR for the attack respectively). When 5 unit quantization steps are used, the system is nearly invulnerable to the implemented hill-climbing attacks.

In the systems under analysis, the score quantization steps considered do not significantly affect the verification performance. Nevertheless score quantization presents some drawbacks, being the most important of them that as the quantization step size grows, the matching scores loose their utility for multi-biometric applications [Ross *et al.*, 2006], which typically rely on fusion techniques of real-valued scores [Fierrez-Aguilar *et al.*, 2005c]. In addition, Adler [2004] introduced a modified hill-climbing algorithm which was robust to quantized scores. However, this algorithm was applied to the input images of the feature extractor and was very specific for face recognition systems, so its application to attacks directed to input of the matcher over fingerprint minutiae-based systems is at least unclear.

QS	1	2	5
SR before 1,000 it. (%)	26.7	2.00	0.7
SR before 5,000 it. (%)	96.7	34	0.7

(a) Results for the hill-climbing algorithm against the NIST system with different score Quantization Steps (QS).

QS	1	2	5
SR before 630 it. (%)	82.0	4.0	0.0
SR before 2,000 it. (%)	97.3	17.3	0.0

(b) Results for the hill-climbing algorithm against the MoC system with different score Quantization Steps (QS).

Table 5.7: *Evaluation of the hill-climbing attack against the NIST and MoC systems with score quantization.*

5.5. Chapter Summary and Conclusions

In this chapter we have analyzed the vulnerabilities of fingerprint recognition systems to different direct and indirect attacks, and we have proposed several countermeasures to reduce the effects of this type of threats.

Direct attacks starting from a latent fingerprint and from a standard minutiae ISO template have been evaluated. Regarding those in which a latent fingerprint is used to generate the gummy fingers, the attacks were performed on the NIST minutiae-based system and a proprietary ridge feature-based system, and were studied on a database of real and fake samples from 68 fingers, generated with and without the cooperation of the legitimate user, captured with three different sensors (optical, thermal and capacitive). Two different attacks were considered, namely: *i*) enrollment and test with gummy fingers, and *ii*) enrollment with a real fingerprint and test with its corresponding fake imitation. Statistically significant results on the performance of the attacks were reported and compared to the normal operation mode of the system.

The results show that, when considering the minutiae-based system, the attacks success rate is highly dependent on the quality of the fake fingerprint samples: the better the image quality of the captured fake fingerprints, the lower the robustness of the system against the two studied attacks. The ridge-based system proved to be more robust to high quality fake images and, in general, to variations in fingerprint image quality.

In the case of the direct attacks performed using gummy fingers generated from the compromised template of the genuine user, the vulnerability evaluation was carried out on a highly competitive ISO minutiae-based matcher using a standard and publicly available fingerprint database [Fierrez *et al.*, 2007b].

The results obtained, supported on a quality analysis of the fingerprint images, prove the suitability of the technique and the lack of robustness of automated minutiae-based recognition systems against this type of attack. The fact that these direct attacks are carried out starting from the compromised minutiae template of a user and not from a recovered latent fingerprint,

reinforces the idea that such a reverse engineering process (i.e., recovering the fingerprint from its minutiae information) is completely feasible, thus disproving the widespread belief of non-reversibility of fingerprint templates.

Furthermore, the study raises a key vulnerability issue about the usage of standards. It is unquestionable the convenience of standards in terms of the systems interoperability and the development of the biometric technology. However, we cannot forget that standards also provide very valuable information about the system functioning (e.g., format in which the templates are stored) which can be used to carry out attacks such as the one evaluated in the present contribution if a user's template is compromised.

The results reached in these two vulnerability evaluations to direct attacks, reinforce the need of considering and designing specific countermeasures which minimize the risks entailed by these threats (e.g., specific protection for templates [Clancy *et al.*, 2003; Ratha *et al.*, 2007], liveness detection approaches [Antonelli *et al.*, 2006; Tan and Schuckers, 2006], or multimodal authentication architectures [Fierrez-Aguilar *et al.*, 2005c]). In the present study we have evaluated the efficiency of the quality-based liveness detection approach proposed in Chapter 4 to detect these attacks. The results have proven that the described method is a powerful tool to prevent these fraudulent actions, being able to detect over 98% of the illegal access attempts.

Finally, the vulnerabilities to indirect attacks of different fingerprint verification systems have been evaluated. Two fingerprint recognition systems, one running on a PC and the other system fully embedded in a smart card, were evaluated against hill-climbing attacks. Experiments were carried out on a sub corpus of the MCYT database. The attacks showed a big dependency on the type of iterations performed and on the system being attacked. For a sufficient number of iterations, success rates of over 90% were reached for both systems, being the PC system the one that needed a higher number of attempts to be cracked. Score quantization was also studied as a possible countermeasure against hill-climbing attacks, proving to be an effective way of preventing these threats. Interestingly, not all the fingerprints showed the same robustness against this type of attacks, being some of them much more difficult to crack than others.

This chapter includes novel contributions in the consistent and replicable methodology used, the quality related findings, the development of a direct attack starting from the compromised ISO template of the legitimate user, and the sensor- and matcher-dependent findings in the security evaluation of fingerprint systems.

Chapter 6

Security Evaluation of On-Line Signature-Based Authentication Systems

This chapter studies the vulnerabilities of on-line signature-based recognition systems to two different indirect attacks, and several approaches to countermeasure these security threats are evaluated.

As in the previous chapter, the order followed for the analysis of the attacks has been selected on the basis of the knowledge needed to carry them out. First, we study a brute-force attack performed with synthetically generated signatures produced using the novel approach presented in Sect. 4.3 (access to the input of the feature extractor is required in order to execute this attack). Then, we analyze the hill-climbing attack based on Bayesian adaptation described in Sect. 4.1 (information on the template format is needed, as well as access to the matcher input and to the score returned by the system). The results obtained from the vulnerabilities evaluation to the hill-climbing attack serve as well as validation experiments of the iterative algorithm and help to better understand the attacking approach.

Apart from other possible general countermeasures (such as the limitation of the permitted number of unsuccessful attempts to access a given account), one biometric-based method to increase the robustness of dynamic signature verification systems against each of the attacks is proposed. In the case of the brute-force attack we discuss the feasibility of using synthetically generated duplicated samples of real signatures to complement the enrollment data in order to enhance the efficiency of the system, and reduce the access probabilities of the attack. For the hill-climbing algorithm we analyze the most robust feature subsets (from the 100 feature set proposed by Fierrez-Aguilar *et al.* [2005b]) to the attack, and we perform a comparative study between robustness and performance for the tested system.

The chapter is structured as follows. One section is dedicated to each of the studied attacks (Sects. 6.2 and 6.1, respectively). Both sections share a common structure: first, a description

of the attack is given, then the systems used in the evaluation are presented, the database and experimental protocol are described in another subsection, and finally we analyze and discuss the results. The experiments regarding the evaluation of countermeasures for the analyzed attacks are described in Sect. 6.3. The summary and conclusions of the chapter appear in the final section (Sect. 6.4).

This chapter is based on the publications: Galbally *et al.* [2009d,e, 2007, 2008b]

6.1. Indirect Brute-Force Attack with Synthetic Signatures

From all the possible vulnerability threats that biometric systems might present, one of them, which arises from their inherent probabilistic nature, is common to all automatic recognition systems: there is always a certain probability of accessing the system with a different biometric trait to that of the genuine user. This probability, which is represented by the False Acceptance Rate (FAR) at each operating point, is the origin of the so called brute-force attacks [Martinez-Diaz *et al.*, 2006]. This type of attacks try to take advantage of this security breach by presenting to the system successive biometric samples until one of them obtains a positive answer from the system.

Apart from possible countermeasures that could be included in recognition systems, such as limiting the number of consecutive access attempts, the main drawback of brute force attacks is the great amount of biometric data necessary for the attack to be carried out (e.g., in a signature recognition system operating at a point with FAR=0.01%, the attacker would need to have, in average, a database comprising 10,000 different signatures to carry out a successful brute force attack). Such a big quantity of biometric samples is not easy to obtain, which has led in many cases to not consider this type of attacks as a realistic danger to the security level of the system.

However, in the past few years, several works have presented different algorithms to generate synthetic biometric traits such as fingerprints [Cappelli *et al.*, 2007b], iris [Zuo *et al.*, 2007], or signature [Djioua and Plamondon, 2009; Popel, 2007]. In many cases, these synthetically generated traits have proven to present, when used in automatic recognition systems, a very similar performance to that of the real ones [Cappelli *et al.*, 2006b]. In addition, synthetic databases have the clear advantage over real datasets of presenting a nearly effort-free generation process in comparison to the time-consuming and complicated process of real acquisition campaigns. All these characteristics make synthetic samples very useful tools for the performance evaluation of biometric systems. However, at the same time they turn brute force attacks into a feasible security threat as they might be used to overcome the lack of biometric data by an eventual attacker.

In the present section we present an evaluation of a HMM-based on-line signature verification system against a brute force attack carried out with synthetically generated handwritten signatures. The signatures are generated according to the algorithm presented in Sect. 4.3, which is based on the modeling of the trajectory functions in the frequency domain. Comparative results between a brute force attack carried out with real and synthetic signatures are given, proving

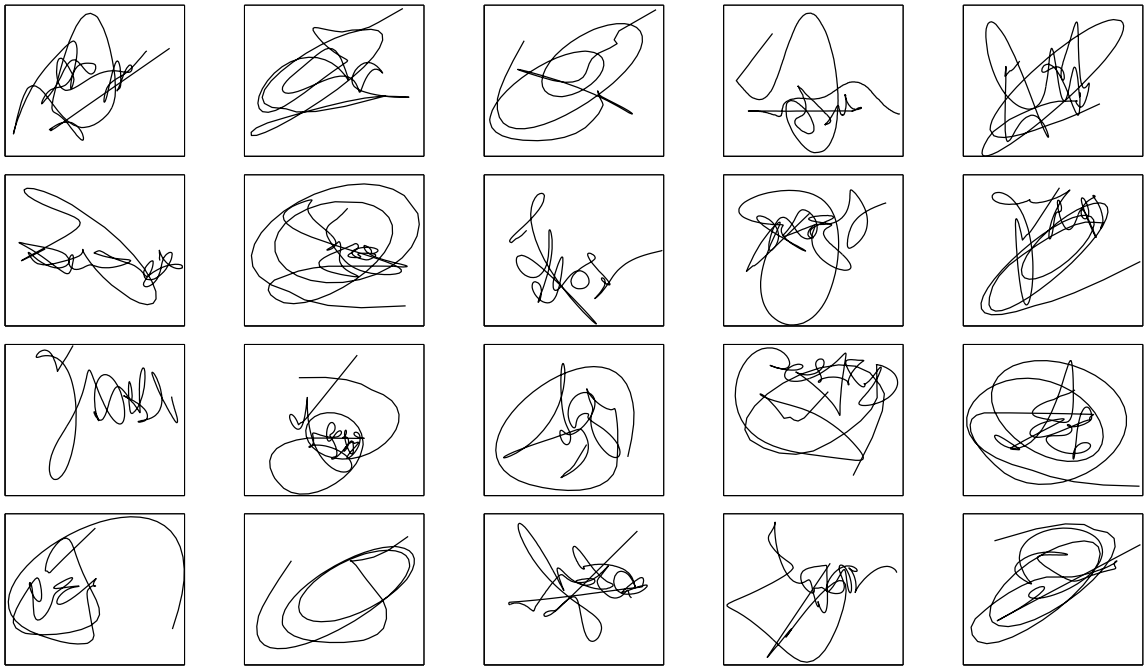


Figure 6.1: *Examples of synthetic signatures used in the experiments.*

the feasibility of executing such an attack with artificial samples.

6.1.1. Generation Process of the Synthetic Signatures

The synthetic signatures used to perform de brute-force attack were produced following the generation scheme of synthetic signatures based on spectral analysis described in Sect. 4.3. As explained there, in a first stage totally synthetic individuals are created (no real samples are used in the process), and then different duplicated samples of those subjects are produced. The parameters defining the generation algorithm are those presented in Sect. 4.3.3 and used in the validation experiments of the method (extracted from the BiosecurID database [Fierrez *et al.*, 2009]).

In Fig. 6.1 we show some examples (one impression per user) of synthetic signatures generated following the proposed algorithm and used in the brute-force attack.

6.1.2. On-Line Signature Verification Systems

The system used in this vulnerability study is based on the one described by Fierrez-Aguilar *et al.* [2005b] which participated in the Signature Verification Competition 2004 [Yeung *et al.*, 2004], where it reached the first and second positions against random and skilled forgeries respectively.

The main differences between the original system and the one used in this security evaluation, is that in the latter a set of 7 functions was extracted from the raw signature time signals (spatial coordinates x and y, and pressure p), from which the first and second order derivatives were

#	Feature	Description
1	x-coordinate	x_n
2	y-coordinate	y_n
3	Pen-pressure	z_n
4	Path-tangent angle	$\theta_n = \arctan(\dot{y}_n/\dot{x}_n)$
5	Path velocity magnitude	$\upsilon_n = \sqrt{\dot{y}_n + \dot{x}_n}$
6	Log curvature radius	$\rho_n = \log(1/\kappa_n) = \log(\upsilon_n/\dot{\theta}_n)$, where κ_n is the curvature of the position trajectory
7	Total acceleration magnitude	$a_n = \sqrt{t_n^2 + c_n^2} = \sqrt{\dot{\upsilon}_n^2 + \upsilon_n^2\theta_n^2}$, where t_n and c_n are respectively the tangential and centripetal acceleration components of the pen motion.
8-14	First-order derivative of features 1-7	$\dot{x}_n, \dot{y}_n, \dot{z}_n, \dot{\theta}_n, \dot{\upsilon}_n, \dot{\rho}_n, \dot{a}_n$

Table 6.1: *Set of features used by the HMM-based system tested against the brute-force attack performed with synthetic signatures.*

computed, leading to 21-dimensional feature vector. In the present system the second order derivatives are discarded as they proved to haver a very low contribution in the verification performance. In Table 6.1 the whole set of 14 functions used by the system is presented.

As well, in this implementation an initial step is added to the original HMM training scheme [Fierrez-Aguilar *et al.*, 2005b], leading to the following stages: *i*) the global mean and covariance of the training signatures is assigned to all the mixtures, *ii*) k-means segmentation and Maximum Likelihood training is performed, *iii*) Baum-Welch re-estimation is carried out. The first step allow to have a trainable model for step *iii* (despite being inaccurate) in the case where step *ii* fails due to the large number of parameters to be estimated, or other computational problems.

Similarity scores are computed as the log-likelihood of the signature (using the Viterbi algorithm) divided by the total number of samples of the signature. In order to keep scores between reasonable range, normalized scores s_n between (0,1) are obtained as $s_n = \exp(s(\mathbf{x}, C)/30)$, where $\mathbf{x}$ and C represent respectively the input signature to verify and the enrolled model of the claimed identity.

In the present vulnerability study the attacked models were constructed using the described HMM-based recognition system using a configuration of 12 left-to-right HMM states and mixtures of 4 Gaussians per state.

6.1.3. Database and Experimental Protocol

As in the security evaluation performed with Bayesian hill-climbing attack, the experiments are carried out on the publicly available MCYT database [Ortega-Garcia *et al.*, 2003]. Real signature models constructed from the MCYT subjects and using the HMM-based recognition system described in Sect. 6.1.2, were attacked with a synthetically generated database following the same structure as MCYT (330 signatures $\times$ 25 samples per signature). The evaluation was carried out in four different conditions: with and without considering the pressure function (as

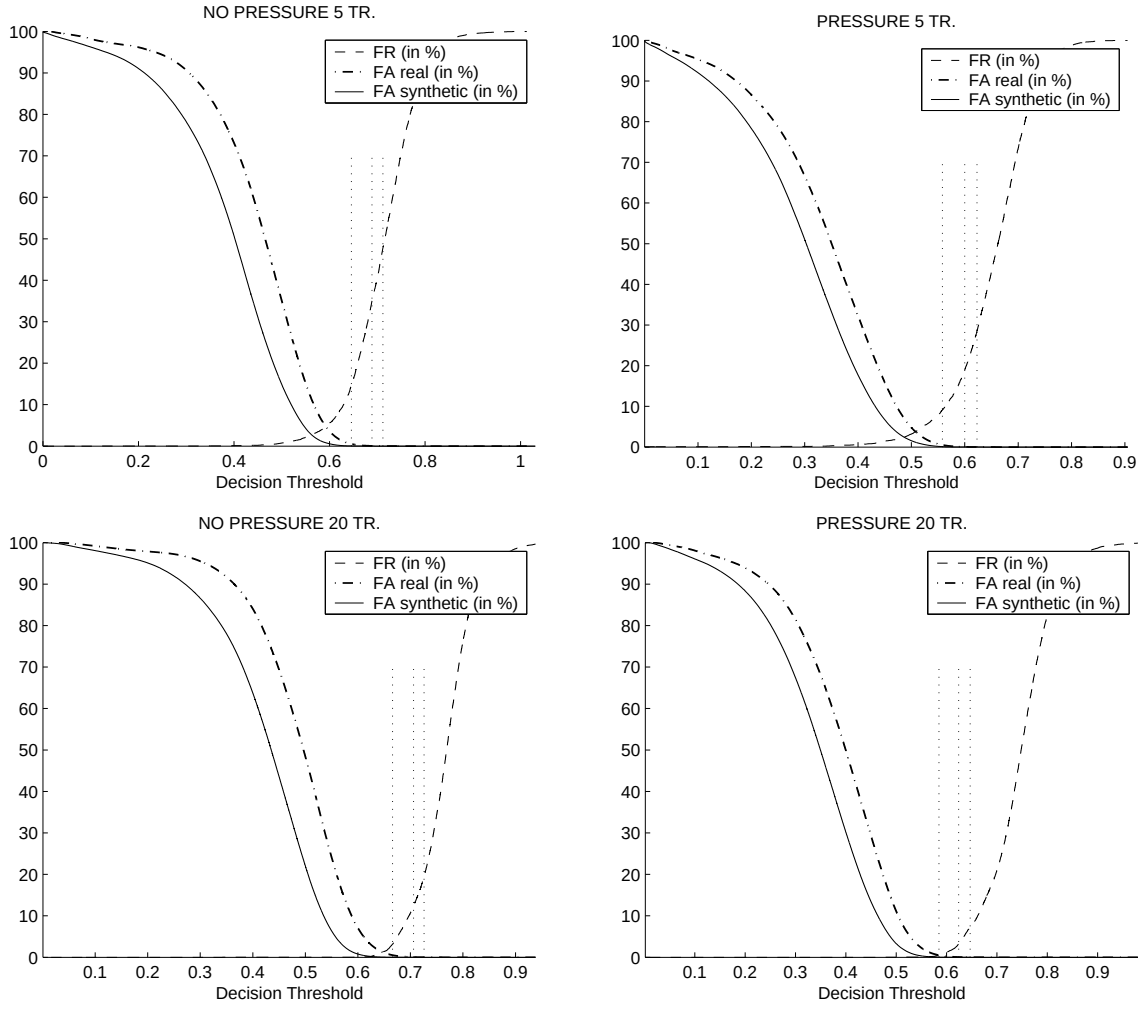


Figure 6.2: *FRR (dashed curves), FAR with real impostors (dashed doted curves), and FAR with synthetic impostors (solid curves), for all the configurations of the system used (with and without considering the pressure function, and for 5 and 20 training signatures). The vertical doted lines correspond to the operating points with FAR (real impostors) of 0.5%, 0.05%, and 0.01%.*

not all the on-line signature acquisition devices capture this information), and for 5 and 20 training signatures.

A brute force attack is successful when, after a certain number of attempts, the attacker is able to enter the system using a different signature to that of the genuine user. Thus, the Success Rate (SR) of a brute force attack can be defined as $1/N$ (where N is the mean number of attempts necessary to access the system), which coincides with the False Acceptance Rate (FAR) of the system. For this reason the FAR of the evaluated system was computed under two different working scenarios:

- **Normal operation mode**. In this scenario both enrollment and test are performed with real signatures (i.e., only the MCYT database is considered). The results obtained in this scenario are used as reference. In order to compute the genuine and impostor sets of

FAR real impostors (in %)		0.5	0.05	0.01
No Pressure	**5 Tr.**	0.04	0.001	NaN
	20 Tr.	0.02	NaN	NaN
Pressure	**5 Tr.**	0.1	0.006	0.001
	20 Tr.	0.05	0.002	NaN

Table 6.2: *Success Rate (in %) of the brute force attacks carried out with synthetic signatures at three different operating points of the system being attacked (decision threshold corresponding to FAR against real impostors = 0.5%, 0.05%, and 0.01%). NaN means that none of the impostor matchings performed during the brute force attack broke the system.*

scores, the MCYT database was divided into training and test sets, where the training set comprises either 5 or 20 genuine signatures of each user (used to train the system), and the test set consists of the remaining samples, thus resulting in 330×20 or 330×5 genuine scores. Impostor scores are obtained using one signature of each of the remaining users (i.e., 330×329 impostor scores). These sets of scores are used to compute the FAR (real impostors) and FRR (False Rejection Rate) of the system.

- **Brute force attack with synthetic signatures**. In this case only impostor scores are computed, matching the trained models of real users with all the synthetic signatures generated. This results in a set of $330 \times 330 \times 25$ impostor scores, which are used to compute the FAR curve of the system when using synthetic signatures (synthetic impostors).

6.1.4. Results

In Fig. 6.2 we show the FRR (dashed curve), the FAR with real impostors (dash-doted curve) for the four configurations considered (i.e., with and without taking the pressure function into account, and for 5 and 20 training signatures) in the normal operation mode, and the FAR (solid curve) for the brute force attack using synthetic signatures. We can observe that both FAR curves (using real and synthetic signatures) present a very similar behaviour in all the range of scores.

Worth noting, the FAR curve obtained with the synthetic signatures is below the FAR curve for the normal operation mode of the system for all the operating points. This means that, as expected, the system distinguishes better between real and synthetic signatures, than in the case of considering only real signatures. However the values of both curves are quite close, proving this way the feasibility of using synthetically generated signatures to carry out this type of attack.

In Table 6.2 we show the quantitative results for the three operating points highlighted in Fig. 6.2 with vertical doted lines which correspond to FAR (i.e., using real impostors) of 0.5%, 0.05%, and 0.01% under the normal operation mode. We can observe that the difference in the SR between both attacks (i.e., with real and synthetic signatures) is around one order

of magnitude. Interestingly, this difference is lower when we take into account the pressure function, which means that this information makes synthetic signatures have a more realistic appearance, so that the system has a greater difficulty in distinguishing between them and real signatures.

6.2. Indirect Hill-Climbing Attack

In the present section we study the performance of the novel hill-climbing attack based on Bayesian adaptation presented in Chapter 4, over an on-line signature recognition system using global features. Although several other works have analyzed the impact of indirect hill-climbing attacks on biometric systems [Adler, 2004; Uludag and Jain, 2004], non of them studied the vulnerabilities of on-line signature verification systems or used a matcher-independent approach as the one used in the present evaluation.

With these premises the objectives of this study are to analyze the weaknesses of signature recognition systems, and at the same time to perform a number of tests which serve as validation experiments of the proposed attacking algorithm and which give some insight about the working and efficiency of the attack.

6.2.1. Bayesian-Based Hill-Climbing Algorithm

The attacking technique used in this evaluation is the Bayesian approach to a hill-climbing attack presented in Chapter 4. As was explained there, the core idea behind the algorithm is to iteratively adapt a known global distribution to the local specificities of the unknown user being attacked. For this purpose, a pool of users (signatures in this particular case) is used to compute the general statistical model G, which is sampled N times. Each of the points in the distribution is compared with the client being attacked $\mathcal{C}$, generating N similarity scores $J(\mathcal{C}, \mathbf{y}_i)$, $i = 1, \ldots, N$. The M points which have generated highest scores are then used to compute a local distribution L, which is used to generate an adapted distribution A, that trades off (according to a parameter α) the general knowledge provided by G and the local information given by L. The global distribution is then redefined as $G = A$, and the process continues until the finishing criterion is met, i.e., one of the scores $J(\mathcal{C}, \mathbf{y}_i)$ exceeds the similarity threshold, or the maximum number of iterations is reached.

6.2.2. On-Line Signature Verification Systems

The proposed Bayesian hill-climbing algorithm is used to attack a feature-based on-line signature verification system. The signatures are parameterized using the set of features described by Fierrez-Aguilar *et al.* [2005b]. In that work, a set of 100 global features was proposed, and the individual features were ranked according to their individual discriminant power. A good operating point for the systems tested was found when using the first 40 parameters (in Table 6.3 we show the whole set of 100 parameters, with the 40 features used in our system highlighted

in light grey). In the present study we use this 40-feature representation of the signatures, normalizing each of them to the range [0,1] using the tanh-estimators described by Jain *et al.* [2005]:

$$p_k^{'} = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{p_k - \mu_{p_k}}{\sigma_{p_k}}\right)\right) + 1\right\}, \tag{6.1}$$

where p_k is the kth parameter, $p_k^{'}$ denotes the normalized parameter, and μ_{p_k} and σ_{p_k} are respectively the estimated mean and standard deviation of the parameter under consideration.

The similarity scores are computed using the Mahalanobis distance between the input vector and a statistical model of the attacked client $\mathcal{C}$ using a number of training signatures (5 in our experiments). Thus,

$$J(\mathcal{C}, \mathbf{y}) = \frac{1}{\left((\mathbf{y} - \boldsymbol{\mu}^{\mathcal{C}})^T (\boldsymbol{\Sigma}^{\mathcal{C}})^{-1} (\mathbf{y} - \boldsymbol{\mu}^{\mathcal{C}})\right)^{1/2}}, \tag{6.2}$$

where $\boldsymbol{\mu}^{\mathcal{C}}$ and $\boldsymbol{\Sigma}^{\mathcal{C}}$ are the mean vector and covariance matrix obtained from the training signatures, and $\mathbf{y}$ is the 40-feature vector used to attack the system.

6.2.3. Database and Experimental Protocol

The experiments are carried out on the MCYT signature database [Ortega-Garcia *et al.*, 2003], comprising 330 users. The database was acquired in 4 different sites with 5 time-spaced capture sets. Every client was asked to sign 5 times in each set, and to carry out 5 skilled forgeries of one of his precedent donors, thus capturing a total 25 genuine signatures and 25 skilled forgeries per user. A more detailed description of the dataset can be found in Chapter 3.

The database is divided into a training (used to estimate the initial K-variate distribution G) and a test set (containing the user's accounts being attacked), which are afterwards swapped (two-fold cross-validation). The training set initially comprises the genuine signatures of the odd users in the database and the test set the genuine signatures of the even users. This way, the donors captured in the 4 sites are homogenously distributed over the two sets.

For each user, five different genuine models are computed using one training signature from each acquisition set, this way the temporal variability of the signing process is taken into account. With this approach, a total $330 \times 5 = 1,650$ accounts are attacked (825 in each of the two-fold cross-validation process).

In order to set the threshold δ, where we consider that the attack has been successful, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) curves of the system are computed. In the case of considering skilled forgeries (i.e., impostors try to access other's accounts imitating their signature), each of the 5 estimated models of every user are matched with the remaining 20 genuine signatures ($5 \times 20 \times 330 = 33,000$ genuine scores), while the impostor scores are generated comparing the 5 statistical models to all the 25 skilled forgeries of every user ($5 \times 25 \times 330 = 41,250$ skilled impostor scores). In the case of random forgeries (i.e., impostors try to access other's accounts using their own signature), genuine scores are

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

Table 6.3: *Set of global features proposed by Fierrez-Aguilar et al. [2005b] and sorted by individual discriminative power. The 40 feature subset used in the evaluated system is highlighted in light grey. T denotes time interval, t denotes time instant, N denotes number of events, θ denotes angle.*

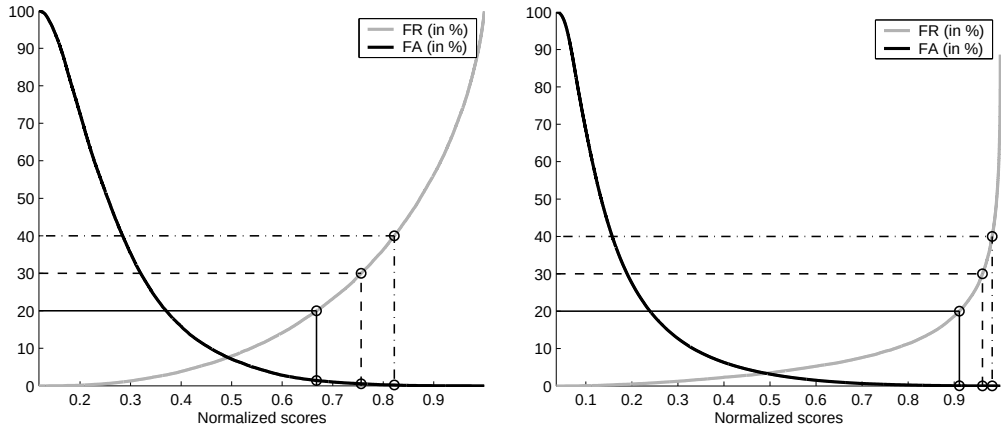


Figure 6.3: *FAR and FRR curves for skilled (left) and random (right) forgeries.*

computed as above, while the set of impostor scores is generated matching the 5 user models with one signature of the remaining donors, making a total of $5 \times 330 \times 329 = 542,850$ random impostor scores. The FAR and FRR curves both for skilled (left) and random (right) forgeries are depicted in Fig. 6.3, together with three different realistic operating points used in the attacks experiments (FRR=20%, FRR=30%, and FRR=40%). The similarity scores were normalized following the criterion described in Eq. (6.1).

6.2.4. Results

The goal of the experiments is to study the effect of varying the three parameters of the algorithm (N, M, and α), on the success rate (SR) of the attack, while minimizing the average number of comparisons (E_{ff}) needed to reach the fixed threshold δ (see Sect. 3.2 for definitions of SR and E_ff). As described in Sect. 6.2.1, the above mentioned parameters denote: N the number of sampled points of the adapted distribution at a given iteration, M the number of top ranked samples used at each iteration to adapt the global distribution, and α is an adaptation coefficient.

Although the proposed hill-climbing algorithm and a brute-force attack are not fully comparable (for example, the resources required differ greatly as an efficient brute-force attack needs a database of thousands of signatures), in the experiments we compare E_{ff} with the number of matchings necessary for a successful brute-force attack at the operating point under consideration ($E_{ff-bf} = 1/\text{FAR}$).

6.2.4.1. Analysis of N and M (Sampled and Retained Points)

For the initial evaluation of the algorithm, a point of [FRR=30%, FAR=0.01%] for random forgeries was fixed. This FAR implies that an eventual brute-force attack would be successful, in average, after 10,000 comparisons. Given this threshold, the algorithm was executed for different values of N and M (fixing $\alpha = 0.5$) and results are given in Table 6.4. The maximum number of

		N				
		10 (2500)	25 (1000)	50 (500)	100 (250)	200 (125)
M	3	5.03 **24,082**	68.18 **11,292**	78.78 **9,725**	86.78 **10,611**	84.00 **14,406**
	5	2.72 **24,404**	71.27 **10,713**	85.57 **7,957**	92.00 **8,752**	91.09 **12,587**
	10		38.18 **17,598**	84.18 **8,609**	92.78 **8,602**	92.06 **12,261**
	25			41.33 **17,972**	89.57 **10,857**	91.63 **13,633**
	50				51.45 **18,909**	83.15 **16,660**
	100					39.39 **22,502**

Table 6.4: *Success Rate (in %) of the hill-climbing attack for increasing values of N (number of sampled points) and M (best ranked points). The maximum number of iterations allowed is given in brackets. The SR appears in plain text, while the average number of comparisons needed to break an account (Efficiency, E_{ff}) appears in* ***bold****. The best configurations of parameters N and M are highlighted in grey.*

iterations (n_{it}) allowed for the algorithm appears in brackets. This value changes according to N in order to maintain constant the maximum number of comparisons permitted ($E_{ff} = N \cdot n_{it}$). In plain text we show the success rate of the attack (in % over the total 1,650 accounts tested), while the average number of comparisons needed for a successful attack is represented in **bold**.

An analysis of the results given in Table 6.4 shows that for $N \gg M$, the points selected to estimate the local distribution are too specific and thus, the success rate of the attacks degrades slightly with respect to the best trade-off combination ($N \approx M$). On the other hand, if $N \simeq M$, the local distribution computed is too general, and the attack success rate is significantly reduced. The same effect is observed for the average number of comparisons (E_{ff}).

In this case, two good configurations of the parameters [N,M] can be extracted from Table 6.4 (highlighted in grey), namely: *i*) [50,5], and *ii*) [100,10]. For these two points, the number of accounts broken is close to the total attacked, 85.57% and 92.78% respectively, while E_{ff} reaches a minimum (7,957 and 8,602, respectively) which is lower than the expected number of matchings required for a successful brute-force attack based on random forgeries (10,000 in average).

6.2.4.2. Analysis of α (Adaptation Coefficient)

For the two best configurations found, the effect of varying α on the performance of the attack is studied sweeping its value from 0 (only the global distribution G is taken into account), to 1

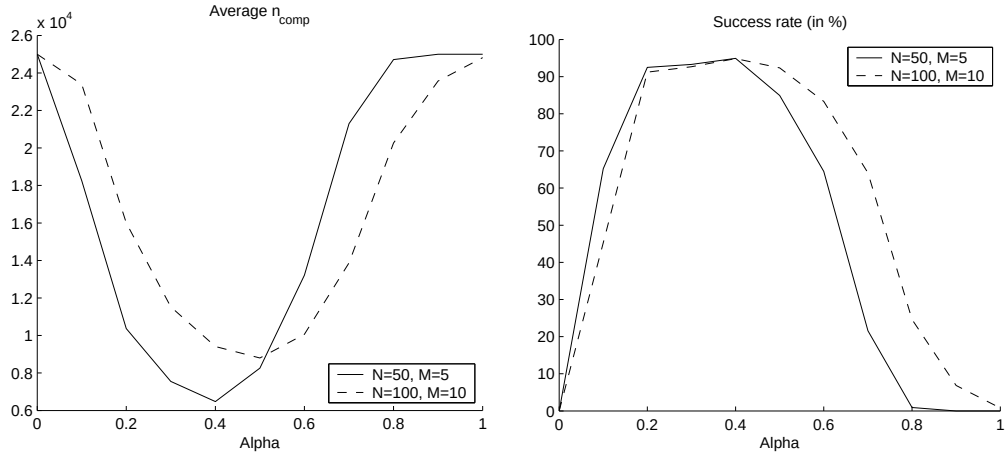


Figure 6.4: *Impact of α (adaptation coefficient) on the average number of comparisons needed for a successful attack (left), and on the success rate (right).*

(only the local distribution L affects the adaptation stage). The results are depicted in Fig. 6.4 where we show the evolution of E_{ff} (left), and the success rate (right), for increasing values of α and for the two configurations mentioned above.

It can be observed that for the point [50,5], the maximum number of accounts broken, and the minimum number of comparisons needed is reached for $\alpha = 0.4$ and both (maximum and minimum) are respectively greater and lower than those achieved with the values [100,10]. Thus, the best configuration of our algorithm is obtained for the values [N,M,α]=[50,5,0.4], which leads to 1,594 broken accounts (out of the 1,650 tested), and an average number of comparisons for a successful attack of 6,076, which represents almost half of the attempts required by a brute-force attack based on random forgeries. This value of α indicates that, for the best performance of the attack, the global and local distributions should be given approximately the same importance.

6.2.4.3. Analysis of Different Operating Points

Using the best configuration found, the algorithm was evaluated in two additional operating points of the system, namely (random forgeries): *i*) FRR=20%, FAR=0.05% (which implies a 2,000 attempt random brute-force attack), and *ii*) FRR=40%, FAR=0.0025%, where a random brute-force attack would need in average 40,000 matches before gaining access to the system. Results are given in Table 6.5 where the success rate over the total 1,650 accounts appears in plain text , and the average number of comparisons required by the bayesian hill-climbing attack in **bold**.

Smaller values of the FAR rate imply a bigger value of the threshold δ to be reached by the algorithm, which causes a rise in the average number of iterations required for a successful attack. Compared to brute-force attacks, this increase of the number of iterations is significantly lower, which entails that the hill-climbing algorithm is clearly better than brute-force for FR rates over 25% and less effective for smaller values of the FR rate. Even though for some operating points

	Operating points (in %)		
	FRR=20	FRR=30	FRR=40
Success rate (in %)	98.12	96.60	94.90
E_{ff}	**5,712**	**6,076**	**6,475**
E_{ff-bf} (random)	2,000 (FAR=0.05)	10,000 (FAR=0.01)	40,000 (FAR=0.0025)
E_{ff-bf} (skilled)	70 (FAR=1.42)	180 (FAR=0.55)	475 (FAR=0.21)

Table 6.5: *Results of the proposed algorithm for different points of operation considering random and skilled forgeries, for the best configuration found of the attacking algorithm (N=50, M=5, α = 0.4). The Success Rate is given in plain text (% over a total 1,650 attacked accounts), and E_{ff} in* ***bold****. The average number of matchings needed for a successful brute-force attack (E_{ff-bf}) is also given for reference, together with the FAR in brackets.*

the attacking strategy described in the present contribution is slower than a brute-force attack, it has to be emphasized that this latter approach would require, for instance in FRR=20%, a database of 2,000 different signatures, which is not straightforward.

As described in Sect. 6.2.3 the genuine scores for the skilled forgeries case are computed the same way as in the random approach, therefore the FR rates remain unaltered. This means that the threshold δ to be reached by the hill-climbing algorithm is the same in both cases (comparing the proposed hill-climbing to either random or skilled brute-force attack), thus, the performance measures (success rate and number of comparisons E_{ff}) do not change. Only the FAR values have to be recomputed and, as a result, the number of comparisons required by a successful skilled brute-force attack also change, being in the skilled forgery case: 70 for FRR=20%, 180 for FRR=30%, and 475 for FRR=40%. These are significantly smaller than the average number of iterations needed by the hill-climbing algorithm, however, it has to be taken into account that in this case, for instance in FRR=30%, we would need 180 different *skilled forgeries* of the same signer to access the system.

6.2.4.4. Graphical Analysis of the Attack

Two example executions of the attack, at the FR=30% operating point and using the best algorithm configuration (N=50, M=5, α=0.4), are shown in Fig. 6.5 (successful attack) and Fig. 6.6 (unsuccessful attack).

In Fig. 6.5 a signature which was successfully attacked in very few iterations (57), is depicted. The evolution of the best similarity score through all the iterations is shown in the top right plot, where we can see how the threshold δ (dashed line) is quickly reached. In the bottom row we show the evolution followed by the two dimensional Gaussian distributions of the first two parameters (left), and of the parameters 3 and 4 (right). A lighter color denotes a previous iteration (corresponding to the highlighted points of the top right plot) and the dashed ellipse is the target distribution of the attacked model. It can be observed that the adapted distribution

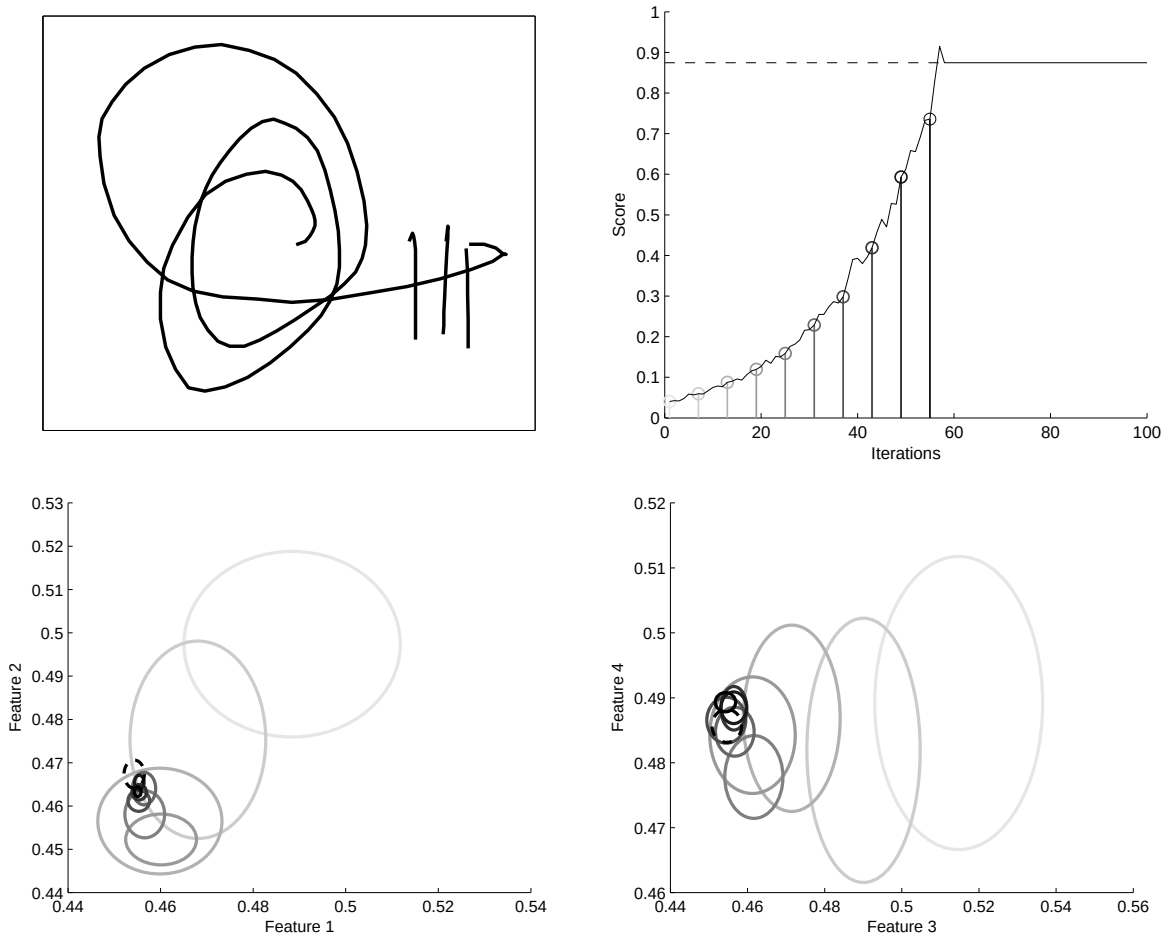


Figure 6.5: *Example execution of a successful attack, showing a sample signature of the attacked model (top left), evolution of the best score through the iterations (top right) with the threshold δ marked with a dashed line, and progress of the adapted distribution for the first two parameters (bottom left) and for the third and fourth parameters (bottom right). Lighter gray denotes a previous iteration, and the dashed ellipse the target model.*

rapidly converges towards the objective model.

A sample signature of one of the few models which was not bypassed with the proposed algorithm is given in Fig. 6.6. The curves depicted are analog to the those plotted in Fig 6.5. The curves in the bottom row are zoomed versions of the squares shown in the pictures above, in order to show how in this case the adapted distribution does not converge towards the target model (dashed).

6.3. Attack Protection

The results obtained in the previous sections have shown the vulnerability of the tested signature recognition systems to the studied attacks. Thus, effective countermeasures should be generated to detect and avoid these threats.

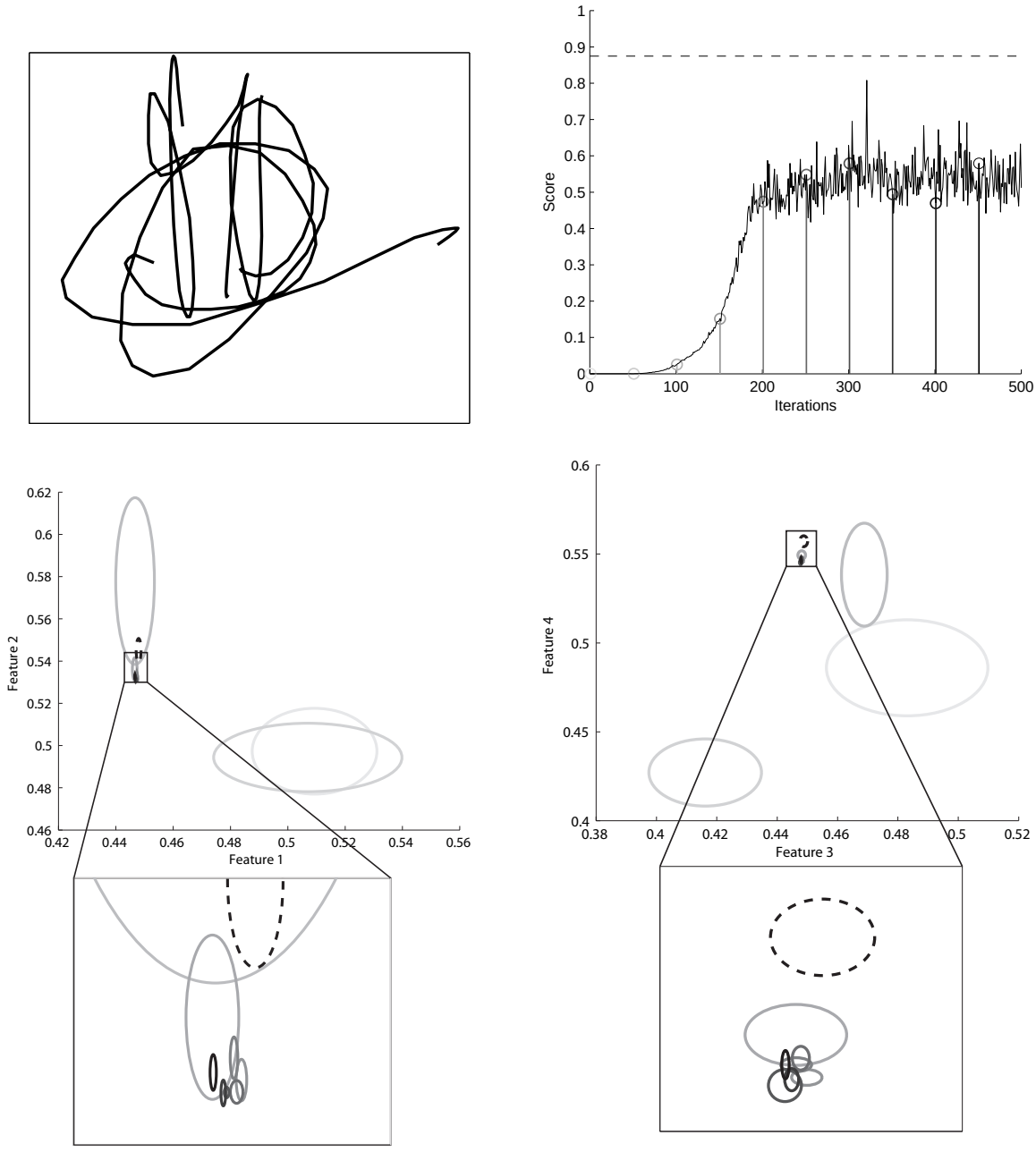


Figure 6.6: *Example execution of an unsuccessful attack. The images shown are analogue to those reported in Fig. 6.5. The bottom pictures are enlarged versions of the squares depicted in the above images.*

One common property to both analyzed attacks (brute-force and hill-climbing) is that they require a relatively large number of attempts before success. Hence, one possible countermeasure for such attacks is to restrict the number of consecutive unsuccessful attempts. However, this still leaves the system vulnerable to a spyware-based attack that interlaces its false attempts with the attempts by genuine users (successful attempts) and collects information to iterate

over a period of time. In the case of the hill climbing-based attacks, they could still be detected as the templates at the $i-th$ attempt (iteration) are generated from the $(i-1)th$ attempts (iterations) and are similar to each other. Hence, if we monitor all unsuccessful attempts for a particular targeted account within a fixed time interval, we will discover a pattern of similar faces with decreasing dissimilarity scores. Therefore, a continuous observation of unsuccessful match scores will help to detect hill climbing-based spyware attacks.

The previously cited countermeasures, although probably effective, are pure electronic algorithms applicable to all general security systems (based or not on biometric recognition) which fall out of the scope of the Thesis. In this chapter we will focus on the analysis of specific biometric-based countermeasures for the studied systems. In particular we consider two ways of minimizing the effects of the attacks:

- For the brute-force attack we reduce its success possibilities by enhancing the performance of the system (i.e., reducing its FAR implies increasing the number of attempts needed by the attack) through the use of synthetic duplicated samples of real signatures in the enrollment stage.

- In the case of the hill-climbing attack we study the possibility of using the most robust subset of features to the attack (out of the 100 feature set proposed by Fierrez-Aguilar *et al.* [2005b]), and we study its impact in the system's performance compared to the best performing feature subset.

6.3.1. Countermeasuring the Brute-Force Attack: Enrollment Enhancement

As has already been exposed, from a general security perspective, brute-force attacks might be avoided by controlling the number of unsuccessful access attempts to a certain account. However, from a pure biometric point of view, as these attacks are derived from the FAR of the system, the only way of minimizing their success chances is reducing the number of impostor access errors (i.e., reaching a lower FAR). In this section we study the efficiency of using synthetic duplicated samples at the enrollment stage in order to improve the performance of the system, thus making more difficult the success of an eventual brute force attack.

The synthetic duplicated samples generated from real signatures are produced following the novel algorithm described in Sect. 4.3.2. This way we analyze another potential application of the signature synthetic generation method, apart from the security evaluation assessment explored in Sect. 6.1.

The experimental framework (i.e., system and database) used in this countermeasure study is the same as the one employed in the vulnerability evaluation to the brute-force attack with synthetic signatures presented in Sect. 6.1. In this case, the dynamic signature data of the MCYT database are used to estimate the performance of the HMM-based signature recognition system for both random and skilled forgeries under different conditions of enrollment: using only real samples from the user, or complementing these data with synthetically generated signatures.

6.3.1.1. Experimental Protocol

The aim of the experiments is to find if adding synthetically generated samples (according to the model described in Chapter 4) to the real enrollment data of the clients, can improve the performance of signature recognition systems.

For this purpose we evaluate the state-of-the-art HMM-based system described in Sect. 6.1.2 under different scenarios for enrollment:

- Using only real samples to compute the enrollment model of each user.
- Complementing the real data of the user with synthetically generated samples.

In particular, we consider the cases of enrolling with 1, 5, and 20 real signatures, and enrolling with 1R+4S (1 Real, 4 Synthetic generated from that real signature), 1R+19S, and 4R+16S (4 synthetic samples produced from each of the 4 real samples). The experiments are carried out with and without taking into account the pressure information, and for both random and skilled forgeries.

In the two scenarios considered, skilled and random forgeries, the genuine scores are computed matching the enrollment data with the last 5 original signatures of the user (resulting in $330 \times 5 = 1,650$ similarity scores). The way to obtain the impostor scores differs between both scenarios: *i*) in the random forgeries case each user's model is compared with one signature of the remaining users (i.e., $330 \times 329 = 108,529$ impostor scores), and *ii*) when considering skilled forgeries the enrollment data of each user is matched with the 25 imitations of that same user (i.e., $330 \times 25 = 8,250$ impostor scores).

Different examples of the signatures (real and synthetic) used in the experiments are shown in Fig. 6.7. In the odd rows we depict six real samples of three different users in MCYT. The first two signatures correspond to the first acquisition set, while each of the remaining samples belong to each of the other four sets. In the even rows we depict six synthetic samples corresponding to the same users, generated from the real samples highlighted with a thicker frame following the method proposed in Chapter 4. The first two synthetic samples were produced applying intrasession variability, and the other four with intersession parameters.

6.3.1.2. Results

The results for the different cases considered (i.e., random and skilled forgeries, with and without the pressure information, and with different combinations of the enrollment data) are given in Table 6.6 in the form of Equal Error Rates (EER in %).

From the results obtained with no pressure information, we can see that in the case of having just one real signature for the enrollment of the client, we can improve the system performance in nearly 70% (from EER=23.84% to 7.87%) for the random forgeries scenario, and nearly 50% (from 32.15% to 16.24%) for the skilled forgeries case, by adding just four synthetic samples generated from that real signature. Furthermore, the EER obtained using

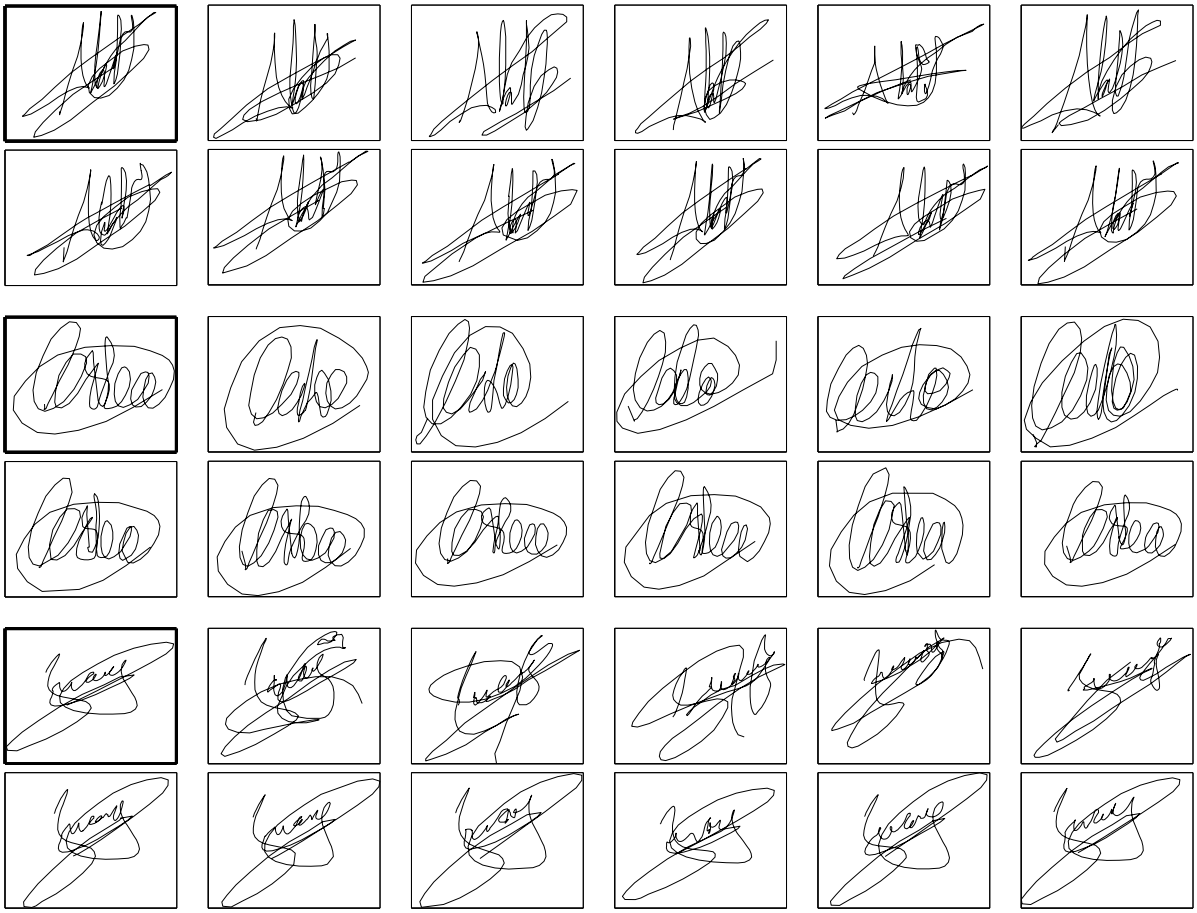


Figure 6.7: *Real (odd rows) and synthetic (even rows) samples of three different users of MCYT. The duplicated samples were generated from the real signature highlighted with a thicker frame.*

five real enrollment signatures from the same session (5.71% in random forgeries, and 14.57% for skilled) is comparable to that obtained using only one real sample complemented with four synthetic samples (7.87% and 16.24% for random and skilled forgeries, respectively).

We can also observe in Table 6.6, comparing the results 1R+4S with 1R+19S, that the EER gain introduced with an increasing number of synthetic samples generated from the same real signature saturates: EER of 7.87% with 1R+4S, to 7.11% with 1R+19S. This fact suggests that the variability modeled by the proposed approach, although very realistic as has been proven in the comparison between 1R, 5R and 1R+4S, is not enough to totally capture the natural signature variability (this is specially evident if we compare 20R with 1R+19S).

To avoid this EER gain saturation we tested the HMM-based recognition system in a 4R+16S enrollment data scenario, where four synthetic samples are generated from each of the four real samples (all taken from the first session as in the 5R case). The results are highlighted in **bold** in Table 6.6. We can observe that, even though we are just considering four real signatures, the introduction of additional synthetic samples for training drastically improves the system's EER compared to training with five real samples (over 60% improvement for random forgeries and

	Without pressure information. EER (%)					
	1R	5R	20R	1R + 4S	1R + 19S	4R + 16S
Random	23.85	5.71	1.81	7.87	7.11	**2.12**
Skilled	32.15	14.57	9.13	16.24	15.60	**10.25**

	With pressure information. EER (%)					
	1R	5R	20R	1R + 4S	1R + 19S	4R + 16S
Random	22.84	4.27	0.87	7.40	6.60	**1.17**
Skilled	31.03	10.97	5.57	16.07	15.60	**6.35**

Table 6.6: *EER for the HMM-based signature verification system, with and without considering the pressure information, for the random and skilled forgeries scenarios and for different cases of enrollment data. R stands for* **Real**, *and S for* **Synthetic**.

nearly 30% for skilled forgeries). The results are in this case (4R+16S) totally comparable to the (unrealistic) scenario where the enrolling data comprises 20 real samples (1.81% and 9.13% EER in 20R for random and skilled forgeries, against 2.12% and 10.25% EER for the same cases with 4R+16S).

Although the analysis of the results has been made for the case in which the pressure function was not considered, very similar conclusions can be drawn from the table where this information is taken into account.

6.3.2. Countermeasuring the Hill-Climbing Attack: Feature Selection

The results obtained by the Bayesian hill-climbing attack presented in Sect. 6.2.4 have shown that, in order to choose the best set of features possible for a particular signature recognition application, a trade-off between performance of the system and robustness to the attack has to be reached. In this section we analyze both aspects under the same experimental framework (i.e., system, database, and protocol) as the security evaluation described in Sect. 6.2, using the 100-feature set introduced by Fierrez-Aguilar *et al.* [2005b]. The SFFS feature selection algorithm proposed by Pudil *et al.* [1994] is used to search for the best performing feature subsets under the skilled and random forgeries scenarios, and to find the most robust subsets against the Bayesian hill-climbing algorithm used in the attacks. Comparative experiments are given resulting in some findings on the most/least discriminant features for the scenarios considered, and the groups of features which are best suited to enhance/decrease the robustness of the system.

The signatures in the MCYT database (used in the attack evaluation, see Sect. 6.2.3) are parameterized using the set of features described by Fierrez-Aguilar *et al.* [2005b] and shown in Table 6.3. We have divided this set of parameters into four different groups according to the signature information they contain (all the features assigned to each class are specified in Table 6.7), namely:

	FEATURES
Time	1,13,22,32,38,40–42,50,52,58-60,62,64,68,74,79,81–82,87-90,94,100
Speed	4–6,9–11,14,23,26,29,31,33,39,44–45,48,69,76,80,83,85,91-92,96
Direction	34,51,56-57,61,63,66,71–73,77-78,84,93,95,97–98,99
Geometry	2–3,7–8,12,15–21,24–25,27–28,30,35–37,43,46–47,49,53–55,65,67,70,75,86

Table 6.7: *Division of the feature set introduced in [Fierrez-Aguilar et al., 2005b] according to the signature information they contain.*

- **Time**: for instance feature 1 of the 100 parameter set, which indicates the signature total duration and is the most discriminant individual feature according to the ranking criterion followed in [Fierrez-Aguilar *et al.*, 2005b].
- **Speed and acceleration**: for instance features 5, 6, 9 and 10, which represent the standard deviation of the acceleration and the speed in both directions y and x.
- **Direction**: for instance feature 98, which indicates the signature initial direction angle Θ.
- **Geometry**: for instance features 8 and 12, which indicate the number of local maxima in x and y, respectively.

6.3.2.1. Experimental Protocol

In the experimental study we analyze several subsets selected from the original 100-feature set. Due to the high dimensionality of the problem, exhaustive search is not feasible (there are 2^{100} possibilities to be explored). The feature selection method used in the experiments is the SFFS algorithm introduced by Pudil *et al.* [1994], which has shown remarkable performance over other selection algorithms [Jain and Zongker, 1997]. Two types of search are carried out, one directed to find the best performing features, and the other one the most robust subset. Finally, a comparative study between both feature subsets is presented.

- **Performance experiments**. The aim of these experiments is to find in the original 100-feature set, a number of subsets (each of a different dimension) which minimize the EER of the signature recognition system.

  Two different scenarios are considered, *i*) skilled forgeries, in which the intruder tries to access the system imitating the original users's signature, and *ii*) random forgeries, where impostors try to access other's accounts using their own signature. In the first case, genuine scores are generated matching each of the five computed models of every user with the remaining 20 genuine signatures ($5 \times 20 \times 330 = 33,000$ genuine scores), while the impostor scores are computed comparing the 5 statistical models with all the 25 skilled forgeries,

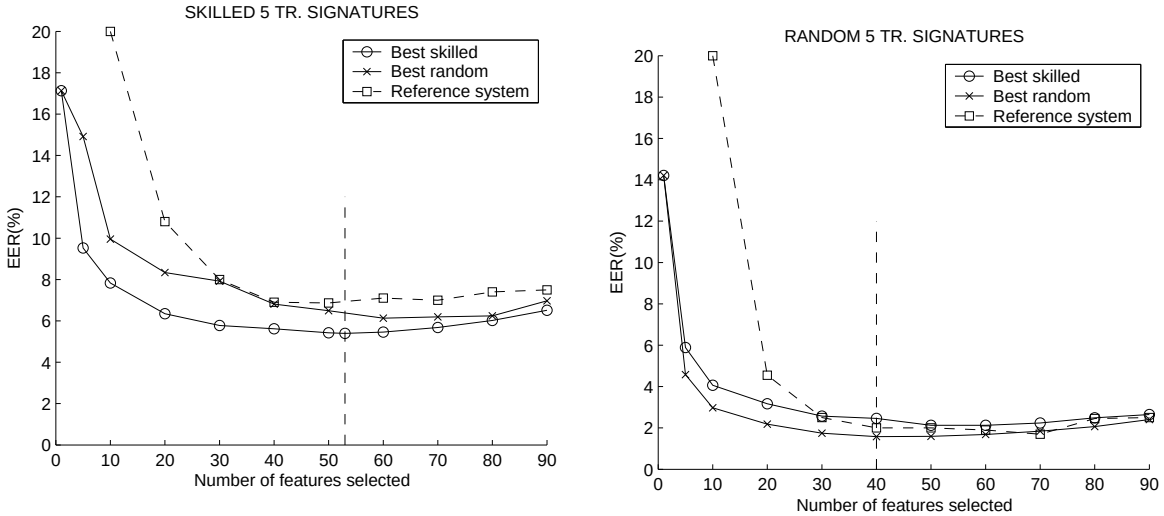


Figure 6.8: *System performance on the skilled (a), and random forgeries scenarios (b) using the SFFS feature subset selection maximizing the EER for skilled (circles), and random forgeries (crosses), compared to the reference system (squares) described in Fierrez-Aguilar et al. [2005b].*

resulting in $5 \times 25 \times 330 = 41,250$ impostor scores. In the random forgeries scenario, genuine scores are computed as above, while each statistical model is matched with one signature of the remaining users to generate the $5 \times 330 \times 329 = 542,850$ impostor scores.

These sets of genuine and impostor scores are then used to compute the EER of the system which is the criterion to be minimized in the SFFS algorithm.

- **Robustness experiments**. The objective of these experiments is to find a feature subset in the original 100 dimensional parameter space, which maximizes the robustness of the signature recognition system (i.e., minimizes the number of accounts bypassed) against the best configuration of the Bayesian hill-climbing algorithm found in Sect. 6.2.4.

  In order to perform the robustness analysis, the same protocol described in Sect. 6.2.3 is used: the database is divided into a training set (used to estimate the initial distribution G) and a test set comprising all the accounts being attacked, which are afterwards swapped (two-fold cross-validation). With this approach, a total $330 \times 5 = 1,650$ accounts are attacked.

  The number of broken accounts is used as the minimization criterion in the SFFS algorithm.

6.3.2.2. Results

- **Performance Experiments**. In Fig. 6.8, verification performance results for different subset sizes are given for the skilled forgeries scenario (a), and the random forgeries scenario (b). In circles we show the system performance when considering the subsets that perform

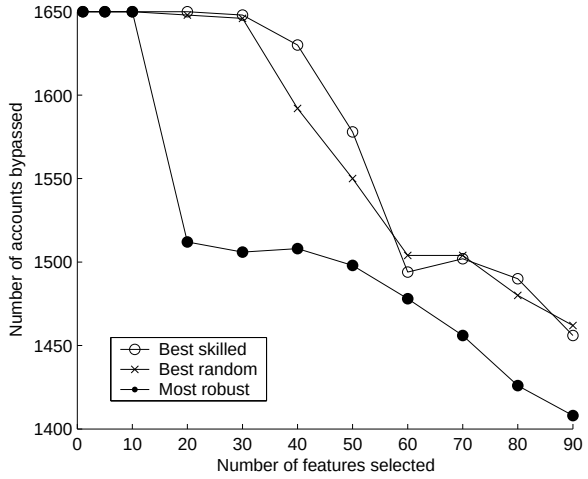


Figure 6.9: *Number of accounts bypassed for the skilled subsets (circles), the random subsets (crosses), and the feature subsets maximizing the robustness of the system (dots).*

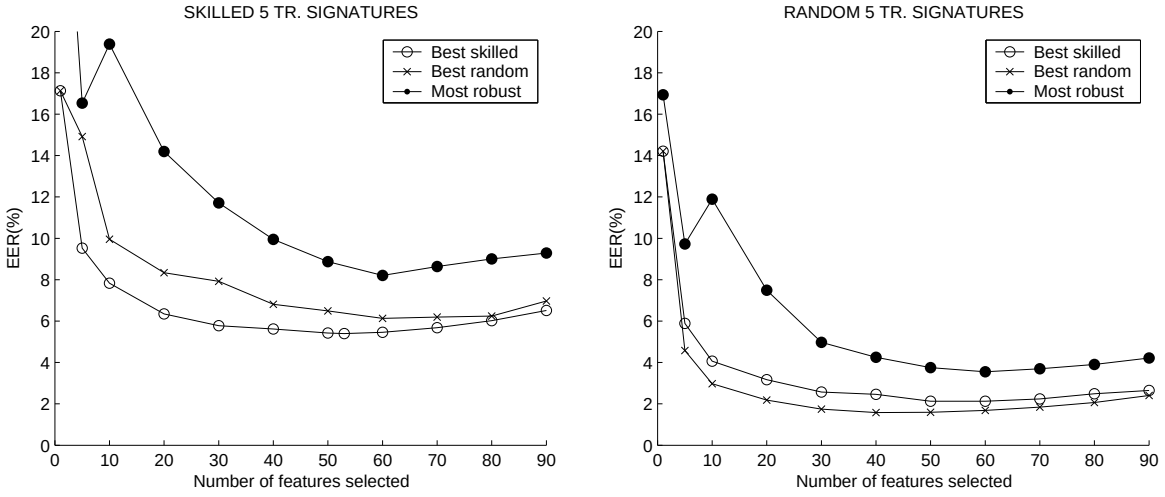
best when coping with skilled forgeries (from now on, skilled subsets), while the system EER for the best random subsets is depicted with crosses. These results are compared to the on-line signature recognition system based on global features described in Fierrez-Aguilar *et al.* [2005b] (using a Parzen Windows based matcher and a top ranked selection scheme of best individual features).

As expected, the skilled subsets perform the best in the skilled forgeries scenario, while the random subsets minimize the EER in the random forgeries scenario. In both cases the combination of the Mahalanobis distance matcher and the SFFS feature selection outperforms the verification scheme described in Fierrez-Aguilar *et al.* [2005b], with relative improvements in the verification performance against skilled forgeries around 22% using 50 features, and more than 60% for small set sizes (10 features).

The curse of dimensionality is clearly patent in both figures, where the minimum EER has been highlighted with a vertical dashed line. The best performance point is reached for a 53 dimensional subset in the case of skilled forgeries (EER=5.39%), and for a subset comprising 40 features in the random forgeries scenario (EER=1.58%).

- **Robustness Experiments**. In Fig. 6.9 we depict the number of accounts bypassed with the Bayesian hill-climbing attack using the skilled (circles) and random subsets (crosses), and the most robust feature subsets found by the SFFS algorithm. Although the robust subsets show a better behaviour against the attack, none of the parameter sets show a significantly decrease in the system vulnerability, with only 15% of the accounts resisting the attack in the best case.

- **Comparative Experiments**. The verification performance for the different subsets found in the previous experiments is shown in Fig. 6.10, both for the skilled (a), and the random



(a) (b)

Figure 6.10: *System performance on the skilled (a), and random scenarios (b) using the suboptimal subsets for skilled (circles) and random forgeries (crosses), and the subsets maximizing the system robustness (dots).*

forgeries scenarios (b). The circled solid line depicts the system EER for the skilled subsets, the solid line with crosses represents the EER for the random subsets, while the dots indicate the system verification performance when using the robust subsets. It is clear from the results shown in both figures that the use of more robust sets of features leads to a significant decrease in the verification performance of the system.

In Table 6.8, we show the number of features belonging to each of the groups described in Sect. 6.3.2, for the different subsets (skilled, random and robust) found in the previous experiments. From this analysis we can see that the most robust features are those regarding time information while the most vulnerable are the speed related features. On the other hand, the most discriminant parameters are those containing geometry information, and the least discriminant the direction related features.

6.4. Chapter Summary and Conclusions

In this chapter we have performed a security evaluation of on-line signature recognition systems to two different indirect attacks (the first one a brute-force attack carried out with synthetic signatures, and the second a hill-climbing attack), and we have proposed a biometric-based countermeasure for each of them.

In the case of the brute force attack carried out with synthetically generated signatures, the experiments were performed by attacking real signature models obtained with a HMM-based recognition system with synthetic signatures (which were produced with the novel synthetic signature generation method described in Chapter 4). The results show the feasibility of such a brute-force attack using synthetic samples.

	Time	Speed	Direct.	Geomet.
Skilled	2	2	0	1
Random	0	1	0	4
Robust	2	0	1	2

(a) Best 5-dimensional subsets.

	Time	Speed	Direct.	Geomet.
Skilled	3	3	0	4
Random	1	2	1	6
Robust	5	0	2	3

(b) Best 10-dimensional subsets.

	Time	Speed	Direct.	Geomet.
Skilled	6	5	7	12
Random	5	6	7	12
Robust	10	7	6	7

(c) Best 20-dimensional subsets.

Table 6.8: *Number of features for the skilled, random, and robust subsets belonging to each one of the four groups according to the signature information they contain.*

These results stress the importance of considering this type of vulnerability when designing practical biometric security applications and encourage us to further study effective countermeasures to prevent this type of attacks. With this objective we analyzed the feasibility of using synthetic duplicated samples in the enrollment stage in order to decrease the FAR of the system, and this way minimize the success chances of a brute-force attack. The results showed that the use of synthetically generated signatures (following the algorithm proposed in Sect. 4.3.2) drastically improves the system performance with gains of up to 70% in the EER for realistic testing scenarios. As a result, it is patent that adding synthetic data to the enrollment stage is a very powerful tool to enhance the performance of automatic signature recognition systems, decreasing this way the potential access capacity of brute-force attacks.

The hill-climbing attack algorithm based on Bayesian adaptation presented in Chapter 4 was evaluated on a feature-based signature verification system over the MCYT database. The experiments showed a very high efficiency of the hill-climbing algorithm, reaching a success rate for the attacks of over 95% for the best algorithm configuration found.

The performance of the hill-climbing attack was directly compared to that of a brute-force attack. The iterative algorithm needed less number of matchings than the brute-force approach in two out of the three operating points evaluated when considering random forgeries. Worth noting that the resources required by both approaches are not fully comparable. In order

to perform an efficient brute-force attack, the attacker must have a database of more than a thousand real different templates, while the hill-climbing approach does not need real templates to be successful.

As a way to countermeasure this security breach, we studied the possibility of selecting the most robust features to the attack and using them in signature recognition. With this objective the SFFS algorithm was used to search for the most robust parameter subset against the hill-climbing attack, and for the best performing subset. It was shown experimentally that the most discriminant parameters are those containing geometry information, and the least discriminant the direction related features. On the other hand, the most robust features are those regarding time information while the most vulnerable are the speed related features.

It was also found that, although a trade-off between performance and robustness should be reached, experiments show that the most robust subsets do not significantly decrease the system vulnerability compared to the best performing subsets, while the EER is clearly increased. Thus, it would be more advisable to search for parameter sets which improve the performance of the system, rather than those which enhance its robustness.

This chapter includes novel contributions in the evaluation of on-line signature recognition systems to the Bayesian hill-climbing attack and to a brute-force attack carried out with synthetic signatures, in the use of synthetic signatures for performance enhancement, and in the global parameters information-related findings regarding the robustness and efficiency of signature-based applications.

Chapter 7

Security Evaluation of Face-Based Authentication Systems

In this chapter we carry out a vulnerability evaluation of face verification systems against the Bayesian hill-climbing attack described in Sect. 4.1, and score quantization is analyzed as a possible countermeasure to reduce the effects of this threat.

The experimental results, as well as revealing certain security flaws of the studied systems (one based on PCA and the other working on GMMs), serve as validation of the novel Bayesian-based attacking approach. Together with the vulnerability study of on-line signature recognition systems, this security evaluation has given some important insight on the working of the hill-climbing method, proving its capacity of adaptation and its high efficiency breaking into different biometric systems, and its behaviour consistency through totally different working conditions.

The chapter is structured as follows. First (Sect. 7.1.1) the hill-climbing algorithm is briefly summarized (as it was already described in detail in Sect. 4.1), then we present the two face verification systems used in the evaluation (Sect. 7.1.2). The database and experimental protocol are explained in Sect. 7.1.3, while the results of the evaluation are given and discussed in Sect. 7.1.4. The experiments regarding the attack protection approache are described in Sect. 7.2. Finally the chapter summary and conclusions are presented in Sect. 7.3.

This chapter is based on the publications: Galbally *et al.* [2010, 2009g].

7.1. Indirect Hill-Climbing Attack

Some works studying the robustness of face recognition systems against indirect attacks can be found in the literature. Mohanty *et al.* [2007] presented a model-based attack which is capable of reconstructing the user's face images from the matching scores. The method has the strong constraint of needing a large number of real face images to initialize the algorithm.

Adler proposed a hill-climbing attack to a face recognition system in [Adler, 2004]. The input image, which is selected from an arbitrary set of real face images, is modified using an

independent set of eigenfaces (which makes it applicable only to face recognition systems) until the desired matching score is attained. This algorithm, which was adapted to be robust to score quantization [Adler, 2004], reported results on a PCA-based face recognition system and showed that after 4,000 iterations, a score corresponding to a very high similarity confidence (99.9%) was reached. The success rate of the attack (how many accounts were broken out of the total attacked), or the operating point of the system are not given, so the results are difficult to interpret or compare.

In the present chapter the Bayesian hill-climbing attack described in Sect. 4.1 is successfully applied to two automatic face recognition systems thus showing its big attacking potential and its ability to adapt to different biometric systems and matchers which use fixed length feature vectors of real numbers and delivering real similarity (or dissimilarity) scores. Two case studies are presented where several aspects of the algorithm are investigated. The first one examines the effectiveness of the technique on an Eigenface-based verification system while the second uses a more advanced Gaussian Mixture Model (GMM) Parts-based approach. For both case studies the experiments are conducted on the XM2VTS database and it is shown that the attack is able to bypass over 85% of the accounts attacked for the best configuration of the algorithm found. Furthermore, the hill-climbing approach is shown to be faster than a brute-force attack for all the operating points evaluated, as well as being capable of reconstructing the user's face image from the similarity scores, without using any real face images to initialize the algorithm. As a result, the proposed algorithm has vulnerability implications related to both security and privacy issues of the users.

7.1.1. Bayesian-Based Hill-Climbing Algorithm

The attacking algorithm, as the rest of hill-climbing approaches, is an iterative method that takes advantage of the scores returned by the system to modify a number of synthetically generated templates until a positive answer is attained. The main difference with other hill-climbing techniques is that in this case the modification scheme of the synthetic templates makes use of the Bayesian theory to adapt a general pool of users to the specificities of a local set of subjects which are closer to the attacked account. This fact allows the algorithm to be used in a straight forward manner against biometric systems working with fixed length feature vectors containing real numbers, and returning real similarity scores (regardless of the biometric trait, or the type of matcher being used). The algorithm, which is thoroughly described in Sect. 4.1, is defined by three main parameters: *i*) N, which defines the number of templates sampled from the general distribution, *ii*) M, which indicates the number of templates selected to compute in the local distribution, and *iii*) α, which is an adaptation coefficient taking values in the range [0,1].

7.1.2. Face Verification Systems

The Bayesian hill-climbing algorithm is used to test the robustness against this type of attacks of two different face verification systems, one based on Eigenfaces [Turk and Pentland, 1991], and a second using GMM with a part-based representation of the face [Cardinaux *et al.*, 2003]:

- **Eigenface-based system**. The face verification system used for the evaluation of the hill-climbing attack is based on the well known eigenfaces technique introduced by Turk and Pentland [1991]. This algorithm applies eigen-decomposition to the covariance matrix of a set of M vectorised training images $\mathbf{x}_i$. In statistical pattern recognition this technique is referred to as PCA [Fukunaga, 1990]. This method has become a *de facto* standard for face verification and was used to present initial results for the recent Face Recognition Grand Challenge evaluation [Phillips *et al.*, 2005].

  The first similarity measure used to compare PCA based features was the Euclidean distance, however several other similarity measures have been later proposed and studied [Yambor *et al.*, 2000].

  The evaluated system uses cropped face images of size 64×80 to train a PCA vector space where 80% of the variance is retained. This leads to a system where the original image space of 5120 dimensions is reduced to 91 dimensions ($K = 91$). Similarity scores are then computed in this PCA vector space using the standard correlation metric, $d(\mathbf{x}, \mathbf{y}) = 1 - [(\mathbf{x} - \mu_x) \cdot (\mathbf{y} - \mu_y)]/\sigma_x \sigma_y$, as it showed the best performance out of the tested similarity measures.

- **GMM Parts-based system**. The GMM Parts-based system used in the evaluation tesselates the 64×80 images into 8×8 blocks with a horizontal and vertical overlap of 4 pixels. This tessalation process results in 285 blocks and from each block a feature vector is obtained by applying the Discrete Cosine Transform (DCT); from the possible 64 DCT coefficients only the first 15 coefficients are retained ($K = 15$). The blocks are used to derive a world GMM Ω_w and a client GMM Ω_c [Cardinaux *et al.*, 2003]. Experimentation found that using a 512 mixture component GMM gave optimal results.

  When performing a query, or match, the average score of the 285 blocks from the input image are used. The DCT feature vector from each block v_i (where $i = 1 \ldots 285$) is matched to both Ω_w and Ω_c to produce a log-likelihood score. These scores are then combined using the log-likelihood ratio, $S_{llr,j} = log[P(v_j|\Omega_c)] - log[P(v_j|\Omega_w)]$, and the average of these scores is used as the final score, $S_{GMM} = \frac{1}{285} \sum_{j=1}^{285} S_{llr,j}$. This means that the query template can be considered to be a feature matrix formed by 285 fifteen dimensional vectors (representing each of the blocks in the image).

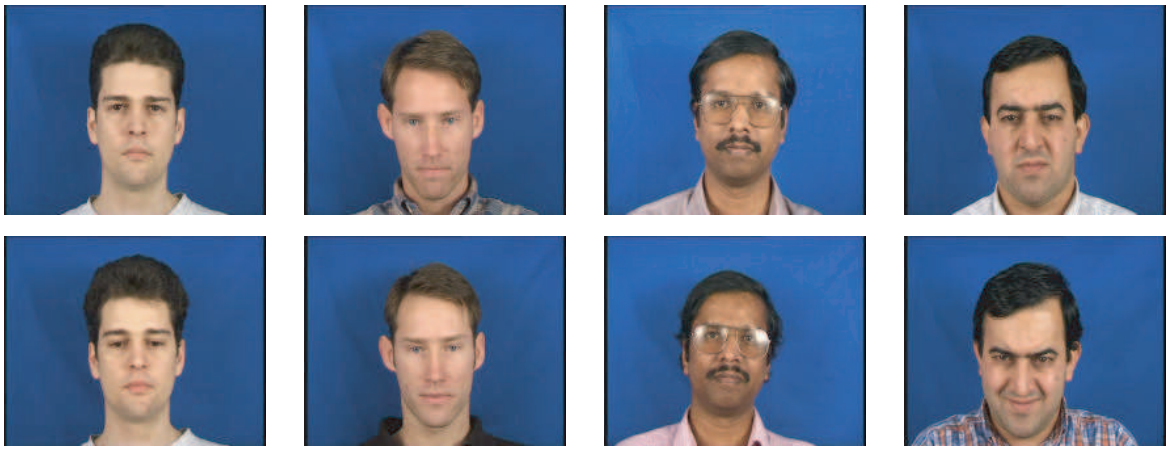


Figure 7.1: *Examples of the images that can be found in XM2VTS.*

7.1.3. Database and Experimental Protocol

The experiments are carried out on the XM2VTS face database [Messer *et al.*, 1999], comprising 295 users. The database was acquired in four time-spaced capture sessions in which two different face images of each client were taken under controlled conditions (pose and illumination) to complete the total $295 \times 8 = 2,360$ samples of the database. Two evaluation protocols are defined for this database, the Lausanne Protocol 1 and 2 (LP1 and LP2). In Fig. 7.1 some examples of images that can be found in the XM2VTS are shown.

7.1.3.1. Performance Evaluation

The performance of the evaluated systems is computed based on the LP2 protocol. This protocol is chosen as the training and evaluation data are drawn from independent capture sessions.

According to LP2 the database is divided into: *i*) a training set comprising the samples of the two first sessions of 200 clients (used to compute the PCA transformation matrix, and the world GMM Ω_w, respectively), and *ii*) a test set formed by the fourth session images of the previous 200 users (used to compute the client scores), and all the 8 images of 70 different users with which the impostor scores are calculated. As a result of using the same subjects for PCA training and client enrollment, the system performance is optimistically biased, and therefore harder to attack than in a practical situation (in which the enrolled clients may not have been used for PCA training). This means that the results presented in this paper are a conservative estimate of the attack's success rate. In Fig. 7.3 a general diagram showing the LP2 evaluation protocol is given (although defined by LP2, the development set was not used in our experiments).

In the case of the Eigenface-based system, the final score given by the system is the average of the p scores obtained after matching the input vector to the p templates of the attacked client model $\mathcal{C}$, while in the GMM system the p templates are used to estimate the parameters of the

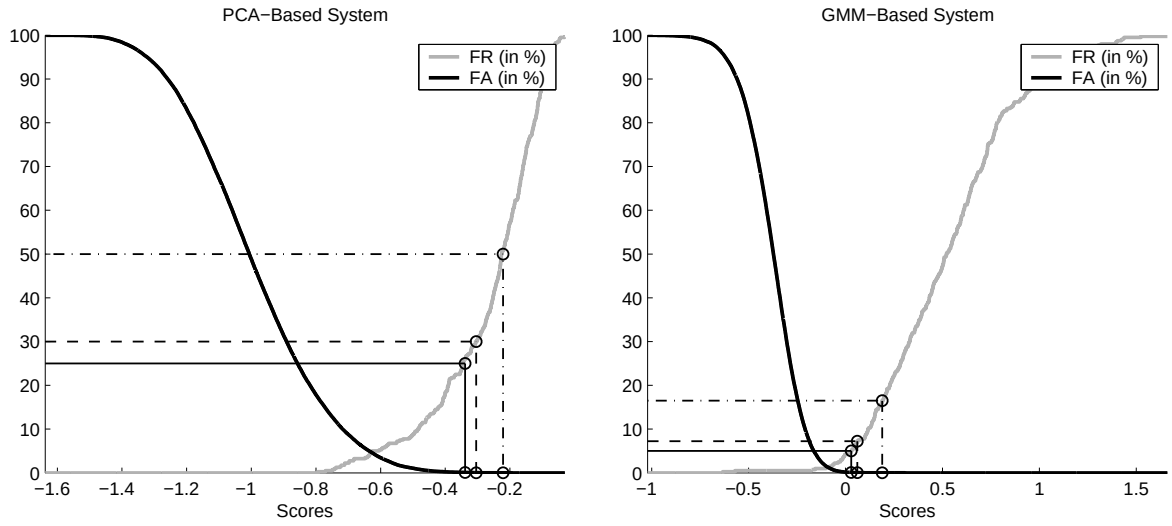


Figure 7.2: *FAR and FRR curves for the Eigenface-based system (left) and the GMM-based system (right).*

		XM2VTS DB (295 Users)		
Session	Sample	200 Users	25 Users	70 Users
1	1	Training	Development (Impostors)	Test (Impostors)
2	1			
3	1	Development (Clients)		
4	1	Test (Clients)		

Figure 7.3: *Diagram showing the partitioning of the XM2VTS database according to the LP2 protocol (which was used in the performance evaluation of the present work).*

client GMM (Ω_c). In Fig. 7.2 we can see the system False Acceptance Rate (FAR) and False Rejection Rate (FRR) curves for the Eigenface-based system (left) and for the GMM system (right), using the described protocol with $p = 4$ enrollment templates. The Eigenface-based system presents an Equal Error Rate (EER) of 4.71%, while the GMM system shows a better performance with a 1.24% EER. The three operating points where the hill-climbing algorithm is evaluated (corresponding to FAR=0.1%, FAR=0.05%, and FAR=0.01%) are also highlighted. These operating points correspond to a low, medium, and high security application according to [ANSI-NIST, 2001].

7.1.3.2. Experimental Protocol for the Attacks

In order to generate the user accounts to be attacked using the hill-climbing algorithm, we used the train set defined by LP2 (i.e., samples corresponding to the first 2 sessions of 200 users).

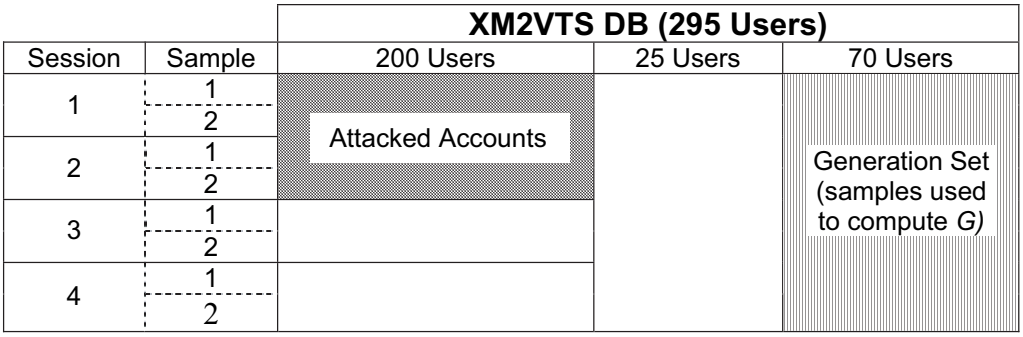


Figure 7.4: *Diagram showing the partitioning of the XM2VTS database followed in the attacks protocol.*

The initial K-variate distribution G of the algorithm, was estimated using part or all the samples (depending on the experiment) from the impostors in the test set (70 users) defined in LP2 (referred to in the rest of the work as generation set). This way, there is no overlap between the attacked set of users (200 accounts), and the subjects used to initialize the algorithm, which could lead to biased results on the success rate (SR) of the attack. In Fig. 7.4 the partitioning of the database used for the attacks is shown.

7.1.4. Results

The goal of the experiments is to study the vulnerability of automatic face recognition systems to hill-climbing attacks. This is achieved by examining the success rate (SR) and efficiency (E_{ff}) of the Bayesian-based hill-climbing algorithm in attacking two different face recognition systems at several operating points (see Sect. 3.2 for definitions of SR and $E_f f$). By performing these attacks it will also be studied the ability of the Bayesian-based hill-climbing algorithm to adapt, not only to different matchers, but also to other biometric traits (it was already shown to be successful attacking an on-line signature verification system in Chapter 6).

Two case studies are presented for the attacks on the two separate face verification systems. The first case study examines the effectiveness of the Bayesian-based hill-climbing attack on the Eigenface-based system (Sect. 7.1.4.1). The second study uses the previously found optimal configuration to attack the GMM Parts-based system (Sect. 7.1.4.2). By using the same optimal configuration between studies we can determine if the performance of the attack is highly dependent on the values of the parameters selected.

7.1.4.1. Case study 1: Attacking an Eigenface-Based Face Verification System

In the first set of experiments, we follow an analogue protocol to that used in the evaluation described in Sect. 6.2 of an on-line signature verification system to the Bayesian hill-climbing attack. This way, we study the effect of varying the three parameters of the algorithm (N, M, and α) on the SR of the attack over the Eigenface-based system described in Sect. 7.1.2. The objective is to reach an optimal configuration where the number of broken accounts is maximized,

		N				
		10 (2500)	25 (1000)	50 (500)	100 (250)	200 (125)
M	3	84.5 **5,162**	86.0 **4,413**	86.0 **4,669**	86.0 **5,226**	86.0 **6,296**
	5	81.5 **5,796**	86.0 **4,275**	86.0 **4,512**	86.0 **5,022**	86.0 **5,988**
	10		85.5 **4,534**	86.0 **4,540**	86.0 **5,019**	86.0 **5,941**
	25			86.0 **5,213**	86.0 **5,379**	86.0 **6,256**
	50				86.0 **6,455**	86.0 **6,934**
	100					86.0 **8,954**

Table 7.1: *Success Rate (in %) of the hill-climbing attack for increasing values of N (number of sampled points) and M (best ranked points). The maximum number of iterations allowed is given in brackets. The SR appears in plain text, while the average number of comparisons needed to break an account (Efficiency, E_{ff}) appears in* ***bold****. The best configuration of parameters N and M is highlighted in grey.*

while minimizing the average number of comparisons (E_{ff}) needed to reach the fixed threshold δ. As presented in the description of the algorithm in Sect. 4.1, the above mentioned parameters denote: N the number of sampled points of the adapted distribution at a given iteration, M the number of top ranked samples used at each iteration to adapt the global distribution, and α is an adaptation coefficient which varies from $[0 \dots 1]$.

The importance of the initial distribution G is also examined by evaluating the attack performance when a smaller number of real samples is used to compute G. The case where G is randomly selected is also examined.

As was done in the on-line signature evaluation experiments (Sect. 6.2.4), when presenting results the brute-force approach is used to provide a baseline to compare with the hill-climbing algorithm. We compare E_{ff} with the number of matchings necessary for a successful brute-force attack at the operating point under consideration ($E_{ff-bf} = 1/\text{FAR}$). However, again it should be noticed that the proposed hill-climbing algorithm and a brute-force attack are not fully comparable as the latter requires much greater resources (e.g., a database of thousands of samples).

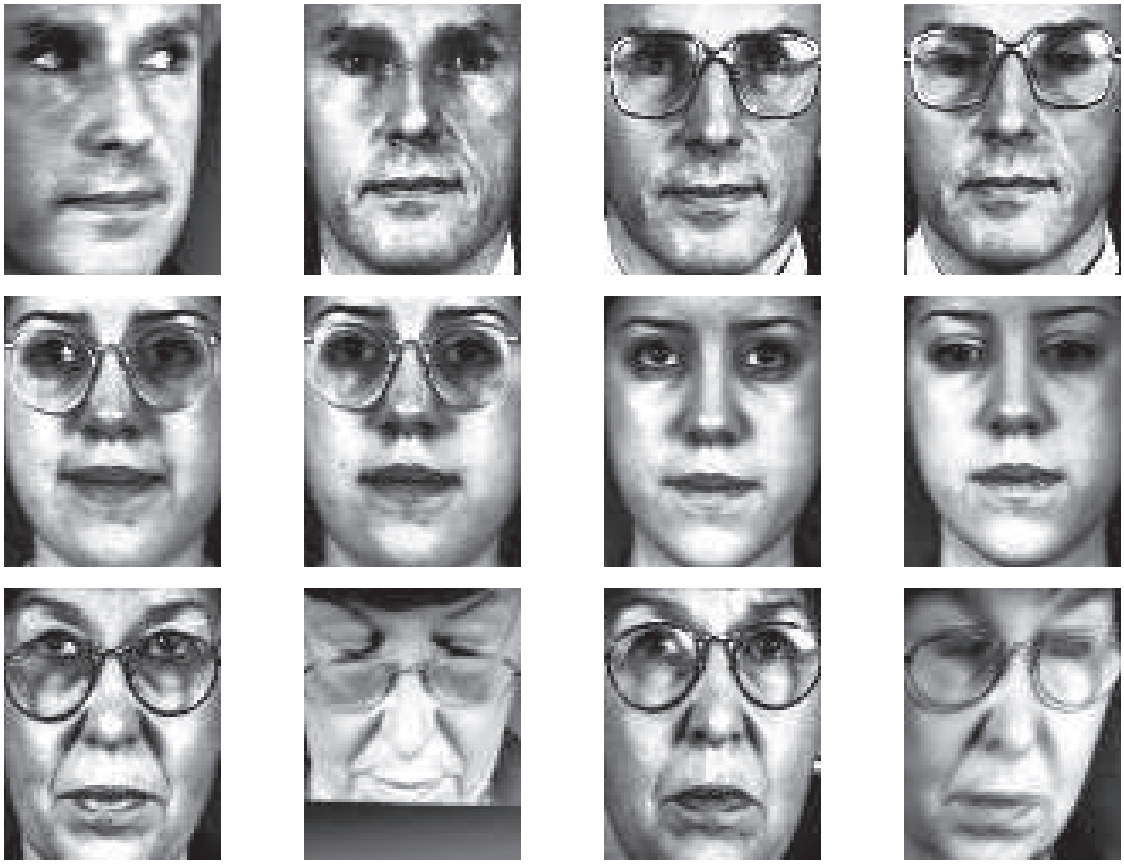


Figure 7.5: *The four enrollment images (columns) constituting the model of three of the unbroken accounts (rows).*

Analysis of N and M (sampled and retained points).

For the initial evaluation of the algorithm an operating point of FAR=0.01% was fixed (this FAR leads to an FRR of 50%). This FAR implies that an eventual brute-force attack would be successful, on average, after 10,000 comparisons. Given this threshold the algorithm was executed for different values of N and M (fixing $\alpha = 0.5$) and the results are given in Table 7.1. The maximum number of iterations (n_{it}) allowed for the algorithm appears in brackets. This value changes according to N in order to maintain constant the maximum number of comparisons permitted ($E_{ff} = N \cdot n_{it}$). In plain text we show the success rate of the attack (in % over the total 200 accounts tested), while the average number of comparisons needed for a successful attack is represented in **bold**.

Examining Table 7.1 the optimal configuration for these parameters is $[N = 25, M = 5]$ (highlighted in grey). For this point, the number of accounts broken is maximized (86%) and E_{ff} is minimized (4,275). This minimum represents less than half of the expected number of matchings required for a successful brute-force attack ($E_{ff-bf} = 1/\text{FAR} = 10,000$).

Further analysis of the results indicate that selecting the best possible N has a deeper impact in the speed of the attack than choosing a good value for M. This is because N represents the

α	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
SR(%)	0	84.5	86.0	86.0	86.0	86.0	86.0	81.0	71.5	51.0	20.0
E_{ff}	**25,000**	**6,468**	**5,121**	**4,617**	**4,381**	**4,275**	**4,380**	**4,990**	**7,901**	**10,404**	**14,154**

Table 7.2: *Success Rate (in %) of the hill-climbing attack for increasing values of α and for $[N, M] = [25, 5]$. The SR appears in plain text, while E_{ff} appears in **bold**. The optimal value of α is highlighted in grey.*

number of scores produced at each iteration of the attack and consequently has a direct impact on the number of comparisons performed E_{ff}.

It can also be drawn from the results presented in Table 7.1 that choosing a value such that $N > M$ provides a better efficiency (in terms of E_{ff}) than if $M \simeq N$ (the sub-sampling of the local distribution is too general and so the speed of the attack is reduced) or $N \gg M$ (the sub-sampling of the local distribution is too specific which again reduces the speed of the attack). These results are analogue to those obtained in the evaluation to the attack of an on-line signature verification system presented in Sect. 6.2, which suggests that the algorithm behaviour is consistent regardless of the matcher or biometric trait being attacked.

Irrespective of how N and M are optimized the number of accounts broken by the attack remains stable. For almost all the configurations evaluated 86% of the accounts were broken (172 out of a total of 200). Further examining this result it was found that the 28 clients who remain robust to the attack are the same in all cases.

To search for an explanation, the 28 unbroken client models (comprising the four images of the first two database sessions) were matched to the other four images of the user (those corresponding to sessions three and four). It was found that none of the client models produced a score high enough to enter the system, which means that these 28 clients would not be suitable for face recognition under the considered system working at the selected operating point. We can then conclude that the attack successfully broke all the models that would be used in a real application. In Fig. 7.5 the enrollment images which form three of the resistant accounts are shown. In all cases we can observe a great variance among the samples of a given model (glasses/not glasses, different poses, and blurred images).

Analysis of α (adaptation coefficient)

As in the on-line signature evaluation, for the optimal configuration of N and M the effect of varying α on the performance of the attack is studied. This parameter is changed from 0 (only the global distribution G is taken into account) to 1 (only the local distribution L affects the adaptation stage). The results are presented in Table. 7.2 where the success rate of the attack appears in plain text (%), while the average number of comparisons needed for a successful attack is shown in **bold**.

From Table. 7.2 it can be seen that the optimal point is $\alpha = 0.5$ (where both the number of accounts broken is maximized, and the number of comparisons needed minimized). This

Number of real samples used to compute G							
5	10	35	70	140	280	560	Random (μ=0,σ=1)
86.0 **4,353**	86.0 **4,307**	86.0 **4,287**	86.0 **4,283**	86.0 **4,279**	86.0 **4,285**	86.0 **4,281**	86.0 **4,492**

Table 7.3: *Success Rate (in %) of the hill-climbing attack for increasing number of samples used to compute the initial distribution G, and for $[N, M, \alpha] = [25, 5, 0.5]$. The SR appears in plain text, while E_{ff} appears in* ***bold****.*

corresponds to the case where both the global and local distribution are given approximately the same importance. As in the previous experiment, it can be noticed that 14% percent of the accounts (the same 28 clients as in the previous experiments) is never bypassed as a consequence of the large user intra-variability.

As in the case of the analysis of N and M, the result for α is very similar to the one obtained in the on-line signature evaluation where a best success rate of the attack was reached for $\alpha = 0.4$. Again, this corroborates the consistency of the algorithm and indicates that, irrespective of the system under attack, the best configuration of the approach should be one where $N > M$ (and not $N \gg M$ or $N \simeq M$), and $\alpha \simeq 0.5$.

Analysis of the initial distribution G

In the previous experiments the K-variate initial distribution G was computed using the two images from the first session of the 70 users comprised in the generation set (see Fig. 7.4). In this section the effect of estimating G using different number of samples, and a random initialization of G, are both explored.

In Table 7.3 we show how the performance of the attack varies depending on the number of samples used to estimate this distribution G, for the best configuration of the attack $[N, M, \alpha] = [25, 5, 0.5]$. As the generation set comprises 70 users, for numbers of images smaller than 70, one sample per subject (randomly selected from the generation set) was used, while for 70 images or larger numbers, 1, 2, 4, and 8 samples from each subject are used. In all cases, the resulting multivariate gaussian G results in $[-0.8 < \mu_i < 0.5]$ and $[0.2 < \sigma_i < 18]$, where μ_i and σ_i are respectively the mean and variance of the i-th dimension, with $i = 1 \ldots 91$.

No real samples are used in the random initialization, where G corresponds to a multivariate Gaussian of zero mean and variance one.

From the results shown in Table 7.3 we can see that the number of samples used to compute the initial distribution G has little effect on the performance of the attack. In fact, the experiment shows that the algorithm can be successfully run starting from a general initial distribution G of zero mean and unit variance. This means that an attacker would not need to have any real face images to carry out the attack (on the studied system), which is in stark contrast to a brute

	Operating points (in %)		
	FAR=0.1,FRR=25	FAR=0.05,FRR=30	FAR=0.01,FRR=50
Success Rate (in %)	99.0	98.5	86.0
E_{ff}	**840**	**1,068**	**4,492**
E_{ff-bf}	1,000	2,000	10,000

Table 7.4: *Results of the attack for different points of operation and the best configuration found of the attacking algorithm ($N = 25$, $M = 5$, $\alpha = 0.5$). The SR is given in plain text (in percentage, over the total 200 attacked accounts), and E_{ff} in* ***bold****. The average number of matchings needed for a successful brute-force attack (E_{ff-bf}) is also given for reference.*

force attack which requires a large database to perform a successful attack.

Analysis of different operating points

Using the best configuration $[N, M, \alpha] = [25, 5, 0.5]$ and starting from a general initial distribution G of zero mean and unit variance, the algorithm was evaluated in two additional operating points of the system (see Fig. 7.2). The two additional operating points are: *i*) FAR=0.05%, which implies $E_{ff-bf} = 2,000$ and leads to FRR=30%, and *ii*) FAR=0.1%, which implies $E_{ff-bf} = 1,000$ and leads to FRR=25%. Results are given in Table 7.4.

Smaller values of the FAR imply a bigger value of the threshold δ to be reached by the algorithm, which causes a rise in the average number of iterations required for a successful attack. However, the results in Table 7.4 demonstrate that this technique is effective across multiple operating points. In all cases the number of comparisons needed to break the system (using the Bayesian hill-climbing attack) is lower than that of a brute force attack. The hill-climbing approach has the added advantage that it does not need any real face images to initialize the attack.

Graphical analysis of the attack

In order to illustrate graphically how the hill-climbing algorithm works we repeated the attack for the best configuration $[N,M,\alpha]=[25,5,0.5]$ at a high security operating point (FAR=0.01%). To visualize the hill climbing attack we present the results using the Euclidean distance as the similarity measure. This metric provides very similar results to those obtained with the standard correlation metric (in terms of the SR of the attack and E_{ff}), however, due to the different characteristics of both measures (the standard correlation is angle based) the Euclidean distance provides a more intuitive visual insight into the effect of the hill-climbing attack, as can be observed in Figs. 7.6 and 7.7.

In Figs. 7.6 and 7.7 two examples of broken and non-broken accounts (corresponding to two of the users presented in Fig. 7.5) are shown. For each of the examples the evolution of the score through the iterations of the algorithm is depicted. Highlighted in each example are

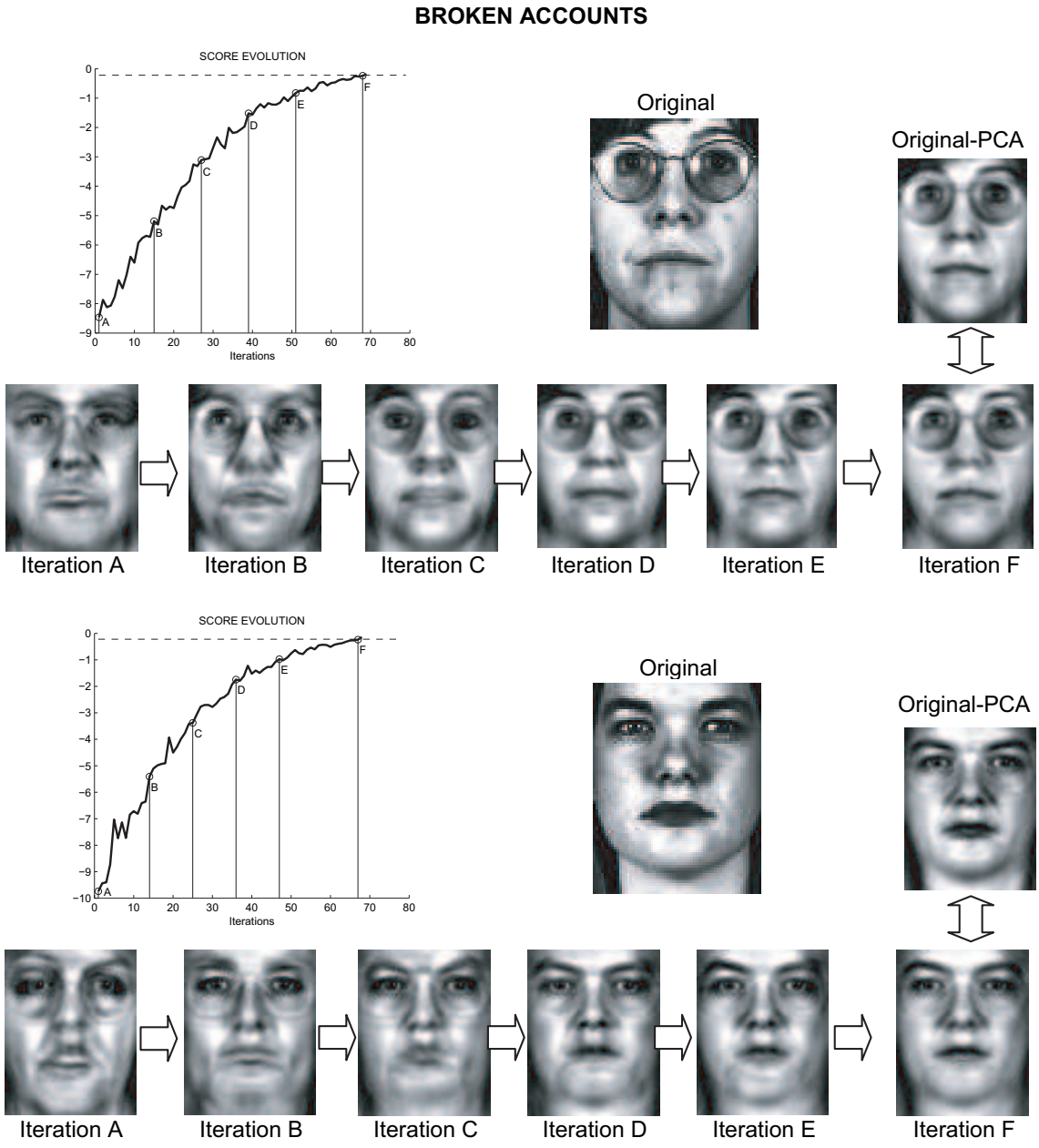


Figure 7.6: *Examples of the evolution of the score and the synthetic eigenfaces through the iterations of the attack for broken and accounts. The dashed line represents the objective threshold.*

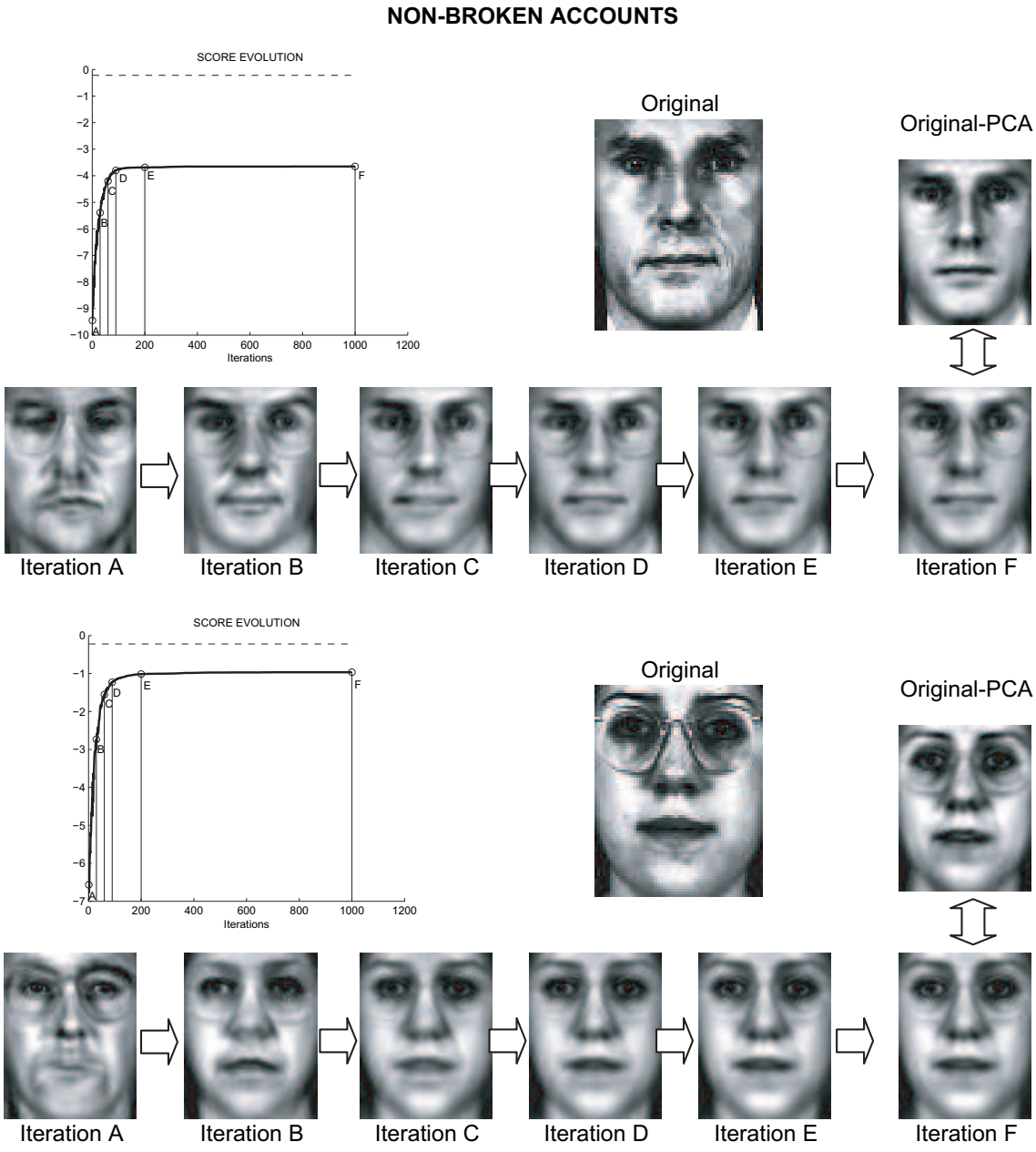


Figure 7.7: *Examples of the evolution of the score and the synthetic eigenfaces through the iterations of the attack for non-broken and accounts. The dashed line represents the objective threshold.*

six points, including the first and the last one, of the iterative process marked with letters A through to F. The dashed line represents the objective value to be reached (i.e., the threshold δ). The two upper faces correspond to one of the original images of the attacked user and the reconstructed image of a K-dimensional eigenface template (where part of the information has been lost because of the dimensionality reduction). The sequence of the six faces below correspond to the feature vectors that produced each of the six scores marked with A through to F. The first point A is produced by randomly sampling the estimated general distribution $\mathcal{G}$ and the last point F represents the image which is able to break the system. These two figures show that the algorithm can be used not only as a break-in strategy but also as a method to accurately reconstruct the client's face image (with the privacy issues that this entails).

In Figs. 7.6 and 7.7 we can observe that the hill-climbing algorithm starts from a totally random face which is iteratively modified to make it resemble as much as possible to the PCA projection of the attacked user´s face labeled as "Original-PCA" (this effect cannot be observed as clear when using the standard correlation metric). In both cases (broken and non-broken accounts) the attack successfully finds a final image which is very similar to the objective face, however, in the case of the accounts resistant to the attack, the threshold is not reached as a consequence of the large user intra-variability, which leads to low scores even when compared with images of the same client.

7.1.4.2. Case study 2: Attacking a GMM Face Verification System

In order to attack the GMM-based system, the best configuration of the algorithm found in the previous experiments was used ($N = 25$, $M = 5$, and $\alpha = 0.5$). The default operating point to attack the system corresponds to FAR=0.01% (this means that a brute force attack would need on average to be successful $E_{ff-bf} = 10,000$ matchings), which leads to FRR=16%.

Using the optimal parameters ($N = 25$, $M = 5$, and $\alpha = 0.5$) from the previous will permit to see if the attack configuration is highly dependent on the matcher tested, or if, on the contrary, a good set of parameter values can perform successfully on different systems.

Two different approaches to the problem of attacking the GMM system are tested in these experiments:

- **Single block search**. This attack searches for one block to break the client's account. As explained in Sect. 7.1.2, the client score Sc is computed by taking the average score from all the blocks, therefore, if we are able to find one good matching block and replicate it for all the other blocks we should be able to produce a score high enough to be granted access. With these premises, this attack uses the Bayesian adaptation to search for one 15 dimensional vector which is repeated 285 times in order to produce the final synthetic template capable of breaking the system.

- **Multiple block search**. In this case we search for a unique set of vectors which are capable of breaking into the client's account. Like the single block search this attack undertakes a search in a 15 dimensional space, however, in this case 285 random vectors

	Number of real samples used to compute G						
	5	10	35	70	140	280	560
Sing. Block Search	100 **25**	100 **25**	100 **25**	100 **25**	100 **25**	100 **25**	100 **25**
Mult. Block Search	100 **1,031**	100 **1,025**	100 **1,631**	100 **1,514**	99.5 **1,328**	100 **1,293**	100 **1,254**

Table 7.5: *Success Rate (in %) of the hill-climbing attack under single (top) and multiple (bottom) block search, for increasing number of real samples used to compute the initial distribution G. The SR appears in plain text, while the average number of comparisons needed to break an account (Efficiency, E_{ff}) appears in* ***bold****.*

(of 15 dimensions) are sampled to generate the synthetic client template. As before, when performing the Bayesian adaptation the average of the M best synthetic templates is used to produce the vectors $\boldsymbol{\mu}_L$ and $\boldsymbol{\sigma}_L$. The fact that we are looking for a greater number of vectors than in the single block search makes the multiple block search more difficult to accomplish and also more difficult to detect.

Experiments starting from an average initial distribution G

For these experiments we computed an initial distribution G representing the average block (i.e., mean and average of the 15 dimensional blocks found in several images). The distribution was computed using a different number of images selected from the generation set defined in the attack protocol (see Fig. 7.4). For numbers of images smaller than 70, one sample per user (randomly selected) is picked, while for larger numbers (140, 280, and 560) 2, 4, and 8 samples per subject are selected respectively. In Table 7.5 the results for the single and multiple block search approaches are shown.

For the single block search all the accounts are broken at the first iteration of the attack (at each iteration 25 comparisons are computed). This means that the Bayesian adaptation hill-climbing algorithm is not necessary and that the system can be broken using synthetic templates built replicating 285 times a random average block estimated using as few as 5 images. This serious security flaw can be countermeasured by checking if all the blocks in the template trying to access the system are different.

The multiple block search attack has almost a 100% success rate regardless of the number of images used to compute the initial distribution G. However, for this attack we would need, on average, around 1,200 comparisons (corresponding to 55 iterations of the attack) to break the system. This represents less than one sixth of the matchings required by a successful brute force attack ($E_{ff-bf}10,000$) with the added advantage that just 5 real face images are needed to perform the hill-climbing attack. Although the multiple block search is slower than the single block search approach, in this case countermeasuring the attack is significantly more difficult as

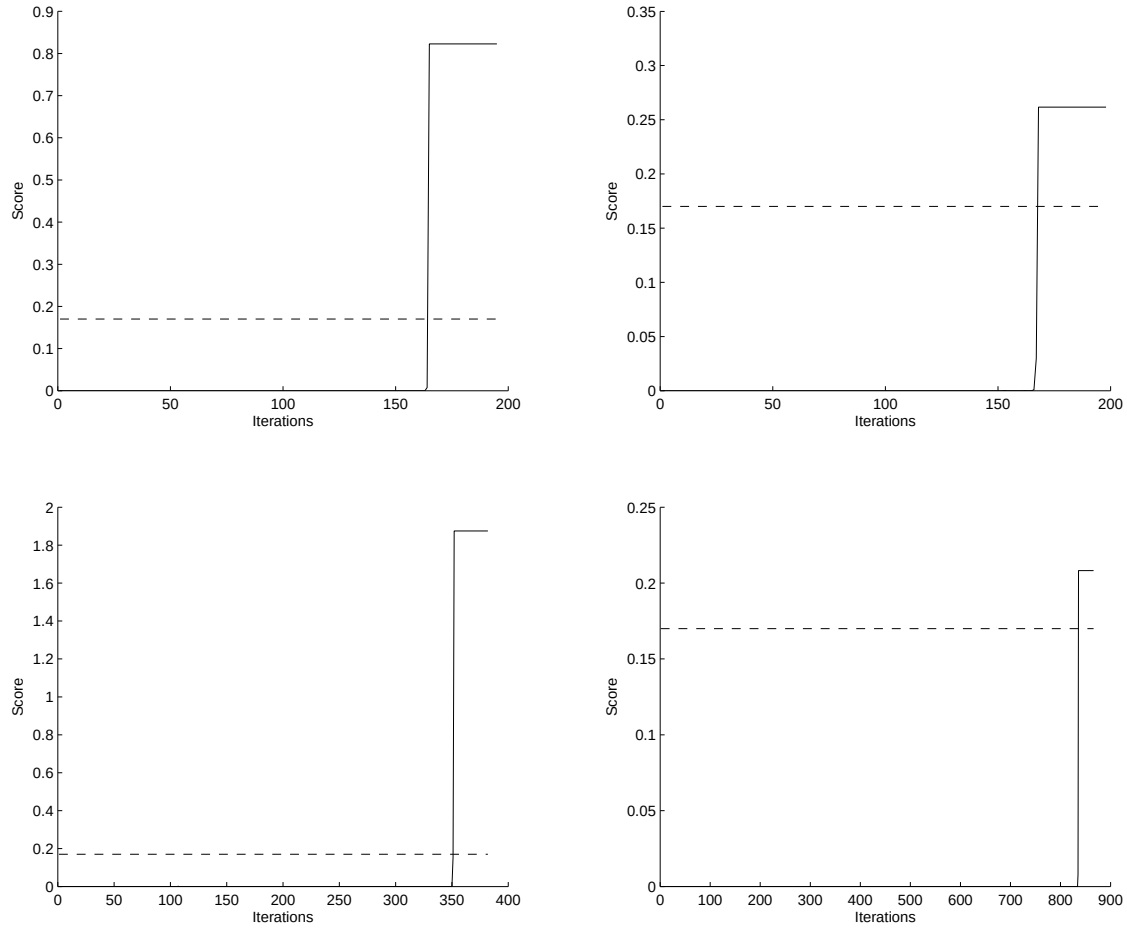


Figure 7.8: *Evolution of the score for four of the broken accounts using the single block search approach on the GMM-based face verification system. The dashed line represents the objective threshold.*

all the vectors, which form the synthetic template, are different amongst themselves.

Experiments starting from a random initial distribution G

The GMM-based system was also attacked starting from a random initial distribution G with zero mean and unit variance. For the single block search approach 98% of the accounts (out of the total 200 tested) were bypassed, and the average number of matchings needed to enter the system was 1,102. Although that success rate is very high, we can observe in Fig. 7.8 that the hill-climbing is not working properly as the score remains unaltered and equal to zero throughout the iterations (there is no increasing or *hill-climbing* effect) until at one point it very rapidly (two or three iterations) reaches the objective value (shown with a dashed line).

This behaviour can be explained by the fact that the score given by the system is the substraction of the client and the world scores (see Sect. 7.1.2). As the synthetic templates are built duplicating a block randomly selected from a general distribution G, their appearance is

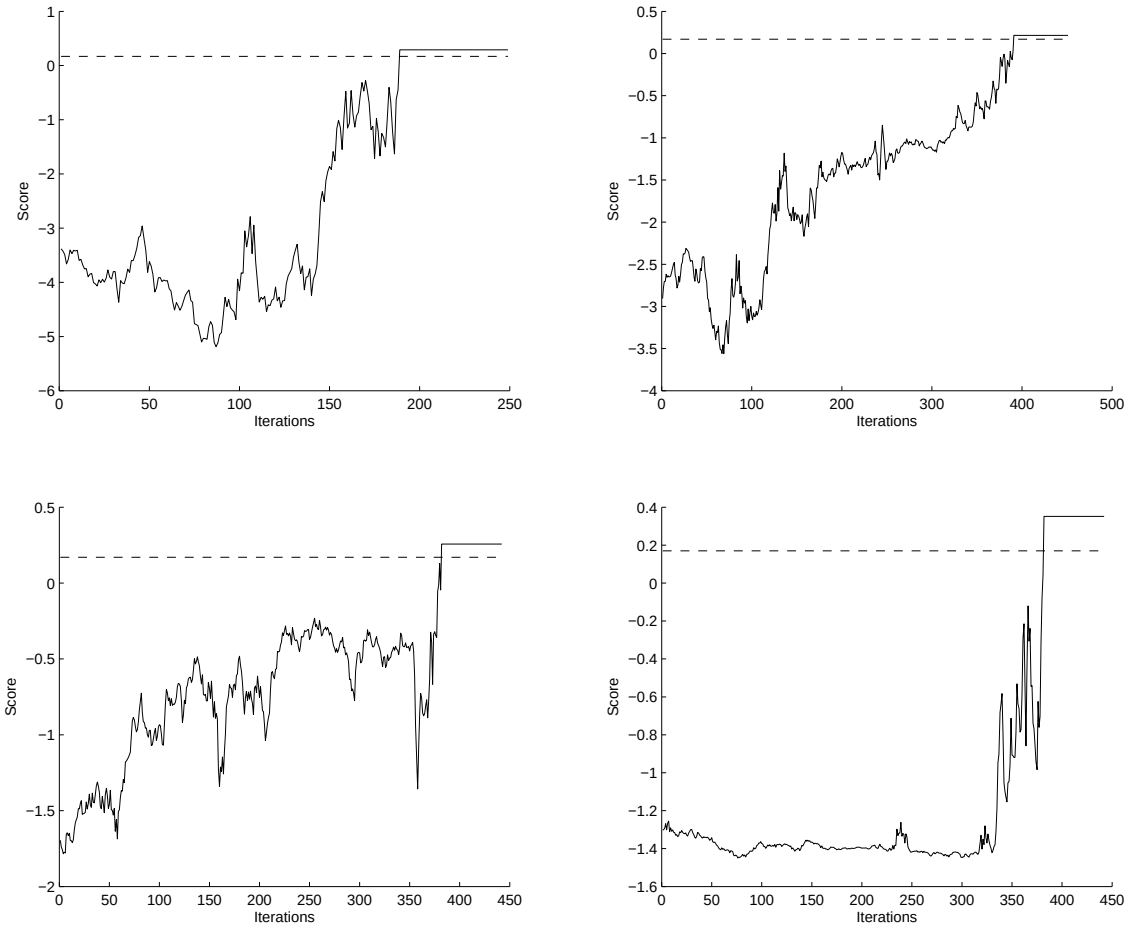


Figure 7.9: *Evolution of the score for four of the broken accounts using the multiple block search approach on the GMM-based face verification system. The dashed line represents the objective threshold.*

completely different to that of a face and so both similarity scores (those obtained from the world and client model) are the same, leading to a zero final score. As the final score obtained by all the synthetic templates is the same (zero), we have no feedback as about the local distribution L (representing those templates which are more similar to the attacked one). Therefore, the algorithm ends up doing a random search until at some point one of the templates produces (by chance) a non-zero score.

Even though this attack is the equivalent of a random search it successfully breaks the system at the first attempt (corresponding to 25 matchings) for 43% of the tested accounts. Therefore, this security breach should be taken into account when designing countermeasures (e.g., checking that all the blocks of the template are different) for final applications.

The above experiments were repeated using the multiple block search scheme. In this case, all 200 accounts were bypassed and the average number of comparisons needed to break the system was 3,016. In Fig. 7.9 it can be observed that the hill-climbing algorithm is able to produce the desired increasing effect in the score throughout the iterations. We can see that

	Operating points (in %)		
	FAR=0.1,FRR=5	FAR=0.05,FRR=7	FAR=0.01,FRR=16
Sing. Block Search	100 **123**	100 **413**	98 **1,102**
Mult. Block Search	100 **724**	100 **1,835**	100 **3,016**
E_{ff-bf}	1,000	2,000	10,000

Table 7.6: *Results of the attack for different points of operation and the best configuration found of the attacking algorithm (N=25, M=5, $\alpha = 0.5$). The SR is given in plain text (in percentage, over the total 200 attacked accounts), and E_{ff} in (**bold**). The average number of matchings needed for a successful brute-force attack (E_{ff-bf}) is also given for reference.*

the synthetic templates produce a negative final score (they get a better matching score from the world model than from the client model, $S = Sc - Sw$) and thus, the algorithm gets the necessary feedback to iteratively improve the estimate of the vector distribution G. Again, this approach is slower than the single block search, but on the other hand it is more difficult to countermeasure as all the image blocks are different amongst themselves.

Analysis of different operating points.

The GMM-based system was evaluated at two additional operating points, these being: *i*) FAR=0.05%, which implies $E_{ff-bf} = 2,000$ and leads to FRR=7%, and *ii*) FAR=0.1%, which implies $E_{ff-bf} = 1,000$ and leads to FRR=5%. For these experiments the initial distribution G was chosen as a Gaussian distribution with zero mean and unit variance and the two different attacking approaches (single block search and multiple block search) were tested.

The results, shown in Table 7.6, indicate that the Bayesian hill-climbing attack is effective for all of the operating points. The number of broken accounts remains unaltered (100% for all cases) and, the same as in the PCA-based system study, the number of comparisons needed to break the system are always lower than that of a brute force attack.

7.2. Attack Protection

The results achieved by the Bayesian hill-climbing algorithm against both face recognition systems considered in the experiments, have shown their high vulnerability against this type of attacking approach and the need to incorporate some attack protection method that increases their robustness against this threat. In the next section we analyze the performance of score quantization as a way to countermeasure the attack.

QS	10^{-6}	10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}	2.5×10^{-1}
PI (%)	48.95	30.61	23.27	18.22	10.18	0.38	0.02
EER (%)	4.71	4.70	4.72	4.74	4.75	4.79	8.13

Table 7.7: *Percentage of iterations of the hill-climbing attack with a positive score increase (PI), and EER of the Eigenface-based system for different quantization steps (QS) of the matching score.*

QS	10^{-6}	10^{-3}	10^{-1}
SR	86	84.5	16.5
E_{ff}	4,492	4,697	20,918

Table 7.8: *Performance (in terms of SR and E_{ff}) of the Bayesian hill-climbing attack against the Eigenface-based system for different Quantization Steps (QS).*

7.2.1. Countermeasuring the Hill-Climbing Attack: Score Quantization

As was already introduced in Sect. 2.2 score quantization has been proposed as an effective biometric-based approach to reduce the effects of hill-climbing attacks and, although Adler [2004] presented a modified attacking algorithm for PCA-based face recognition systems robust to this countermeasure, the BioAPI consortium [BioAPI, 2009] recommends that biometric algorithms emit only quantized matching scores in order to prevent eventual hill-climbing attacks.

Here we will study the efficiency of this attack protection technique against the novel Bayesian-based hill-climbing algorithm proposed in the Thesis.

7.2.1.1. Score Quantization: Eigenface-Based System

We will consider the Eigenface-based system using the standard correlation metric, and operating at the FAR=0.01% threshold. For the hill-climbing attack we will assume the best configuration found in the vulnerability assessment experiments, $[N, M, \alpha] = [25, 5, 0.5]$, and an initial distribution of zero mean and unit variance.

In order to choose the quantization step we analyzed the results obtained from the attack performed in Sect. 7.1.4.1 under the previously described conditions, and the findings are summarized in Table 7.7. *QS* stands for Quantization Step, *PI* is the percentage of iterations out of the total performed in the attack that produced a Positive Increase in the matching score (i.e., the score increase was higher than the quantization step), and *EER* is the Equal Error Rate of the system for the quantization step considered. The first quantization step (i.e., 10^{-6}) is the default precision of the system, therefore it is the QS at which all the previous experiments were carried out.

From results shown in Table 7.7 we can see that for the last QS considered ($2.5 \times 10_{-1}$) the EER suffers a big increase (QS is too big), while for the previous QS values the system performance is not affected. Therefore, the hill-climbing attack is repeated considering another

QS	10^{-4}	10^{-3}	10^{-2}	10^{-1}	2.5×10^{-1}	5×10^{-1}
PI (%)	45.16	42.32	34.75	12.42	4.01	0.93
EER (%)	1.25	1.27	1.31	1.37	1.74	8.91

Table 7.9: *Percentage of iterations of the hill-climbing attack with a positive score increase (PI), and EER of the GMM-based system for different quantization steps (QS) of the matching score.*

QS	10^{-4}	10^{-1}	2.5×10^{-1}
SR	100	99.5	81
E_{ff}	3,016	3,155	5,218

Table 7.10: *Performance (in terms of SR and E_{ff}) of the Bayesian hill-climbing attack against the GMM-based system for different Quantization Steps (QS).*

two QS values (in addition to $QS = 10^{-6}$), $QS = 10^{-3}$, and $QS = 10^{-1}$. Results are presented in Table 7.8, where we can see that score quantization reduces the success chances of the attack (for bigger QS, the SR decreases). However, it can also be noticed that the attacking algorithm is quite robust to this type of countermeasure, as even for the biggest value of QS (increasing it would imply a deterioration of the system EER as shown in Table 7.7), the SR of the attack is still over 15%.

7.2.1.2. Score Quantization: GMM-Based System

After the observations made in Sect. 7.1.4.2, the attacks will be performed using the best configuration found for the hill-climbing algorithm $[N, M, \alpha] = [25, 5, 0.5]$, starting from a synthetic initial distribution of zero mean and unit variance, and for the random blocks search case. The operating point at which the GMM-based system will be tested corresponds to FAR=0.01%.

An analogue initial experiment to the one carried out in the case of the Eigenface-based system, is performed here in order to determine the Quantization Steps (QS) which will be used to countermeasure the attack. Results are shown in Table 7.9. Again, there is no significant impact of the QS on the performance of the system except for the last considered value ($QS = 5 \times 10^{-1}$) where a big decrease in the system EER can be observed. Thus, the performance of the attack is analyzed using $QS = 10^{-1}$ and $QS = 2.5 \times 10^{-1}$ as quantization steps, and results are given in Table 7.10. We can observe that for the case of the GMM-based system the score quantization has very little impact on the performance of the attack which presents a SR of 81% for the highest QS considered (selecting a step over this value would mean decreasing the performance of the system under the normal operation mode).

7.3. Chapter Summary and Conclusions

In this chapter we have studied the robustness of two different face verification systems (one PCA-based and one working on GMMs) against the hill-climbing attack based on Bayesian adaptation proposed in Chapter 4. Experimental results show that the two face verification systems studied are highly vulnerable to this approach, with over an 85% success rate for all of the attacks; even when no real images were used to initialize the algorithm. Furthermore, the attack showed its ability to reconstruct the user's real face image from the scores, thus arising security issues concerning the privacy of the client.

The performance of the Bayesian hill-climbing algorithm was compared to a brute force attack. It was found that the iterative approach is more efficient under all tested conditions. In addition, it is worth noting that the resources required by both approaches differ greatly. In order to perform an efficient brute-force attack, the attacker must have a database of more than a thousand real different templates, while the hill-climbing approach does not need any real templates to be successful.

It has also been found that the GMM-based system, although its overall performance is significantly better than the PCA-based system, is very vulnerable to random attacks carried out with templates formed by a replicated random or average block. This important security flaw can be solved by incorporating to the systems a mechanism to detect duplicated patterns in the image.

At the same time, the present study points out the serious risk that the Bayesian-based hill-climbing algorithm represents as it has been successfully applied not only to different matchers but also to different biometric traits (in Chapter 6 it was shown to be an effective method to attack an on-line signature verification system). Furthermore, the experimental results reached in both security evaluations (against face and on-line signature verification systems) have proven the behaviour consistency of the hill-climbing algorithm and its ability to adapt to totally different environments. Thus, this threat should be studied when designing biometric security systems working with fixed length feature vectors of real numbers and delivering real similarity scores.

Furthermore, the attack showed a high degree of robustness against countermeasures based on score quantization (specially in the case of the GMM-based system), reaching success rates of over 15% for all the studied score quantization scenarios .

The case of systems which do not produce matching similarity measures (e.g., some SVM implementations), for which our approach may not be adequate, represents a challenging attacking scenario that will be the source of future research.

This chapter includes novel contributions in the evaluation of face recognition systems to the Bayesian hill-climbing attack, the demonstration that the attack can be successfully applied to different traits and matchers, the security flaw of GMM-based systems regarding attacks performed with templates formed by replicated blocks, and the effectiveness of the hill-climbing approach as a face reconstruction algorithm.

Chapter 8

Conclusions and Future Work

This Thesis has considered the problem of evaluating the security offered by biometric systems through the statistical and systematic analysis of different vulnerabilities and countermeasures. After a summary of the state-of-the-art in vulnerability assessment and countermeasures in the biometric technology, the security evaluation methodology followed in the Thesis has been presented. These procedural guidelines for the systematic and objective evaluation of biometric security have been applied in the experimental studies described in the last chapters of the Dissertation to competitive systems based on three different traits, namely: fingerprint, signature and face; using standard biometric data and benchmarks. Besides, in the experimental chapters of the Dissertation, the efficiency of several attacks and countermeasures, contribution of the Thesis, has been explored.

8.1. Conclusions

Chapter 1 introduced the basics of biometric systems, biometric modalities, our perspective of the security evaluation problem, the motivation of the Thesis, and the research contributions originated from this Thesis. Chapter 2 summarized the most relevant works related to the different research lines developed in the Dissertation and which served as basis for the motivations that originated the Thesis. The security evaluation methodology followed in the Thesis was presented in Chapter 3, which also described the state-of-the-art in multimodal biometric databases and the most relevant dataset used in the Thesis. The first part of the Dissertation concluded with the description of three original algorithmic methods that were later deployed for vulnerability assessment and attack protection in the experimental chapters, namely: *i*) a hill-climbing attack based on Bayesian adaptation, *ii*) a fingerprint liveness detection approach based on quality measures, and *iii*) a method for the generation of synthetic on-line signatures based on spectral analysis.

The experimental part of the Thesis started in Chapter 5 studying the vulnerabilities of fingerprint-based recognition systems to direct and indirect attacks and proposing countermeasures to reduce the effects of this type of threats. The robustness of different fingerprint recog-

nition systems was evaluated against two type of direct attacks, the first one starting from a latent fingerprint (produced with and without the cooperation of the user), and the second starting from a standard ISO minutiae template. This last approach questions the widespread belief of minutiae template non-reversibility and constitutes a serious security breach for those applications working with non-encrypted standard templates. These direct attacks were counteracted using a novel liveness detection approach based on quality measures which showed a high efficiency detecting the fake fingerprints and drastically reducing the success chances of the attacking approaches. Also in this chapter, we evaluated the vulnerability of a PC-based and of a Match-on-Card fingerprint recognition systems against an indirect hill-climbing attack. Although the iterative algorithm showed a high performance and was able to break the systems for over 90% of the attempts, its efficiency was drastically reduced when a countermeasure based on score-quantization was incorporated.

Chapter 6 studied the vulnerabilities of biometric systems based on on-line signature recognition. Two type of indirect attacks were implemented: a novel hill-climbing attack based on Bayesian adaptation, and a brute-force attack carried out with synthetically generated signatures. The hill-climbing algorithm was used against a feature-based verification system and reached a success rate of over 95% for the best configuration found. In order to reduce the vulnerability of the system to the attacking approach, a comparative study between the most robust and the best performing features was carried out. In the case of the brute force attack carried out with synthetically generated signatures, the experiments were performed by attacking real signature models obtained with a HMM-based recognition system with synthetic samples (which were produced with the novel synthetic signature generation method described in Chapter 4). Using synthetic traits instead of real ones to carry out this type of attack overcomes the problem of biometric data scarcity and turns it into a real threat that should be studied in order to design effective countermeasures to prevent it. With this objective we analyzed the feasibility of using synthetic duplicated samples in the enrollment stage in order to decrease the FAR of the system, and this way minimize the success chances of brute-force attacks.

Chapter 7 analyzed the robustness of two face verification systems (one PCA-based and one working on GMMs) against the Bayesian-based hill-climbing algorithm already used in Chapter 6 to attack a biometric system based on dynamic signature recognition. The experimental results showed that the two face verification systems studied were highly vulnerable to this type of attack, even when no real images were used to initialize the algorithm. Furthermore, the attack showed its ability to reconstruct the user's real face image from the scores, thus arising security issues concerning the privacy of the client. The combined results of Chapters 6 and 7, where the proposed hill-climbing attack based on Bayesian adaptation was used to attack signature and face verification systems respectively, have proven the behavior consistency of the hill-climbing algorithm and its ability to adapt to totally different environments. Thus, this threat should be studied when designing biometric security systems working with fixed length feature vectors of real numbers and delivering real similarity scores. Besides the security evaluation against the hill-climbing approach, we obtained experimental evidence of the vulnerability of the GMM-

based system against attacks carried out with templates formed with replicated random blocks.

In summary, the main results and contributions obtained from this Thesis are:

- The security evaluation methodology for biometric systems followed throughout the Dissertation.
- The different novel algorithmic methods developed and used for vulnerability assessment and as countermeasures against attacks (new hill-climbing attack based on Bayesian adaptation, new method based on spectral analysis for the generation of synthetic on-line signatures, and new liveness detection approach for fingerprint recognition systems based on quality measures).
- The multimodal biometric data acquired, which is now available for research purposes.
- The experimental evidence of the application of the security evaluation methodology to different biometric systems based on very relevant traits: fingerprint, signature, and face.

8.2. Future Work

A number of research lines arise from the work carried out in this Thesis. We consider of special interest the following ones:

- Applying the proposed security evaluation methodology to other biometrics. Several works have already been published where the authors study the feasibility of carrying out different attacks (generally direct attacks) to biometric systems working on traits different to the ones considered in this Thesis, such as iris [Matsumoto, 2004; Thalheim and Krissler, 2002], hand geometry and the vein pattern [Geradts and Sommer, 2006], or voice [Bonastre *et al.*, 2007]. Using the evaluation guidelines followed in this Thesis to analyze these security breaches would help to build understanding about the real magnitude of the vulnerabilities.
- Searching for new vulnerabilities of biometric systems. For instance, biometric systems could be vulnerable to the so-called *side-channel* attacks (e.g., the timing attacks [Kocher, 1995], or the Differential Power Analysis [Kocher *et al.*, 1999]). These attacking methods try to take advantage of easily measurable parameters of the system (such as the response time, or the power consumption) in order to break into the application, and have been widely studied in other security applied technologies like cryptography. Recently it has been shown that in some biometric systems, the matching time and the score returned are not independent and that this correlation could be used to gain access to the system [Galbally *et al.*, 2009c].
- Generating new liveness detection methods based on quality measures for other commonly used traits different from fingerprints. Biometric quality assessment is a current research challenge and it has not been until recent years when it has received specific attention

form the biometric community [ISO/IEC 29794-1, 2006; NIST, 2006]. Quality assessment could be used, as has been done in this Thesis for the fingerprint trait, to develop liveness detection schemes in other biometrics such as iris [Chen *et al.*, 2006], or face [Kryszczuk and Drygajlo, 2007].

- Evaluating the robustness of a multimodal biometric system against the proposed hill-climbing attack based on Bayesian-adaptation. Multimodal biometric systems are claimed to be more robust against attacks than unimodal systems [Jain *et al.*, 2006; Prabhakar *et al.*, 2003], however their actual level of security has not yet been tested. The Bayesian hill-climbing attack proposed in this Thesis has proven to adapt to different systems using fixed length feature vectors of real numbers and returning real similarity scores, thus it could be used to evaluate, not only the independent unimodal systems, but also the multimodal biometric system as a whole.

- Combine the proposed synthetic signature generation model with other existing methods [Djioua and Plamondon, 2009], in order to analyze the individuality information content in signatures so as to improve the understanding of robust signatures against forgeries and attacks.

- Studying the feasibility of applying to handwriting synthetic generation a similar spectral-based approach as the one used in this Thesis for the generation of synthetic signatures. This would give an alternative to the actual methods based on the concatenation of previously acquired characters [Guyon, 1996; Lin and Wang, 2007; Varga *et al.*, 2005].

- Studying new preventive countermeasures based on offering specific protection for templates [Adler, 2008; Jain *et al.*, 2008a]. These methods would be specially relevant for the direct attack using gummy fingers generated from standard ISO templates studied in Chapter 5.

Apéndice A

Resumen Extendido de la Tesis

Vulnerabilidades y Protección Frente a Ataques en Sistemas de Seguridad Basados en Reconocimiento Biométrico

Se denomina *reconocimiento biométrico* al proceso que permite asociar una identidad con un individuo de forma automática, mediante el uso de alguna característica personal que le sea inherente [Jain *et al.*, 2006]. Aunque en el ámbito forense (judicial, policial y pericial), el análisis científico de evidencias biométricas se ha venido usando desde hace más de un siglo, el reconocimiento biométrico como medio automático de autenticación personal en aplicaciones comerciales o civiles es un área de investigación y desarrollo reciente.

Hoy en día el reconocimiento biométrico se puede considerar como un campo de investigación asentado, con libros de referencia [Jain *et al.*, 2008b; Ratha and Govindaraju, 2008; Ross *et al.*, 2006], conferencias específicas en el área [Boyer *et al.*, 2008; Lee and Li, 2007; Tistarelli and Maltoni, 2007; Vijaya-Kumar *et al.*, 2008], evaluaciones y pruebas comparativas [Cappelli *et al.*, 2006b; LivDet, 2009; Mayoue *et al.*, 2009; Przybocki and Martin, 2004; Yeung *et al.*, 2004], proyectos internacionales [BioSec, 2004; Biosecure, 2007; COST, 2007; MTIT, 2009], consorcios específicos dedicados al reconocimiento biométrico [BC, 2009; BF, 2009; BI, 2009; EBF, 2009], esfuerzos de estandarización [ANSI/NIST, 2009; BioAPI, 2009; ISO/IEC JTC 1/SC 27 , 2009; ISO/IEC JTC 1/SC 37 , 2009], y un creciente interés tanto por parte de gobiernos [BWG, 2009; DoD, 2009] como del sector comercial [IBIA, 2009; International Biometric Group, 2009].

Pese a la madurez de este campo de investigación, con trabajos que se remontan más de tres décadas en el tiempo [Atal, 1976; Kanade, 1973; Nagel and Rosenfeld, 1977], el reconocimiento biométrico sigue siendo un área muy activa de investigación, con numerosos problemas prácticos aún por solucionar [Jain *et al.*, 2004a]. Estos problemas prácticos han hecho que, pese al interés

de las aplicaciones biométricas, la integración en el mercado de estas nuevas tecnologías sea más lenta de lo esperado.

Esta Tesis se centra en el análisis estadístico de las vulnerabilidades y métodos de protección frente a ataques de los sistemas biométricos con el objetivo de proponer una serie de directrices, apoyadas por resultados experimentales, que ayuden a las distintas partes implicadas en el campo del reconocimiento biométrico (investigadores, diseñadores, evaluadores y fabricantes) a encontrar soluciones que minimicen los efectos de esas amenazas.

A.1. Introducción

El paradigma de la autenticación biométrica. El reconocimiento de personas se ha realizado históricamente asociando identidad y "algo que la persona pose" (por ejemplo, una llave o una tarjeta), o bien "algo que la persona sabe" (por ejemplo, una palabra-clave o un PIN). El reconocimiento biométrico añade a este paradigma una nueva dimensión, asociando persona e identidad personal mediante "algo que la persona es (o produce)". "Algo que la persona es" nos indica una característica fisiológica asociada de forma inherente a la persona, mientras que "algo que la persona produce" nos indica una aptitud o acto previamente entrenado que la persona realiza como patrón de conducta.

Sistemas biométricos. El reconocimiento biométrico es un término genérico para denominar a los dos modos de funcionamiento de los sistemas biométricos. De forma más precisa, se denomina *identificación* biométrica a la tarea que pretende asociar una muestra biométrica a uno de los N patrones o modelos disponibles del conjunto conocido de individuos registrados. Por este motivo, a esta tarea también se la conoce como comparación uno-contra-muchos o uno-contra-N. La salida de los sistemas que funcionan bajo este modo suele ser una lista ordenada de candidatos, estando ligado el criterio de ordenación al grado de similitud entre la muestra de prueba y el patrón registrado. Por el contrario, la *verificación* (o *autenticación*) biométrica es la tarea que pretende decidir si una determinada muestra de entrada coincide o no con un usuario específico (denominado usuario "solicitado", o "pretendido"). Esta tarea es conocida como problema uno-contra-uno, y la salida será una decisión binaria (aceptado/rechazado) basada en el grado de similitud (en forma de puntuación o *score*) entre la muestra de entrada y el modelo de usuario pretendido: si la puntuación de similitud obtenida supera un determinado umbral de decisión el usuario será aceptado, si no será rechazado. En esta Tesis todos los sistemas biométricos analizados funcionan bajo el modo de verificación que se muestra esquemáticamente, junto con el modo identificación y el modo *registro* (por el que un usuario se da de alta en el sistema), en la Fig. 1.1.

Tipos de errores en verificación. El modo de verificación puede ser considerado como una tarea de detección, comportando un compromiso entre dos tipos de errores: 1) Falso Rechazo (FR), que se produce cuando un usuario auténtico (lo que se conoce también por usuario genuino

o cliente) es rechazado por el sistema, y 2) Falsa Aceptación (FA), que sucede cuando un impostor es aceptado por el sistema como si fuera un usuario auténtico. Estos dos tipos de errores tienen relación inversa entre sí, pudiéndose obtener diversos puntos de funcionamiento del sistema en función del umbral de decisión elegido. El punto de trabajo en cada caso dependerá de cada aplicación en particular. Por esta razón la caracterización de los sistemas biométricos se realiza mediante las curvas completas que relacionan ambos tipos de error (ver Fig. 3.1). Por esta razón también, en el caso de caracterizar el rendimiento de un sistema de verificación con tasas numéricas, se suele optar bien por un par (FA,FR) o por el punto donde coinciden ambas tasas, esto es, el punto de igual error (*Equal Error Rate* –EER).

Representación del funcionamiento en verificación. Tradicionalmente se han venido usando para representar el rendimiento de los sistemas biométricos en modo de verificación las curvas ROC (*Receiver-* o *Relative- Operating Characteristic*), en las que se representa la probabilidad de FA frente a la probabilidad de FR para los diferentes puntos de trabajo (esto es, umbrales de decisión) del sistema. En las curvas ROC, la zona de interés se concentra en la esquina inferior izquierda de la gráfica, que se corresponde con la zona en la que los dos tipos de error se minimizan conjuntamente. El problema de este tipo de representación ocurre cuando los sistemas producen bajas tasas de error, puesto que, en estos casos, las curvas que describen los sistemas tienden a concentrase, de tal forma que no se consigue de forma visual una comparativa clara de sistemas competitivos. Con el objeto de solventar este problema, se han propuesto recientemente las denominadas curvas DET (*Detection Error Tradeoff*) [Martin *et al.*, 1997], que representan también los dos tipos de error pero aplicando una transformación de ejes. Dicha escala produce un efecto de separación de las gráficas correspondientes a sistemas poco distinguibles en la representación a través de curvas ROC. Además las curvas DET tienden a ser líneas rectas para distribuciones de puntuaciones Gaussianas (que son las típicas en sistemas biométricos), haciendo así que las comparaciones entre sistemas competitivos sean directas y sencillas. En la Fig. 3.2 se muestra una comparación entre curvas ROC y DET de dos sistemas hipotéticos de verificación A y B.

Modalidades biométricas. Hay una serie de modalidades fisiológicas que pueden ser consideradas como tecnológicamente "maduras", a saber, la huella dactilar, el iris, la cara, la geometría de la mano, o la huella palmar. En relación con las modalidades conductuales, rasgos como la voz, la escritura y la firma manuscrita, o el modo de andar (marcha), son modalidades objeto de grandes esfuerzos de investigación. La Fig. 1.2 muestra algunos ejemplos de rasgos biométricos utilizados en la actualidad. En teoría, cualquier característica humana puede ser considerada como un rasgo biométrico siempre que satisfaga las siguientes propiedades:

- *universal*, que indica que toda persona debe poseer dicho rasgo;
- *distintivo*, que se refiere a que dicho rasgo debe ser lo suficientemente diferente para diferentes personas;

- *permanente*, que indica que dicho rasgo debe poseer una representación que se mantenga a lo largo del tiempo;
- *mensurable*, que se refiere a la habilidad de medir dicho rasgo cuantitativamente.

Otras propiedades deseables de cara al uso de rasgos biométricos en sistemas de autenticación incluyen:

- *rendimiento*, que se refiere a la eficiencia, precisión, velocidad, robustez, y uso de recursos de las implementaciones prácticas basadas en dicho rasgo;
- *aceptabilidad*, que indica el grado en el que la gente está dispuesta a usar dicho rasgo y en qué términos;
- *seguridad*, que se refiere a la dificultad de burlar un sistema basado en dicho rasgo con métodos fraudulentos;
- *gestión de excepciones*, que se refiere a la posibilidad de completar un proceso de comparación manual en caso de que un determinado usuario no esté capacitado para hacerlo de forma automática;
- *coste*, que hace referencia a todos los costes que conllevaría el instalar un sistema en un escenario operativo real.

De las anteriores características, la presente Tesis doctoral se centra en la evaluación, de forma sistemática y estadística, de la *seguridad* de los sistemas biométricos, y en el análisis y propuesta de nuevas contramedidas que sirvan para paliar las vulnerabilidades encontradas.

Sistemas biométricos y seguridad. Como ya se ha comentado, la tecnología basada en el reconocimiento biométrico (esto es, en algo que *eres*) presenta una serie de ventajas sobre los métodos clásicos de seguridad basados en algo que *sabes* (y por tanto puede ser olvidado o descubierto), o en algo que *tienes* (pudiendo ser robado). Sin embargo, a pesar de sus ventajas y de su gran atractivo para el usuario (tú eres tu propia llave), no podemos olvidar que los sistemas biométricos también están expuestos a ataques que pueden comprometer el nivel de seguridad ofrecido [Adler, 2005; Hill, 2001; Matsumoto *et al.*, 2002]. Así pues, es de especial relevancia el conocer las amenazas a las que están sometidos y analizar sus vulnerabilidades para poder prevenir posibles ataques y aumentar sus beneficios para el usuario final.

De esta forma cobra gran importancia para la introducción definitiva de los sistemas biométricos en el mercado, el desarrollo de un marco común de evaluación de la seguridad de esta tecnología relativamente nueva en comparación con otros métodos ya existentes y ampliamente probados. En este escenario, además de la creación de laboratorios específicos para la evaluación independiente de sistemas de reconocimiento biométrico [BSI, 2009], se están llevando a cabo a nivel internacional diferentes esfuerzos de estandarización para la evaluación de seguridad de

las Tecnologías de la Información. Algunos ejemplos de estos proyectos son la *Common Criteria* [CC, 2006] junto con su *Common Evaluation Methodology* [CEM, 2006], la *Biometric Evaluation Methodology* [BEM, 2002] propuesta por el *Biometric Working Group* [BWG, 2009] dependiente del CESG Inglés, o el *Common Vulnerability Scoring System* [CCVS, 2007]. Recientemente, el primer estándar pensado específicamente para la evaluación de seguridad de aplicaciones basadas en el reconocimiento biométrico ha sido publicado por la Organización Internacional para la Estandarización (*International Organization for Standarization* - ISO) [ISO/IEC 19792, 2009].

Todas estas iniciativas cubren un rango muy amplio de sistemas y tecnologías por lo que dan pautas muy generales sobre los diferentes aspectos que deben ser tenidos en cuenta en una evaluación de seguridad. Por esta razón, existe la necesidad de generar documentos complementarios (tales como los *Supporting Documents* [CC, 2009b] y los *Protection Profiles* [CC, 2009a] de la Common Criteria - CC) que ayuden a las diferentes partes interesadas (diseñadores, industria, y evaluadores) a aplicar las indicaciones generales de las normas a las particularidades de una tecnología en concreto.

A pesar de que algunos productos biométricos ya han sido certificados siguiendo alguna de las iniciativas anteriores (en concreto la Common Criteria, p.ej., [Canadian Certification Body, 2001; German Certification Body, 2008]), aún queda un largo camino por recorrer antes de que la certificación de sistemas biométricos sea una práctica común tal y como ocurre en otras Tecnologías de la Información. Esta Tesis doctoral pretende ayudar a resolver el difícil problema de la evaluación de seguridad en los sistemas biométricos a través del estudio sistemático de sus vulnerabilidades y el análisis de contramedidas que minimicen los efectos de las amenazas detectadas, de tal forma que se aumente la confianza de los usuarios finales en esta pujante tecnología. De esta forma, los estudios experimentales que se describen en esta Disertación pueden servir de ayuda para continuar el desarrollo de los estándares para la evaluación de seguridad de los sistemas biométricos.

Transparencia frente a oscuridad. En primer lugar es importante recordar que la seguridad en términos absolutos no existe: con la suficiente financiación, voluntad, y la tecnología apropiada, cualquier sistema de seguridad se puede romper. Sin embargo, el objetivo de la comunidad dedicada al desarrollo de tecnologías orientadas a la seguridad debe ser el obtener aplicaciones que hagan que el dinero, la voluntad y los medios necesarios para romper el sistema eviten que se intente.

Existen dos enfoques a la hora de enfrentarse al problema de garantizar que el nivel de seguridad ofrecido por un determinado sistema no se vea comprometido: "seguridad a través de la oscuridad" (*security through obscurity*), o "seguridad a través de la transparencia" (*security through transparency*).

El principio de "seguridad a través de lo oscuridad" se basa en el secreto (de diseño, implementación, formatos y protocolos, etc.) para mantener la seguridad. Un sistema que funcione usando este principio puede tener vulnerabilidades reales o teóricas, pero sus diseñadores confían

en que es muy improbable que los atacantes lleguen a conocerlas o a explotarlas. Los defensores de esta metodología mantienen que el dar a conocer los detalles de las contramedidas instaladas en un sistema ayudará a los atacantes a esquivarlas o a romperlas. De igual forma, si los atacantes saben qué medidas de protección no han sido utilizadas esto los ayudará a identificar vulnerabilidades potenciales del sistema y a dirigir los ataques contra esos puntos. De hecho, el primer paso de un atacante suele ser la recopilación de información, paso que se retrasa y dificulta a través de la oscuridad.

En oposición, el esquema de "seguridad a través de la transparencia" sigue el principio de Kerckhoff (establecido por Auguste Kerckhoff en el siglo XIX) [Kerckhoffs, 1883]: "un criptosistema debería ser seguro incluso si todo sobre él, excepto la clave, es conocido". Aunque en un principio fue expuesto para criptografía, el principio fue más tarde reformulado para poder ser aplicado a cualquier sistema de seguridad como "el enemigo conoce el sistema". Sin duda, cualquier sistema de seguridad depende de mantener en secreto ciertas cosas, la pregunta es ¿qué cosas?. El principio de Kerckhoff apunta a que deben ser las partes que sean más fáciles de cambiar en caso de que sean descubiertas. En otras palabras, cuantas menos y más simples sean las cosas que deban mantenerse en secreto dentro de un sistema de seguridad, más fácil es mantener la seguridad del sistema. Citando a B. Schneier, uno de los más aclamados expertos mundiales en seguridad, "*el principio de Kerckhoff puede ser aplicado, más allá de los códigos y los cifrados, a los sistemas de seguridad en general: cada secreto genera un potencial punto de fallo. El secretismo, en otras palabras, es la principal causa de fragilidad -y por tanto algo que hará al sistema tender al colapso. Por el contrario, la transparencia proporciona capacidad de adaptación*" [Schneier, 2000].

El aplicar el principio de seguridad a través de la transparencia a la biometría significaría, en palabras del *Biometric Working Group* [BWG, 2009]: "*exponer públicamente las vulnerabilidades y contramedidas, lo que llevará a la comunidad biométrica a adoptar una actitud más madura y responsable, y a promover el desarrollo de sistemas más seguros en el futuro*" [BWG, 2003].

Nuestra perspectiva de la seguridad biométrica, que ha sido la base para el desarrollo de esta Tesis, se alinea con el principio de seguridad a través de la transparencia. De esta forma, a lo largo de la Disertación, se señalan diferentes amenazas que pueden afectar a los sistemas biométricos, se evalúan de manera sistemática, y se proponen nuevas contramedidas que ayuden a garantizar el nivel de seguridad ofrecido al usuario final.

Esto no implica que la oscuridad no ofrezca ninguna protección, sino más bien que esa protección es impredecible (no se puede garantizar que un atacante no descubra nuestros secretos), y probablemente temporal. Creemos firmemente que para crear dispositivos y aplicaciones biométricas más seguros es necesario entender y estudiar sus amenazas, y desarrollar contramedidas efectivas, tanto técnicas como de procedimiento. Tal y como se dijo anteriormente, se puede encontrar un paralelismo con otras Tecnologías de la Información más maduras donde las vulnerabilidades han sido ampliamente analizadas, y donde no se intenta ocultar la información. Al contrario, el enfoque es el de informar de los problemas para que puedan ser resueltos.

Por supuesto, no podemos olvidar que la biometría no es exactamente equivalente a la crip-

tografía. Los rasgos biométricos son identificadores únicos, pero no son secretos como las claves criptográficas [Schneier, 1999], (todo el mundo conoce nuestra cara, o podría conseguir nuestras huellas dactilares) así que no pueden ser tratados como tales. Así pues, lo que debe mantenerse secreto en un sistema biométrico puede no coincidir con aquello que aplica en criptografía. En concreto, el principio de Kerckhoff se puede generalizar en la siguiente pauta que es aplicable a la biometría: minimiza el número de secretos de tu sistema de seguridad. En la medida que puedas lograr esto estarás aumentando la robustez de tu sistema. Al contrario, lo estarás haciendo más frágil.

Al final, debe alcanzarse un compromiso entre (excesiva) publicidad y supresión de la información, basado, como en otra áreas, en principios alcanzados a partir de la experiencia. En biometría podemos esperar que se adopte un enfoque similar. Creemos, junto con muchas otras partes implicadas [BWG, 2003], que la búsqueda de amenazas, la evaluación de esas vulnerabilidades, y la propuesta de contramedidas, es el camino que nos llevará a una tecnología biométrica más robusta y segura. Este es el camino seguido en la presente Tesis doctoral.

Motivación para la Tesis. Dado que la evaluación de vulnerabilidades es clave para la aceptación entre los usuarios finales de cualquier tecnología relacionada con la seguridad, y que la biometría es una herramienta muy potente para aplicaciones de seguridad donde se requiera la identificación automática de personas, esta Tesis está centrada en la evaluación de vulnerabilidades de los sistemas biométricos. La investigación llevada a cabo en este área ha estado motivada por cinco observaciones desprendidas del estado del arte y de nuestro trabajo práctico en el laboratorio de investigación Grupo de Reconocimiento Biométrico – ATVS.

Primero, aunque diversos trabajos ya han estudiado diferentes vulnerabilidades de los sistemas biométricos [Hennebert *et al.*, 2007; Hill, 2001; Thalheim and Krissler, 2002], en la mayor parte de los casos el problema se ha tratado desde una perspectiva de "sí o no" (esto es, la pregunta para la que se busca respuesta es, ¿puede este sistema biométrico ser burlado utilizando este método de ataque?). Sin embargo, en la mayor parte de estos valiosos trabajos científicos, una pregunta aún más compleja queda sin responder: *¿cómo* de vulnerable es el sistema biométrico al ataque?. La identificación de las amenazas es el primer paso en la evaluación de vulnerabilidades, sin embargo, cuantificar el peligro que suponen esas amenazas es tanto o más importante a la hora de evaluar el nivel de seguridad proporcionado por la aplicación.

La segunda observación está fuertemente relacionada con la primera. En estas publicaciones ya existentes, los resultados experimentales se obtienen y presentan sin seguir un protocolo sistemático, de forma que, incluso en el caso de realizar un análisis estadístico de una determinada vulnerabilidad, los resultados no pueden ser comparados, perdiendo de esta forma parte de su utilidad.

La tercera observación se deriva de las distintas iniciativas que actualmente están desarrollando protocolos estándar para la evaluación de la seguridad [BEM, 2002; CC, 2006; ISO/IEC 19792, 2009]. Estos estándares están dirigidos, por lo general, a un rango muy amplio de productos dentro de las Tecnologías de la Información, lo que implica que se necesiten documentos

adicionales que ayuden a aplicar las pautas generales dadas en esas normas a las particularidades de una tecnología en concreto (con ejemplos prácticos de evaluación, listas de posibles ataques y vulnerabilidades, etc.) Esto es especialmente importante en el campo de la biometría debido al amplio abanico de modalidades existentes (huella dactilar, iris, cara, firma manuscrita, etc.), y a las múltiples áreas de conocimiento que cubre (reconocimiento de patrones, visión artificial, electrónica, etc.)

La cuarta observación que ha motivado la Tesis es la constante necesidad de búsqueda de puntos débiles de las aplicaciones de seguridad (y en este caso concreto, de los sistemas biométricos), para poder informar de ellos y motivar a la industria para que busque soluciones efectivas contra las amenazas. Esta observación está claramente relacionada con el principio de "seguridad a través de la transparencia" (ampliamente utilizado en otras áreas como la criptografía) [Kerckhoffs, 1883], que promueve el desarrollo de sistemas de seguridad tan abiertos como sea posible. Este paradigma se basa en el hecho de que las vulnerabilidades existen independientemente de su publicación, por lo tanto: hagamos frente a los problemas y encontremos soluciones para ellos (riesgo controlado), antes de que alguien encuentre la manera de aprovecharse de nuestros secretos (consecuencias impredecibles).

La última observación es que el desarrollo de nuevas contramedidas contra las vulnerabilidades estudiadas es actualmente un área en el que se está invirtiendo un gran esfuerzo. Aunque ya se han propuesto diferentes posibilidades [Adler, 2004; Jain *et al.*, 2008a; Schuckers, 2002], aún no existe ninguna solución definitiva para algunas de las vulnerabilidades analizadas, por lo que se necesitan nuevas formas de protección contra estas y otras posibles amenazas.

La Tesis. La Tesis desarrollada en la presente Disertación puede ser expuesta como sigue: "la búsqueda de nuevas amenazas (¿se puede burlar el sistema utilizando este método de ataque?), la evaluación de esas vulnerabilidades utilizando un protocolo sistemático y repetible (¿cómo de vulnerable es el sistema a este ataque?), la propuesta de nuevas contramedidas que mitiguen el efecto del ataque, e informar públicamente de los resultados de todo el proceso, ayudan a desarrollar una tecnología biométrica más madura y segura".

La Disertación. Los objetivos principales de la Tesis son los siguientes: 1) revisar y estudiar el problema de la evaluación de vulnerabilidades en los sistemas biométricos con el objetivo de identificar nuevas amenazas; 2) diseñar nuevas contramedidas para los fallos de seguridad analizados de tal forma que se potencia la resistencia de los sistemas biométricos a los ataques; y 3) aplicar las técnicas y metodologías propuestas a escenarios y sistemas de uso común, utilizando para ello bases de datos de fácil acceso para la comunidad biométrica, y poniendo especial énfasis en los sistemas de verificación basados en huella dactilar, firma, y cara.

La Disertación se estructura siguiendo un esquema clásico con un fondo teórico, métodos prácticos, y tres capítulos con estudios experimentales en los que se aplican los métodos propuestos.

En primer lugar se introducen los sistemas biométricos, se expone la motivación de la Tesis

y la Tesis propiamente dicha, se presenta la organización de la Disertación, y se enumeran las contribuciones relacionadas con el trabajo de investigación.

Después se resume el estado del arte en evaluación de vulnerabilidades de los sistemas biométricos, con especial atención a aquellos trabajos que han promovido las motivaciones de la tesis. Acto seguido se trata el problema de la evaluación del rendimiento de los sistemas biométricos y se presenta la metodología común seguida a lo largo de la Disertación para la evaluación de seguridad de los sistemas biométricos. A continuación se describen las bases de datos utilizadas en la parte experimental de la Disertación.

A continuación se describen tres métodos originales desarrollados en el contexto de la Tesis para el análisis de vulnerabilidades y la protección frente a ataques en sistemas biométricos. Estos métodos son: *i*) un nuevo ataque tipo *hill-climbing* basado en adaptación Bayesiana, *ii*) una técnica de detección de vida basada en medidas de calidad aplicable en sistemas de reconocimiento de huella dactilar para la detección de ataques con dedos de goma, y *iii*) un nuevo método para la generación de firmas manuscritas sintéticas basado en el análisis frecuencial.

La parte experimental de la Tesis comienza con la evaluación de vulnerabilidades en sistemas de verificación de huella dactilar, donde se destapa un fallo de seguridad en sistemas que utilizan plantillas estándar ISO sin encriptación. En este capítulo se analizan diferentes contramedidas contra los ataques estudiados, incluyendo la técnica de detección de vida propuesta en la Tesis, y la cuantificación de puntuaciones contra los ataques *hill-clibing*.

A continuación se realiza la evaluación de vulnerabilidades de sistemas de verificación de firma manuscrita, utilizando para ello el algoritmo Bayaesiano *hill-climbing* y el método de generación automática de firmas propuestos en la Tesis. Entre las diferentes medidas de protección frente a los ataques estudiados están la selección de las características globales de la firma más resistentes al ataque *hill-climbing*, y la mejora del registro a través de datos sintéticos.

En el último capítulo de la parte experimental de la Tesis se estudia el problema de la evaluación de seguridad en sistemas de verificación facial. Se vuelve a utilizar aquí con éxito el ataque *hill-climbing* Bayesiano, previamente aplicado a los sistemas de verificación de firma manuscrita, demostrando así su versatilidad y su habilidad para adaptarse no sólo a diferentes comparadores sino también a diferentes rasgos biométricos. Se considera aquí la cuantificación de puntuaciones como un método de protección frente al ataque.

La dependencia entre capítulos se ilustra en la Fig. 1.3. Nótese que los capítulos experimentales (sombreados) contienen referencias a los métodos utilizados de capítulos anteriores. De esta manera, y asumiendo conocimientos generales en sistemas biométricos [Jain *et al.*, 2006], los capítulos experimentales se pueden leer independientemente.

Contribuciones de la Tesis. Las contribuciones de la Tesis se pueden clasificar como sigue a continuación (por claridad, las publicaciones repetidas en diferentes puntos de la lista aparecen como citas, los artículos de revista con factor de impacto JCR se muestran en negrita):

- REVISIONES DEL ESTADO DEL ARTE.

1. Ataques directos e indirectos a sistemas biométricos.

   - J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez. Fake fingertip generation from a minutiae template. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 1-4, 2008a. (IBM Best Student Paper Award).
   - **J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters*, 2009b. Invited paper. To appear.**
   - **J. Galbally, C. McCool, J. Fierrez, and S. Marcel. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, 2010. To appear.**

2. Técnicas de detección de vida.

   - J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. Fingerprint liveness detection based on quality measures. In *Proc. IEEE Int. Conf. on Biometrics, Identity and Security (BIdS)*, 2009a.

3. Generación sintética de rasgos biométricos.

   - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Synthetic generation of handwritten signatures based on spectral analysis. In *Proc. SPIE Biometric Technology for Human Identification VI (BTHI VI)*, 2009f.

4. Bases de datos biométricas multimodales.

   - J. Galbally, J. Fierrez, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano-Rey, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, and C. Orrite-Uruñuela. Biosecurid: a multimodal biometric database. In *Proc. MADRINET Workshop*, pages 68-76, 2007d.

- MÉTODOS ORIGINALES.

1. Nuevo ataque tipo *hill-climbing* basado en adaptación Bayesiana.

   - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 386-395. Springer LNCS-4642, 2007b.
   - **[Galbally *et al.*, 2010].**

2. Nuevo método de generación sintética de firma dinámica basado en el análisis frecuencial de la trayectoria.

   - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Improving the enrollment in dynamic signature verification with synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009e.
   - [Galbally *et al.*, 2009f].

3. Nuevo método de detección de vida basado en medidas de calidad para sistemas de reconocimiento de huella dactilar.

   - [Galbally *et al.*, 2009a].

- NUEVOS DATOS BIOMÉTRICOS.

1. En el marco de esta Tesis doctoral se adquirió una base de datos multimodal (BiosecurID) que incluye ocho rasgos biométricos distintos, de 400 usuarios, capturados en cuatro sesiones de adquisición.

   - **J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications*, 2009. To appear.**

2. Una base de datos de más de 800 huellas dactilares de 68 personas diferentes, y otras tantas muestras artificiales capturadas a partir de dedos de goma generados con y sin la cooperación del usuario (esto es, 800 imágenes reales, 800 imágenes de dedos de goma con cooperación, y 800 muestras artificiales sin cooperación).

   - J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador. On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, volume 1, pages 130-136, 2006.

- NUEVOS ESTUDIOS EXPERIMENTALES

1. Ataques directos a sistemas de verificación de huella dactilar utilizando dedos de goma generados con y sin la cooperación del usuario.

   - [Galbally *et al.*, 2006].

2. Ataques directos a sistemas de verificación de huella dactilar utilizando dedos de goma generados a partir de plantillas estándar ISO.

   - [Galbally *et al.*, 2008a].
   - **[Galbally *et al.*, 2009b]**.

3. Ataques indirectos tipo *hill-climbing* a sistemas de verificación basados en firma manuscrita.

   - [Galbally *et al.*, 2007].

4. Ataques indirectos tipo *hill-climbing* a sistemas de verificación basados en cara.

   - [Galbally *et al.*, 2010].

5. Ataques tipo fuerza bruta a sistemas de verificación de firma manuscrita utilizando muestras sintéticas.

   - J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Evaluation of brute-force attack to dynamic signature verification using synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Machine Intelligence (ICDAR)*, 2009d.

6. Estudio comparativo de los parámetros globales más resistentes y de los de mejor rendimiento para sistemas de verificación de firma.

   - J. Galbally, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. Feature selection based on genetic algorithms for on-line signature verification. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 198-203, 2007a.
   - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Performance and robustness: a trade-off in dynamic signature verification. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1697-1700, 2008b.

7. Mejora del registro y del rendimiento en sistemas de verificación de firma manuscrita utilizando muestras sintéticas.

   - [Galbally *et al.*, 2009e].

Otras contribuciones relacionadas con la Tesis no incluidas en el presente volumen incluyen:

- REVISIONES DEL ESTADO DEL ARTE.

1. Avances recientes en bases de datos biométricas multimodales.

   - **J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. W. R. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran. The multi-scenario multi-environment BioSecure multimodal database (BMDB). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2009. To appear.**

2. Verificación de firma en dispositivos móviles.

   - M. Martinez-Diaz, J. Fierrez, J. Galbally, F. Alonso-Fernandez, and J. Ortega-Garcia. Signature verification on handheld devices. In *Proc. MARINET Workshop*, pages 87-95, 2007.

- MÉTODOS ORIGINALES.

1. *Hashing* biométrico basado en selección genética y su aplicación a firmas dinámicas.

   - M. R. Freire, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Biometric hashing based on genetic selection and its application to on-line signatures. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 1134-1143. Springer LNCS-4642, 2007.

- NUEVOS DATOS BIOMÉTRICOS.

1. Una nueva base de datos biométrica multimodal, capturada en el marco de la Red de Excelencia Biosecure [Biosecure, 2007], que contiene tres conjuntos de datos adquiridos en diferentes escenarios: fijo, móvil, y a través de internet.

   - **[Ortega-Garcia *et al.*, 2009]**.

2. Base de datos de 800 imágenes de iris y sus correspondientes muestras artificiales capturadas a partir de imágenes de iris impresas de alta calidad.

   - V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BioID)*, 2008.

- NUEVOS ESTUDIOS EXPERIMENTALES.

1. Clasificación de las firmas manuscritas en base a la legibilidad del nombre y su utilización en aplicaciones de mantenimiento de la privacidad.

   - J. Galbally, J. Fierrez, and J. Ortega-Garcia. Classification of handwritten signatures based on name legibility. In *Proc. SPIE Biometric Technology for Human Identification IV (BTHI IV)*, 2007c.

2. Análisis de ataques tipo *side-channel* basados en el tiempo de comparación algorítmica en sistemas de verificación de huella dactilar.

   - J. Galbally, S. Carballo, J. Fierrez, and J. Ortega-Garcia. Vulnerability assessment of fingerprint matching based on time analysis. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BIOID)*. Springer LNCS-5707, 2009c.

3. Análisis de ataques directos a sistemas de verificación de iris utilizando imágenes impresas de alta resolución.

   - [Ruiz-Albacete *et al.*, 2008].

4. Estudio de la resistencia de sistemas de verificación de firma a ataques directos realizados por imitadores con distintos niveles de habilidad.

   - F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally, and J. Ortega-Garcia. Robustness of signature verification systems to imitators with increasing skills. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009.

5. Análisis del rendimiento de parámetros globales de la firma en dispositivos móviles.

   - M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Towards mobile authentication using dynamic signature verification: useful features and performance evaluation. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, 2008.

A.2. Evaluación de la Seguridad en Sistemas Biométricos

El análisis del rendimiento de los sistemas biométricos es sólo una de las pruebas que pueden tenerse en cuenta al realizar una evaluación general de una aplicación biométrica. Otras pruebas que deberían considerarse incluyen la fiabilidad, las vulnerabilidades y la seguridad, la aceptación por parte del usuario, o el coste/beneficio [Wayman *et al.*, 2005].

En concreto, la necesidad de realizar evaluaciones de seguridad independientes, repetibles, y consistentes queda evidenciada por la generación de distintos estándares [BEM, 2002; CC, 2006; ISO/IEC 19792, 2009], la organización de competiciones que buscan el desarrollo de nuevas

contramedidas frente a ataques [LivDet, 2009], y la publicación de numerosos trabajos de investigación [Galbally *et al.*, 2007; Ratha *et al.*, 2001a; Uludag and Jain, 2004]. Todos estos esfuerzos no hacen sino resaltar la necesidad de enfocar la evaluación de seguridad de los sistemas biométricos desde una perspectiva rigurosa y sistemática.

Debido a la naturaleza estadística del reconocimiento biométrico, la evaluación de seguridad frente a las amenazas que los afectan debe ser llevada a cabo desde una perspectiva análoga a la utilizada en las evaluaciones de rendimiento (ver Sect. 3.1). El hecho de determinar si un ataque (p.ej., un ataque directo utilizando dedos de goma generados a partir de la huella latente de un individuo) es o no realizable, no es suficiente dentro de una evaluación de seguridad. Para calcular la resistencia del sistema al ataque debe adquirirse una base de datos suficientemente amplia y representativa en términos de usuarios y muestras (p.ej., de huellas reales y de goma) para así poder determinar, desde un punto de vista estadístico, *cómo* de vulnerable es el sistema al ataque.

En este contexto, proponemos un protocolo sistemático de evaluación de la seguridad en sistemas biométricos que puede ser utilizado independientemente del ataque, sistema, o rasgo biométrico considerado, y que ha sido utilizado en las diferentes evaluaciones de vulnerabilidades realizadas en la parte experimental de la Tesis. El protocolo incluye una serie de pautas que ayudan a realizar análisis de la seguridad y a presentar los resultados derivados de ellos de una forma útil y significativa para otros investigadores. En concreto, los pasos seguidos en la Tesis para la evaluación de seguridad de los sistemas biométricos son:

1. Descripción clara y precisa del ataque para el que se quiere determinar las vulnerabilidades del sistema biométrico.

2. Descripción del sistema biométrico que va a ser evaluado.

3. Descripción de la información requerida sobre el sistema para llevar a cabo el ataque.

4. Descripción de la base de datos que será utilizada en la evaluación.

5. Descripción del protocolo experimental que se seguirá durante la evaluación.

6. Realización de una evaluación del rendimiento del sistema biométrico. Esta evaluación del rendimiento nos permitirá determinar cómo de preciso es el sistema y, aún más importante, los puntos de operación en los que se realizarán los ataques (ya que las opciones de éxito de un ataque son en general muy dependientes de las tasas de FA y FR del sistema). Además, definir los puntos de operación permitirá comparar, de forma más justa, las vulnerabilidades de diferentes sistemas para el mismo ataque (esto es, podemos determinar para una tasa de FA o de FR cuál de ellos es más/menos resistente al método de ataque).

7. Realización de la evaluación de seguridad en los puntos de operación estipulados, presentando los resultados al menos en términos de la Tasa de Éxito y la Eficiencia (definidos a continuación) del ataque.

En una evaluación de seguridad al menos dos parámetros principales deben ser calculados para determinar el riesgo real que representa un determinado ataque (y por tanto la vulnerabilidad del sistema hacia el mismo):

- **Tasa de Éxito (*Success Rate, SR*)**. Es la probabilidad de que el ataque consiga romper una determinada cuenta de usuario. Se calcula como el cociente entre el número de cuentas rotas por el ataque A_b, y el número total de cuentas atacadas A_T, esto es $SR = A_b/A_T$. Este parámetro da una estimación de cómo de peligroso es un ataque para un determinado sistema biométrico: cuanto mayor sea SR, mayor será la amenaza.

- **Eficiencia**. Indica el número medio de comparaciones que requiere el ataque para intentar romper una cuenta de usuario. Se define como $E_{ff} = \left(\sum_{i=1}^{A_T} n_i\right)/A_T$, donde n_i es el número de comparaciones realizadas para intentar romper cada una de las cuentas de usuario. Nótese que se calcula en función del número de comparaciones realizadas, y no en función del número de iteraciones realizadas por el ataque (caso de tratarse de un algoritmo iterativo), ya que en cada iteración puede realizarse más de una comparación. Este parámetro da una estimación de cómo de fácil/difícil es para el algoritmo romper el sistema en términos de velocidad: cuanto menor sea E_{ff} más rápido es el ataque.

Con el término "cuenta de usuario" nos referimos a la plantilla/modelo registrado de un usuario legítimo del sistema, que se utiliza como referencia para ser comparado con la/s muestra/s de test.

La SR y la eficiencia de un ataque que consista en una sucesión de intentos de acceso de esfuerzo cero (esto es, ataque tipo "fuerza bruta" en el que intentamos acceder al sistema aprovechándonos de su tasa de FA) ya se han calculado en la evaluación de rendimiento ya que para este caso particular $SR = FAR$ and $E_{ff} = 1/FAR$. Por tanto pueden presentarse como resultado base con los que comparar la SR y eficiencia del ataque que se esté considerando. Esta es una comparación útil ya que todos los sistemas biométricos son vulnerables a un ataque por fuerza bruta (siempre hay alguna probabilidad de que un impostor sea aceptado como un usuario genuino).

De forma similar, cuando se introduce una contramedida en un sistema biométrico para reducir el riesgo de un determinado ataque previamente analizado, debería ser evaluada estadísticamente teniendo en cuenta dos parámetros principales:

- Impacto de la contramedida en el rendimiento del sistema. La inclusión de una determinada contramedida puede hacer que cambien las curvas de FAR y FRR del sistema biométrico, y estos cambios deben ser evaluados y expuestos (otros indicadores del rendimiento del sistema tales como la velocidad, o la eficiencia computacional podrían también verse afectados por una determinada medida de protección frente a ataques, pero estos cambios no serán considerados en la Tesis).

- Rendimiento de la contramedida, esto es, impacto que tiene en la SR y la eficiencia del ataque.

Siguiendo la perspectiva estadística descrita para la evaluación de seguridad de sistemas biométricos, en la Tesis se han realizado análisis de vulnerabilidades de distintos sistemas de reconocimiento biométrico contra tres tipos fundamentales de ataques:

- **Ataques Directos**. Estas amenazas hacen referencia al uso de rasgos biométricos sintéticos (p.ej., dedos de goma, o imágenes impresas de alta calidad de la cara), para intentar acceder al sistema.

- **Ataques tipo *Hill-Climbing***. Son algoritmos iterativos que se aprovechan de las puntuaciones de similitud devueltas por el sistema biométrico para modificar una serie de plantillas generadas sintéticamente hasta que obtienen acceso al sistema.

- **Ataques tipo Fuerza Bruta**. Consisten en una sucesión de intentos de acceso de esfuerzo cero (un impostor intenta acceder al sistema con su propio rasgo biométrico). Por tanto, para este caso particular, la SR y la eficiencia del ataque ya se han calculado en la evaluación de rendimiento del sistema puesto que, en este caso concreto, $SR = FAR$ y $E_{ff} = 1/FAR$. Este resultado puede presentarse como base con el que comparar la SR y eficiencia del ataque que se esté considerando. Se trata de una comparación especialmente útil ya que todos los sistemas biométricos son vulnerables a un ataque por fuerza bruta (siempre hay alguna probabilidad de que un impostor sea aceptado como un usuario genuino).

A.3. Métodos Originales para la Evaluación de Seguridad y Protección frente a Ataques

A continuación se presentan tres métodos algorítmicos originales que se han propuesto a lo largo del desarrollo de la Tesis y que se utilizarán en las evaluaciones de seguridad realizadas durante la parte experimental de la Disertación. Los algoritmos propuestos son: *i*) un ataque tipo *hill-climbing* basado en adaptación Bayesiana y que puede ser utilizado de forma directa para atacar diferentes comparadores y rasgos biométricos, *ii*) un método *software* de detección de vida para sistemas de reconocimiento de huella dactilar basado en medidas de calidad (que presenta la ventaja respecto a otros métodos anteriormente presentados de necesitar una única huella para determinar si es real o falsa), y *iii*) un esquema completo de generación de firmas *on-line* sintéticas basado en la información frecuencial de la trayectoria (al contrario que en enfoques anteriores, en este caso no se requiere de ninguna muestra real para generar los rasgos sintéticos).

Algoritmo *hill-climbing* Bayesiano. Se describe a continuación un algoritmo *hill-climbing* basado en adaptación Bayesiana [Duda *et al.*, 2001]. La contribución de este nuevo método radica en que puede ser utilizado de forma directa para atacar sistemas biométricos (trabajando con diferentes rasgos y comparadores) que utilicen vectores de características de longitud firma y formados por números reales, y que devuelvan puntuaciones de similitud reales. El ataque ustiliza las puntuaciones devueltas por el comparador para adaptar una distribución global calculada a partir de un conjunto de usuarios de desarrollo, a las particularidades locales del cliente atacado.

Planteamiento del problema. Consideremos el problema de encontrar un vector $\mathbf{y}^*$ K-dimensional que, comparado con una plantilla desconocida $\mathcal{C}$ (en nuestro caso perteneciente a un cliente en concreto), produzca una puntuación de similitud mayor que un determinado umbral δ, de acuerdo a alguna función de comparación J, esto es: $J(\mathcal{C}, \mathbf{y}^*) > \delta$. La plantilla puede ser otro vector K-dimensional o un modelo generado a partir de varios vectores K-dimensionales.

Suposiciones. Supongamos que:

- Existe un modelo estadístico G (Gausiana K-dimensional de media $\boldsymbol{\mu}_G$ y matriz de covarianza diagonal $\boldsymbol{\Sigma}_G$, con $\boldsymbol{\sigma}_G^2 = \mathrm{diag}(\boldsymbol{\Sigma}_G)$), en nuestro caso relacionado con un conjunto de usuarios de desarrollo, que se superpone en alguna medida con $\mathcal{C}$.
- Tenemos acceso a la evaluación de la función de comparación $J(\mathcal{C}, \mathbf{y})$ para diversas pruebas de $\mathbf{y}$.

Algoritmo. El problema de encontrar $\mathbf{y}^*$ se puede resolver adaptando la distribución global G a las particularidades locales de la plantilla $\mathcal{C}$, a través del siguiente algoritmo iterativo:

1. Se toman N muestras $(\mathbf{y}_i)$ de la distribución global G, y se calculan las puntuaciones de similitud $J(\mathcal{C}, \mathbf{y}_i)$, con $i = 1, \ldots, N$.
2. Se seleccionan los M puntos (con $M < N$) que han generado una puntuación mayor.
3. Se calcula la distribución local $L(\boldsymbol{\mu}_L, \boldsymbol{\sigma}_L)$, también Gausiana K-dimensional, basándonos en los M puntos seleccionados.
4. Se calcula la distribución adaptada $A(\boldsymbol{\mu}_A, \boldsymbol{\sigma}_A)$, también una Gausiana K-dimensional, que combina la información general proporcionada por $G(\boldsymbol{\mu}_G, \boldsymbol{\sigma}_G)$ y la información local dada por $L(\boldsymbol{\mu}_L, \boldsymbol{\sigma}_L)$. Esto se consigue adaptando los etadísticos principales como sigue:

$$\boldsymbol{\mu}_A = \alpha \boldsymbol{\mu}_L + (1 - \alpha)\boldsymbol{\mu}_G \tag{A.1}$$

$$\boldsymbol{\sigma}_A^2 = \alpha(\boldsymbol{\sigma}_L^2 + \boldsymbol{\mu}_L^2) + (1 - \alpha)(\boldsymbol{\sigma}_G^2 + \boldsymbol{\mu}_G^2) - \boldsymbol{\mu}_A^2 \tag{A.2}$$

5. Se redefine $G = A$ y se vuelve al paso 1.

En las Eq. (A.1) y (A.2), $\boldsymbol{\mu}^2$ se define como $\boldsymbol{\mu}^2 = \text{diag}(\boldsymbol{\mu}\boldsymbol{\mu}^T)$, y α es un coeficiente de adaptación que toma valores en el rango [0,1]. El algoritmo termina cuando una de las N puntuaciones de similitud calculadas en el paso 2 supera el umbral de decisión δ, o cuando se alcanza el número máximo de iteraciones.

En el algoritmo anterior hay dos conceptos clave que no deben confundirse, a saber: *i*) número de *iteraciones* (n_{it}), que es el número de veces que la distribución G es adaptada, y *ii*) número de comparaciones (n_{comp}), que denota el número total de comparaciones ejecutadas durante el algoritmo. Ambos números están relacionados a través del parámetro N, así $n_{comp} = N \cdot n_{it}$.

Método de detección de vida basado en medidas de calidad. El problema de detección de vida se puede ver como un problema de clasificación en el que una imagen de un rasgo biométrico (huella dactilar, en este caso concreto) debe ser asignada a una de dos clases: real (generada por un rasgo real) o falsa (generada por un rasgo artificial). El punto clave del proceso radica en encontrar un conjunto de parámetros discriminantes que permita construir un clasificador que nos devuelva la probabilidad de pertenencia de la imagen a cada una de las clases. En este caso proponemos una parametrización que utiliza medidas relacionadas con la calidad de la imagen de la huella.

En la Fig. 4.1 se muestra un diagrama general del sistema de detección de vida propuesto. El sistema requiere dos entradas: *i*) la imagen de la huella que se va a clasificar, y *ii*) el sensor que se utilizará en el proceso de adquisición.

El primer paso es segmentar la huella propiamente dicha del fondo de la imagen, para esto se utilizan filtros de Gabor en la configuración propuesta por Shen *et al.* [2001]. Una vez que la información útil de la imagen ha sido seleccionada, se extraen diez medidas de calidad que serán utilizadas como vector de características en la clasificación (los distintos rasgos extraídos se especifican a continuación). Antes del paso de clasificación, se seleccionan (utilzando búsqueda exhaustiva) las mejores características dependiendo del sensor utilizado en la adquisición. Una vez que se ha generado el vector de características final la huella se clasifica como real, o falsa, utilizando para ello como datos de entrenamiento del clasificador (LDA) el conjunto de datos de desarrollo correspondientes al sensor en uso.

A continuación se dan algunos detalles de las diez medidas de calidad extraídas de las imágenes de huellas, que estiman alguna de las propiedades siguientes: fuerza de las crestas, continuidad de las crestas, o claridad de las crestas [Alonso-Fernandez *et al.*, 2008].

- **Parámetros de medida de la fuerza de las crestas.**
  - *Nivel de Certidumbre de la Orientación (Q_{OCL})* [Lim *et al.*, 2002],que mide la concentración de energía a lo largo de la dirección dominante de las crestas utilizando el gradiente de intensidad. En la Fig. 4.3 se muestra un ejemplo de este parámetro para dos huellas de distinta calidad.
  - *Concentración de Energía en el Espectro de Potencia (Q_E)* [Chen *et al.*, 2005a], que se calcula sobre bandas de tipo anillo. Para ello, se utilizan una serie de filtros paso

banda que calculan la energía en cada una de las bandas. En la Fig. 4.4 se muestra un ejemplo de estimación de la calidad utilizando este parámetro para dos huellas de distinta calidad.

- **Parámetros de medida de la continuidad de las crestas.**
  - *Calidad de la Orientación Local (Q_{LOQ})* [Chen *et al.*, 2004], que nos da información de cómo de suavemente cambia la dirección de un bloque a otro de la imagen. En imágenes de alga calidad este cambio debe ser más progresivo, mientras que en imágenes de baja calidad el cambio es más brusco. En la Fig. 4.5 se muestra un ejemplo del cálculo de este parámetro para dos huellas de diferente calidad.
  - *Continuidad del Campo de Orientación (Q_{COF})* [Lim *et al.*, 2002]. Este método se basa en el hecho de que el cambio entre valles y crestas en las imágenes de alta calidad sucede de forma abrupta.
- **Parámetros de medida de la claridad de las crestas.**
  - *Media (Q_{MEAN})* y *Desviación Estándar (Q_{STD})* de los valores de la imagen de grises calculados a partir de la huella ya segmentada. Estos dos parámetros ya han sido considerados para la detección de vida por Coli *et al.* [2008].
  - *Puntuación de la Claridad Local (Q_{LCS1} y Q_{LCS2})* [Chen *et al.*, 2004]. La forma de onda sinusoidal que modela los valles y las crestas se utiliza para segmentar ambas regiones (ver Fig. 4.6) [Hong *et al.*, 1998]. La claridad se define como el área de solape de las distribuciones de grises de valles y crestas. En la Fig. 4.7 se muestra un ejemplo de cálculo de este parámetro para dos bloques de una huella dactilar con distinto nivel de calidad.
  - *Amplitud y varianza de la sinusoide que modela valles y crestas (Q_A and Q_{VAR})* [Hong *et al.*, 1998]. En base a estos parámetros los bloques se clasifican como buenos o malos. La calidad de la huella se calcula entonces como el porcentaje de bloques marcados como buenos.

En la Tabla 4.1 se presenta un resumen de las distintas medidas de calidad utilizadas como parametrización en el método de detección de vida propuesto.

Método de generación sintética de firmas basado en análisis frecuencial. Se describe aquí un método original basado en un modelo generativo, para la creación de firmas sintéticas utilizando la información obtenida del análisis de la trayectoria en el dominio de la frecuencia, y que no requiere de ninguna muestra real adquirida previamente para generar los rasgos sintéticos. El algoritmo, tal y como se puede ver en la Fig. 4.10, presenta dos etapas diferenciadas: en la primera se produce una firma matriz que se corresponde con un individuo sintético, utilizando el modelo generativo basado en la información frecuencial (no se utiliza ninguna firma real en

este proceso), en la segunda etapa se usa esa firma matriz para generar diferentes muestras del mismo usuario sintético.

A pesar de que una firma *on-line* pueda contener otras señales, tales como los ángulos de elevación y azimut, nosotros consideraremos que está definida por tres secuencias temporales $[x[n]\ y[n]\ p[n]]$ donde cada una de ellas se corresponde con las coordenadas x e y, y la presión p aplicada durante el proceso de firma en los instantes $n = 1, \ldots, N$.

El algoritmo propuesto para generar la firma matriz de los individuos sintéticos (primera etapa del algoritmo completo), está formada por tres pasos consecutivos tal y como se muestra en la Fig. 4.11:

- **Paso 1**. En el primer paso, llevado a cabo en el dominio de la frecuencia, se genera la Transformada de Fourier (TF) de las señales de la trayectoria x e y coloreando ruido blanco. Para ello se utiliza un modelo paramétrico obtenido a partir del análisis frecuencial de las firmas de un conjunto de usuarios de desarrollo. Los parámetros que definen el modelo son:

  - *Longitud de la firma* (N). Define la longitud de las tres funciones x, y, and p.
  - *Número de coeficientes espectrales relevantes*(N_R). Define el número de coeficientes de la TF que presentan un nivel de potencia alto (esto es, aquellos que se encuentran antes de la línea discontinua en la Fig. 4.12). Este parámetro se calcula como un porcentaje de N, $N_R = \delta N$, donde δ sigue una distribución uniforme entre $\delta^{\min} > 0$ y $\delta^{\max} < 1$.
  - *Relación de potencia* (G). Calculado como el cociente entre la potencia de los coeficientes relevantes, y los coeficientes finales (esto es, en la Fig. 4.12 aquellos que se encuentran tras la línea discontinua), $G = P_R/P_I$. El valor de G se toma de una distribución uniforme, $G \in [G^{\min}, G^{\max}]$.

- **Paso 2**. En el segundo paso, las funciones de la trayectoria resultantes se utilizan para situar los *penups* (trazos con presión cero) de la función de presión. Una vez ubicados los *penups*, se sitúan una serie de máximos entre ellos y la función de presión se genera utilizando un algoritmo de interpolación *spline* cúbica. En esta etapa se definen los siguientes parámetros:

  - *Número de Penups* (PU). Un *penup* es un segmento de la firma con presión cero (se genera al levantar el bolígrafo del papel durante el proceso de firma). Este parámetro es dependiente de la longitud de la firma N (esto es, firmas más largas tienen una probabilidad más alta de presentar un mayor número de *penups*).
  - *Ubicación de los penups.* A partir de un análisis heurístico de las señales y y p de firmas reales, podemos concluir que la mayor parte de *penups* se producen cerca de un punto singular de y (máximo o mínimo).

  - *Refinamiento de la señal de presión*: *i*) muchos dispositivos de adquisición toman 1024 niveles de presión, así pues las muestras de las señal p se redondean al valor entero más cercano y aquellas que superan 1024 se fijan a este valor, *ii*) igualmente, los valores de presión por debajo de 0 se sitúan en el valor mínimo, *iii*) se eliminan los *penups* al inicio o final de una firma, *iv*) se eliminan los *penups* no realistas (demasiado cortos o demasiado largos).

- **Paso 3**. En la tercera y última etapa, las tres señales se procesan en el dominio del tiempo para dar a las firmas sintéticas un aspecto más realista. Las acciones realizadas en esta etapa son:

  - Ambas funciones de la trayectoria x e y se suavizan utilizando un algoritmo de media flotante para eliminar posible ruido de alta frecuencia.
  - En la mayor parte de las firmas realizadas de izquierda a derecha la función x presenta una tendencia creciente, fluctuando alrededor de una recta de pendiente fija. Este comportamiento global se añade de forma artificial en este paso del algoritmo.
  - En muchos casos, las firmas reales presentan al final de las señales x e y una gran forma sinusoidal, que en la mayor parte de los casos se corresponde con una rúbrica de aspecto redondeado. Esta forma de onda final se añade también en esta parte del algoritmo.
  - Además, en este punto se pueden aplicar si se considera necesario transformaciones de rotación, traslación y escalado.

En la segunda etapa del algoritmo de generación de firmas sintéticas (mostrada en la Fig. 4.13), se producen diferentes impresiones de una firma matriz previamente generada en la primera etapa. Con este propósito se consideran tres tipos de distorsiones:

- *Adición de ruido* (SNR). Se añade ruido paso bajo n_x y n_y a las señales de la trayectoria x e y de tal forma que las señales resultantes x_n e y_n presenten una determinada relación señal a ruido (SNR) SNR_x y SNR_y (definida como el cociente entre la potencia de la señal P_x, y la potencia de ruido P_{nx}, esto es, $\text{SNR}_x = P_x/P_{nx}$). La SNR debe variar dependiendo de si queremos generar muestras de la misma sesión o de diferentes sesiones. En nuestros experimentos asumimos que el ruido está incorrelado con las señales de la firma.

  En este paso del algoritmo no se introduce ninguna distorsión a la señal de presión (p).

- *Remuestreo/Submuestreo* (M). Este paso es equivalente a una expansión o contracción temporal de las señales (se aplica la misma expansión o contracción a todas ellas). Considerando T como la duración de una firma (la misma para la función de presión y las de la trayectoria), la duración de la nueva firma expandida/contraída se calcula como $T_M = (1 + M)T$.

El valor del factor de remuestreo/submuestreo M se toma de una distribución uniforme diferente dependiendo de si se quiere generar variabilidad de tipo intrasesión ($M \in [-M^{\text{intra}}, M^{\text{intra}}]$), o intersesión ($M \in [-M^{\text{inter}}, M^{\text{inter}}]$), siendo en general $|M^{\text{intra}}| < |M^{\text{inter}}|$.

- *Amplificación/Atenuación* (α). Finalmente se aplica un escalado afín a las tres señales en función del parámetro α (que varía para cada una de las señales) [Munich and Perona, 2003]. De forma análoga al parámetro de remuestreo M, el factor de amplificación α sigue una distribución uniforme entre $[-\alpha_x^{\text{intra}}, -\alpha_x^{\text{intra}}]$ para muestras intrasesión, y entre $[-\alpha_x^{\text{inter}}, -\alpha_x^{\text{inter}}]$ para muestras intersesión (análogamente para y y p). Para un determinado valor de α_x, la función escalada x_α se calcula como $x_\alpha = (1 + \alpha_x)x$.

En la Fig. 4.14 se muestran tres muestras de cinco firmantes reales (arriba) y sintéticos (debajo). Las firmas reales provienen de la base de datos MCYT [Ortega-Garcia *et al.*, 2003], y los individuos sintéticos fueron generados siguiendo el método propuesto en la Tesis y descrito anteriormente. Las funciones de la trayectoria y de presión de la primera muestra de cada firmante se muestran debajo. Se puede observar que, aunque no se distinga ningún carácter reconocible en las firmas sintéticas, su aspecto y el de sus funciones temporales es muy similar al de las firmas reales.

A.4. Evaluación de Seguridad de Sistemas de Verificación de Huella Dactilar

Este primer capítulo experimental se basa en las publicaciones: Galbally *et al.* [2009a,b, 2008a, 2006]; Martinez-Diaz *et al.* [2006].

En este capítulo se analizan las vulnerabilidades de sistemas de reconocimiento de huella dactilar a diferentes tipos de ataques directos e indirectos (ver Fig. 2.2 para una clasificación de los ataques a un sistema biométrico), y se proponen diversas contramedidas para reducir los efectos de este tipo de amenazas.

En un primer estudio se evalúan ataques directos realizados con huellas de goma generadas a partir de una huella latente y de una plantilla estándar ISO.

Los ataques con dedos de goma generados a partir de huellas latentes se realizan contra el sistema basado en minucias NFIS2 del NIST Americano (*National Institute for Standards and Technology*), y contra un sistema propietario basado en el análisis del patrón de crestas. Para ello se utiliza una base de datos de huellas reales y falsas de 68 dedos, generada con y sin la cooperación del usuario legítimo (ver Figs. 5.1 y 5.2), y capturada con tres sensores diferentes: óptico, térmico y capacitivo (ver Figs. 5.3 y 5.4). Se consideran dos escenarios de ataque, a saber: *i*) registro y prueba con huellas de goma, y *ii*) registro con huellas reales y prueba con sus correspondientes imitaciones. Se presentan resultados estadísticamente significativos sobre el rendimiento de los ataques comparándolos con el modo normal de operación del sistema.

Los resultados (ver Tabla 5.1) muestran que, cuando se considera el sistema basado en minucias, el éxito de los ataques es muy dependiente de la calidad de las huellas de goma: cuanto mejor es la calidad de las imágenes capturadas a partir de las huellas falsas, más vulnerable es el sistema a ambos ataques. El sistema basado en el patrón de crestas es más resistente a las imágenes de buena calidad de las huellas falsas y, en general, a variaciones en la calidad de la imagen de la huella dactilar.

En el caso de ataques directos realizados usando dedos de goma generados a partir de una plantilla estándar ISO de un usuario genuino (ver Fig. 5.7), la evaluación de vulnerabilidades se realiza sobre un sistema basado en minucias (siguiendo el estándar ISO), y utilizando una base de datos de disponibilidad pública [Fierrez *et al.*, 2007b].

Los resultados obtenidos (ver Tabla 5.2), apoyados sobre un estudio de la calidad de las imágenes de las huellas dactilares (ver Fig. 5.12), demuestran la viabilidad del ataque y la falta de robustez de los sistemas automáticos de reconocimiento de huella dactilar contra esta amenaza. El hecho de que este tipo de ataques directos se realice comenzando a partir de la plantilla robada de un usuario, y no de una huella latente que se haya recuperado, refuerza la idea de que este proceso de ingeniería inversa (esto es, recuperar la huella dactilar a partir de la información de las minucias) es totalmente viable, poniendo así en entredicho la creencia generalizada de la no invertibilidad de las plantillas de huella dactilar.

Además, el estudio destapa un problema clave sobre las vulnerabilidades que puede suscitar el uso de estándares. Es incuestionable la conveniencia de los estándares para la interoperabilidad de sistemas y el desarrollo de la tecnología biométrica. Sin embargo, no podemos olvidar que los estándares proporcionan información muy valiosa sobre el funcionamiento del sistema (p.ej., formato de almacenamiento de las plantillas) que puede ser utilizada para llevar a cabo ataques como los evaluados en esta Tesis en caso de que una plantilla de usuario se vea comprometida.

Los resultados alcanzados en estas dos evaluaciones de seguridad contra ataques directos refuerzan la necesidad de considerar y diseñar contramedidas específicas que minimicen los riesgos que conllevan este tipo de amenazas (p.ej., protección específica para plantillas [Clancy *et al.*, 2003; Ratha *et al.*, 2007], técnicas de detección de vida [Antonelli *et al.*, 2006; Tan and Schuckers, 2006], o arquitecturas de autenticación multimodal [Fierrez-Aguilar *et al.*, 2005c]). En el presente estudio se analiza el rendimiento del método de detección de vida propuesto en la Tesis para lograr protección frente a este tipo de ataques. Los resultados demuestran que el esquema propuesto es una herramienta eficaz para prevenir los ataques directos, siendo capaz de detectar por encima del 98% de los intentos ilegales de acceso utilizando dedos de goma (ver Tablas 5.5 y 5.6).

Finalmente se evalúan las vulnerabilidades de dos sistemas de verificación en huella frente a ataques indirectos. Se analiza la resistencia de los sistemas, uno funcionando sobre un PC y el otro un sistema integrado en una tarjeta inteligente, contra ataques de tipo *hill-climbing*. Los experimentos se realizan sobre un subconjunto de la base de datos MCYT [Ortega-Garcia *et al.*, 2003]. Los ataques muestran una gran dependencia del tipo de iteraciones realizadas y del sistema evaluado (ver Tablas 5.3 y 5.4). Para un número suficiente de iteraciones se obtienen

tasas de acierto por encima del 90% para ambos sistemas, siendo el soportado por un PC el que requiere de un mayor número de intentos de acceso para ser roto. Se estudia la cuantificación de puntuaciones como una posible contramedida contra los ataques *hill-climbing* probando ser un método eficiente para prevenir estas amenazas (ver Tabla 5.7). Es interesante el resaltar que no todas las huellas dactilares muestran el mismo grado de resistencia a los ataques, siendo algunas de ellas mucho más difíciles de romper que otras (ver Figs. 5.15 y Fig. 5.16).

A.5. Evaluación de Seguridad de Sistemas de Verificación de Firma Dinámica

Este segundo capítulo experimental se basa en las publicaciones: Galbally *et al.* [2009d,e, 2007, 2008b].

En este capítulo se realiza la evaluación de seguridad de distintos sistemas de verificación de firma dinámica contra dos tipos distintos de ataques indirectos (el primero de ellos un ataque de tipo fuerza bruta realizado con firmas sintéticas, y el segundo un ataque *hill-climbing*), y se propone una contramedida para cada uno de ellos.

En el caso del ataque de tipo fuerza bruta los experimentos se llevan a cabo atacando con firmas sintéticas (generadas con el método original propuesto en esta Tesis) modelos de firmas reales obtenidos a partir de un sistema de reconocimiento basado en HMMs (*Hidden Markov Models*).

Los resultados muestran la viabilidad de este tipo de ataques y acentúan la necesidad de considerar esta vulnerabilidad a la hora de diseñar aplicaciones biométricas de seguridad (ver Tabla 6.2). Con el objetivo de dar protección frente al ataque se analiza la posibilidad de utilizar muestras sintéticas generadas a partir de una real en la etapa de registro, para aumentar la robustez del sistema frente a la variabilidad intrausuario y así disminuir su FAR. Los resultados muestran que el uso de firmas generadas sintéticamente mejora significativamente la tasa de error del sistema, con ganancias de hasta un 70% para el caso de los escenarios de operación más realistas (ver Tabla 6.6). Como resultado, puede decirse que el complementar los datos de usuario con datos sintéticos en la etapa de registro es capaz de mejorar el rendimiento de los sistemas de verificación de firma disminuyendo así la tasa de éxito de un ataque por fuerza bruta.

El algoritmo tipo *hill-climbing* basado en adaptación Bayesiana propuesto en la tesis se utiliza para atacar un sistema de verificación de firma basado en parámetros globales. Los experimentos muestran un rendimiento muy alto del algoritmo, que alcanza una tasa de éxito de más del 95% para la mejor configuración de parámetros encontrada (ver Tabla 6.5).

El rendimiento del ataque *hill-climbing* se compara directamente con el de un ataque tipo fuerza bruta. El algoritmo iterativo necesita menos comparaciones para romper el sistema que el de fuerza bruta para dos de los tres puntos de operación evaluados (ver Tabla 6.5). Nótese sin embargo, que los medios requeridos por ambos métodos no son comparables. Para llevar a cabo un ataque de fuerza bruta, el intruso debe tener una base de datos de más de mil firmas

reales, mientras que en el caso del algoritmo *hill-climbing* no se necesita ninguna plantilla real para tener éxito en el ataque.

Como contramedida para prevenir este fallo en la seguridad se analiza comparativamente el subconjunto de parámetros más resistentes al ataque y aquellos que dan un mejor rendimiento en el modo normal de operación del sistema. Se demuestra experimentalmente que los parámetros más discriminantes son los que contienen información geométrica, y los menos discriminantes aquellos que se relacionan con la dirección de la firma. Por otra parte, las características más resistentes son las concernientes a la información temporal mientras que los más vulnerables son los relacionados con la velocidad (ver Tabla 6.8).

Los experimentos también muestran que, aunque se debe llegar a un compromiso entre rendimiento y resistencia frente a ataques, los subconjuntos más resistentes no disminuyen significativamente la vulnerabilidad del sistema comparado con los que ofrecen un mejor rendimiento, mientras que el número de errores cometido por el sistema aumenta de forma clara (ver Fig. 6.10). Así, es más aconsejable buscar conjuntos de parámetros que mejoran el rendimiento del sistema que aquellos que mejoran su resistencia frente a ataques.

A.6. Evaluación de Seguridad de Sistemas de Verificación de Cara

Este tercer capítulo experimental se basa en las publicaciones: Galbally *et al.* [2010, 2009g].

En este capítulo se estudia la resistencia de dos sistemas de verificación de cara contra el algoritmo *hill-climbing* Bayesiano propuesto en la Tesis: uno basado en *Principal Component Analysis* (PCA) y el otro en *Gaussian Mixture Models* (GMM). Los resultados experimentales muestran que ambos sistemas de verificación son muy vulnerables a este método de ataque que obtiene por encima de un 85% de tasa de acierto para todos los casos considerados, incluso cuando no se utiliza ninguna imagen real para inicializar el algoritmo (ver Tablas 7.4 y 7.6). Además, el ataque muestra su capacidad para reconstruir la imagen de la cara del usuario a partir de las puntuaciones de similitud, con los problemas de privacidad que esto conlleva (ver Figs. 7.6 y 7.7).

El rendimiento del algoritmo *hill-climbing* basado en adaptación Bayesiana se compara con el de un ataque tipo fuerza bruta (ver Tablas 7.4 y 7.6). Se observa que método iterativo es más eficiente para todas las condiciones analizadas, con la ventaja añadida de requerir muchos menos recursos (no se necesita ninguna imagen real para lanzar el ataque, mientras que en el caso de fuerza bruta el intruso debe tener acceso a una gran base de datos de imágenes de cara).

Los resultados también muestran que el sistema basado en GMM, aun siendo su rendimiento global bajo condiciones normales de trabajo mejor que el del sistema basado en PCA, es muy vulnerable a ataques aleatorios llevados a cabo con plantillas generadas replicando un bloque de imagen promedio (ver Tabla 7.5). Este fallo de la seguridad se puede prevenir incorporando a los sistemas mecanismos de detección de patrones duplicados dentro de las imágenes.

Al mismo tiempo, este estudio confirma el serio riesgo que supone el algoritmo *hill-climbing*

Bayesiano ya que ha sido utilizado para atacar con éxito no sólo distintos comparadores sino también distintos rasgos biométricos (en el capítulo experimental anterior ya había conseguido romper con una alta tasa de éxito sistemas de verificación de firma dinámica). Además, los resultados experimentales alcanzados en ambas evaluaciones (contra sistemas de verificación de firma y cara), demuestran la consistencia de comportamiento del algoritmo y su capacidad de adaptación a escenarios totalmente distintos (ver Tablas 6.5 y 7.4). Por tanto, esta amenaza debe ser estudiada y tenida en cuenta a la hora de diseñar sistemas biométricos de seguridad que utilicen vectores de características de longitud fija (formados por números reales), y que devuelvan puntuaciones de similitud reales.

Además, el ataque muestra un alto grado de resistencia contra medidas de protección basadas en cuantificación de puntuaciones (especialmente en el caso del sistema basado en GMMs), alcanzando tasas de éxito por encima del 15% para todos los casos de cuantificación considerados (ver Tablas 7.7 y 7.10).

A.7. Líneas de Trabajo Futuro

Se proponen las siguientes líneas de trabajo futuro relacionadas con el trabajo desarrollado en esta Tesis:

- Aplicar la metodología de evaluación de seguridad a otras modalidades biométricas. Se han publicado ya diversos trabajos en los que los autores estudian la viabilidad de realizar distintos ataques (en general ataques directos) sobre sistemas biométricos basados en rasgos distintos a los considerados en esta Tesis, como por ejemplo iris [Matsumoto, 2004; Thalheim and Krissler, 2002], geometría de la mano y patrón de vasos sanguíneos [Geradts and Sommer, 2006], o voz [Bonastre *et al.*, 2007]. Utilizar las pautas de evaluación seguidas en la Tesis para analizar estas vulnerabilidades ayudaría a comprender mejor la magnitud de las amenazas.

- Buscar nuevas vulnerabilidades de los sistemas biométricos. Por ejemplo, la seguridad de los sistemas biométricos podría ser rota a partir de ataques tipo *side-channel* (p.ej., los *timing-attacks* [Kocher, 1995], o los ataques que utilizan el Análisis Diferencial de Potencia [Kocher *et al.*, 1999]). Estos métodos de ataque intentan aprovechar parámetros del sistema fáciles de medir (tales como la respuesta temporal, o el consumo de potencia) para obtener acceso a la aplicación, y han sido ampliamente estudiados en otras tecnologías aplicadas a la seguridad como la criptografía. Recientemente se ha demostrado que en algunos sistemas biométricos, el tiempo de comparación y la puntuación devuelta por el comparador no son independientes, y que esta correlación podría usarse para acceder fraudulentamente al sistema [Galbally *et al.*, 2009c].

- Generar nuevos métodos de detección de vida basados en medidas de calidad para otros rasgos biométricos diferentes a las huellas dactilares. La evaluación de calidad es un campo

de investigación que no ha recibido hasta tiempos recientes atención específica por parte de la comunidad biométrica [ISO/IEC 29794-1, 2006; NIST, 2006]. La evaluación de calidad de las muestras biométricas podría ser utilizada, tal y como se ha hecho en esta Tesis para la huella dactilar, para desarrollar técnicas de detección de vida en otros rasgos como el iris [Chen *et al.*, 2006], o la cara [Kryszczuk and Drygajlo, 2007].

- Evaluar la resistencia de los sistemas biométricos multimodales contra el ataque *hill-climbing* Bayesiano propuesto en esta Tesis. Se ha afirmado en distintos trabajos que los sistemas multimodales son más resistentes frente a ataques que aquellos que funcionan sobre un único rasgo biométrico [Jain *et al.*, 2006; Prabhakar *et al.*, 2003], sin embargo, su nivel de seguridad real aún no ha sido analizado. Se ha demostrado que el ataque *hill-climbing* Bayesiano propuesto en esta Tesis es capaz de adaptarse a diferentes sistemas que utilizan vectores de características de número reales y de longitud fija, de forma que podría ser utilizado para evaluar, no los sistemas unimodales independientes, sino un sistema multimodal completo con una sola entrada (la plantilla que contiene diferentes rasgos biométricos), y una sola salida (la puntuación ya fusionada).

- Combinar el modelo de generación sintética de firma manuscrita propuesto en la Tesis con otros métodos existentes [Djioua and Plamondon, 2009], para lograr un estudio en profundidad de la información individual contenida en las firmas que nos permita mejorar nuestra comprensión sobre las características de aquellas muestras más resistentes a los ataques e imitaciones.

- Estudiar la viabilidad de aplicar a la generación de escritura un método basado en el análisis espectral similar al utilizado en esta Tesis para la generación de firmas sintéticas. Esto proporcionaría una alternativa a los métodos actuales basados en la concatenación de caracteres reales previamente adquiridos [Guyon, 1996; Lin and Wang, 2007; Varga *et al.*, 2005].

- Estudiar nuevas contramedidas preventivas basadas en la protección de plantillas [Adler, 2008; Jain *et al.*, 2008a]. Este tipo de métodos serían especialmente relevantes para la protección frente al ataque directo utilizando dedos de goma generados a partir de plantillas ISO descrito en esta Tesis.

References

A. Abhyankar and S. Schuckers. Characterization, similarity score, and uniqueness associated with perspiration pattern. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 301–309. Springer LNCS-3546, 2005. xix, 31

A. Adler. Sample images can be independently restored from face recognition templates. In *Proc. Canadian Conference on Electrical and Computer Engineering (CCECE)*, volume 2, pages 1163–1166, 2003. xix, xix, 24, 25

A. Adler. Images can be regenerated from quantized biometric match score data. In *Proc. Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 469–472, 2004. 10, 24, 28, 64, 128, 137, 157, 158, 175, 190

A. Adler. Vulnerabilities in biometric encryption systems. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 1100–1109. Springer LNCS-3546, 2005. 2, 24, 186

A. Adler. *Handbook of biometrics*, chapter Biometric system security, pages 381–402. Springer, 2008. 19, 28, 182, 209

F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally, and J. Ortega-Garcia. Robustness of signature verification systems to imitators with increasing skills. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009. 24

F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun. A comparative study of fingerprint image quality estimation methods. *IEEE Trans. on Information Forensics and Security*, 2(4):734–743, 2008. 67, 103, 116, 200

ANSI-NIST. ANSI x9.84-2001, biometric information management and security, 2001. 114, 161

ANSI/NIST. NIST ITL american national standards for biometrics, 2009. http://fingerprint.nist.gov/standard/. 1, 183

A. Antonelli, R. Capelli, D. Maio, and D. Maltoni. Fake finger detection by skin distortion analysis. *IEEE Trans. on Information Forensics and Security*, 1:360–373, 2006. xix, 28, 30, 31, 130, 205

B. S. Atal. Automatic recognition of speakers from their voices. *Proc. of IEEE*, 64:460–475, 1976. 1, 37, 183

E. Bailly-Bailliere, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz, J. Matas, K. Messer, V. Popovici, F. Poree, B. Ruiz, and J.-P. Thiran. The BANCA database and evaluation protocol. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 625–638. Springer LNCS-2688, 2003. 47

D. Baldiserra, A. Franco, D. Maio, and D. Maltoni. Fake fingerprint detection by odor analysis. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 265–272. Springer LNCS-3832, 2006. 30, 32

L. Ballard, D. Lopresti, and F. Monrose. Forgery quality and its implications for behavioral biometric security. *IEEE Trans. on Systems, Man, and Cybernetics*, 37:1107–1118, 2007. 34, 79

A. M. Bazen and S. H. Gerez. Fingerprint matching by thin-plate spline modelling of elastic deformations. *Pattern Recognition*, 36:1859–1867, 2003. 30

BC. Biometrics consortium, 2009. (http://www.biometrics.org/). 1, 183

BEM. Biometric Evaluation Methodology. v1.0, 2002. 2, 9, 41, 187, 189, 195

C. Bergman. *Advances in biometrics*, chapter Match-on-card for secure and scalable biometric authentication, pages 407–421. Springer, 2008. 3, 117

H. Bezine, M. Kefi, and M. Alimi. On the beta-elliptic model for the control of the human arm movement. *International Journal of Pattern Recognition*, 21:5–19, 2007. 35

BF. The biometric foundation, 2009. (http://www.biometricfoundation.org/). 1, 183

BI. Biometrics institute, 2009. (http://www.biometricsinstitute.org/). 1, 183

J. Bigun. *Vision with Direction*. Springer, 2006a. 67

J. Bigun. *Vision with Direction: A Systematic Introduction to Image Processing and Computer Vision*. Springer, 2006b. 13

J. Bigun, H. Fronthaler, and K. Kollreider. Assuring liveness in biometric identity authentication by real-time face tracking. In *Proc. IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS)*, pages 104–112, 2004. 32

BioAPI. The BioAPI consortium, 2009. http://www.bioapi.org. 1, 127, 175, 183

Biometrika, 2009. http://www.biometrika.it/eng/. 31

BioSec, 2004. Biometrics and Security, FP6 IP IST-2002-001766. (http://www.biosec.org/). 1, 46, 183

Biosecure, 2007. Biometrics for Secure Authentication, FP6 NoE IST-2002-507634. (http://www.biosecure.info/). 1, 16, 46, 183, 194

BiosecurID, 2003. BiosecurID: Seguridad Multimodal basada en Autenticacion Biometrica mediante Fusion de Expertos Unimodales, MCYT TIC2003-08382-C05. 44, 48

S. Bistarelli, F. Santini, and A. Vaccarelli. An asymmetric fingerprint matching algorithm for java card tm. *Pattern Analysis & Applications*, 9(4):359–376, 2006. 117

A. Black and N. Campbell. Optimizing selection of units from speech database for concatenative synthesis. In *Proc. European Conf. on Speech Communication and Technology (EUROSPEECH)*, pages 581–584, 1995. 34

J. Blomme. Evaluation of biometric security systems agains artificial fingers. Master's thesis, Linkoping University, 2003. 23

J.-F. Bonastre, D. Matrouf, and C. Fredouille. Artificial impostor voice transformation effects on false acceptance rates. In *Proc. Interspeech*, 2007. 181, 208

M. Bone and D. Blackburn. Face recognition at a chokepoint. Technical report, DoD Counterdrug Technology Development Program Office, November 2002. 38

M. Bone and C. Crumbacker. Facial recognition: Assessing its viability in the corrections environment. *Corrections Today Magazine*, pages 62–64, July 2001. 38

K. W. Boyer, V. Govindaraju, M. Nixon, and N. Ratha, editors. *Proc. of Second International Conference Biometrics: Theory, advances and systems (BTAS)*, 2008. IEEE Press. 1, 183

BSI. Biometric services international, 2009. (http://www.biometricsinternational.org/). 2, 38, 186

I. Buhan and P. Hartel. The state of the art in abuse of biometrics. Technical report, University of Twente, 2005. 19

BWG. Biometric security concerns, v1.0. Technical report, CESG, UK Government, 2003. 7, 8, 188, 189

BWG. Communications-electronics security group (CESG) – biometric working group (BWG) (UK government), 2009. http://www.cesg.gov.uk/policy_technologies/biometrics/index.shtml. 1, 2, 7, 183, 187, 188

Canadian Certification Body. Eal2 evaluation of bioscrypt enterprise for nt logon. Technical report, Government of Canada, Communications Security Establishment, 2001. Available on-line at http://www.commoncriteriaportal.org/files/epfiles/CRdf. 3, 187

R. Cappelli. *Handbook of Fingerprint Recognition*, chapter Synthetic Fingerprint Generation, pages 203–231. Springer, 2003. xix, 26, 33, 35, 44, 79, 107

R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Can fingerprints be reconstructed from iso templates? In *Proc. IEEE Int. Conf. on Control Automation Robotics and Vision (ICARCV)*, pages 191–196, 2006a. 107

R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Evaluating minutiae template vulnerability to masquerade attack. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 174–179, 2007a. 26, 107, 109

R. Cappelli, D. Maio, A. Lumini, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29:1489–1503, September 2007b. 26, 106, 107, 108, 109, 112, 113, 132

R. Cappelli, D. Maio, and D. Maltoni. Modelling plastic distortion in fingerprint images. In *Proc. Int. Conf. on Advances in Pattern Recognition (ICAPR)*, pages 369–376. Springer LNCS-2013, 2001. 30

R. Cappelli, D. Maio, and D. Maltoni. Synthetic fingerprint-database generation. In *Proc. IEEE Int. Conf. on Pattern Recognition (ICPR)*, volume 3, pages 744–747, 2002. xix, 26

R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain. Performance evaluation of fingerprint verification systems. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(1):3–18, 2006b. 1, 33, 38, 44, 117, 132, 183

F. Cardinaux, C. Sanderson, and S. Marcel. Comparison of MLP and GMM classifiers for face verification on xm2vts. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 911–920. Springer LNCS-2688, 2003. 159

A. Cavoukian, A. Stoianov, and F. Carter. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. In *Proc. International Federation for Information Processing (IFIP)*, pages 57–77, 2008. 28

CC. Common Criteria for Information Technology Security Evaluation. v3.1, 2006. Available on-line at http://www.commoncriteriaportal.org/. 2, 9, 41, 187, 189, 195

CC. Common criteria protection profiles, 2009a. http://www.commoncriteriaportal.org/pp.html. 2, 187

CC. Common Criteria Supporting Documents, 2009b. http://www.commoncriteriaportal.org/supdocs.html. 2, 187

CCVS. Common vulnerability scoring system, version 2.0, 2007. Available on line at http://www.first.org/cvss/cvss-guide.html. 2, 187

CEM. Common Methodology for Information Technology Evaluation. v3.1., 2006. 2, 187

T. Chen, X. Jiang, and W. Yau. Fingerprint image quality analysis. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, volume 2, pages 1253–1256, 2004. 69, 70, 103, 104, 201

Y. Chen, S. Dass, and A. Jain. Fingerprint quality indices for predicting authentication performance. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 160–170. Springer LNCS-3546, 2005a. 68, 69, 103, 200

Y. Chen, S. Dass, and A. Jain. Localized iris image quality using 2-d wavelets. In *Proc. IAPR Int. Conf. on Biomtrics (ICB)*, pages 373–381. Springer LNCS-3832, 2006. 182, 209

Y. Chen, S. Dass, A. Ross, and A. K. Jain. Fingerprint deformation models using minutiae locations and orientations. In *Proc. IEEE Workshop on Applications of Computer Vision (WACV)*, pages 150–156, 2005b. 30

Y. Chen and A. K. Jain. Fingerprint deformation for spoof detection. In *Proc. IEEE Biometric Symposium (BSym)*, pages 19–21, 2005. 29, 31

G. Chetty and M. Wagner. Liveness detection using cross-modal correlations in face-voice person authentication. In *Proc. European Conf. on Speech, Communication and Technology (INTERSPEECH)*, pages 2181–2184, 2005. 32

C. Chibelushi, S. Gandon, J. S. D. Mason, F. Deravi, and R. D. Johnston. Design issues for a digital integrated audio-visual database. In *Proc. IEE Colloquium on Integrated Audio-Visual Processing for Recognition, Synthesis and Communication*, pages 7/1–7/7, November 1999. 47

C. C. Chibelushi, F. Deravi, and J. Mason. A review of speech-based bimodal recognition. *IEEE Trans. on Multimedia*, 4:23–37, 2002. 28, 32

T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. In *Proc. ACM Workshop on Biometrics Methods and Applications (ACMSIGMM)*, pages 45–52, 2003. 130, 205

P. Coli, G. L. Marcialis, and F. Roli. Power spectrum-based fingerprint vitality detection. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 169–173, 2007. 32

P. Coli, G. L. Marcialis, and F. Roli. Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device. *Int. Journal of Image and Graphics*, pages 495–512, 2008. 30, 32, 70, 77, 201

COST. COST 2101: Biometrics for identity documents and smart cards, 2007. http://cost2101.org/. 1, 183

J. Cui, Y. Wang, J. Huang, T. Tan, and Z. Sun. An iris image synthesis method based on pca and super-resolution. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 471–474, 2004. 35

J. Daugman. Iris recognition and anti-spoofing countermeasures. In *Proc. Int. Biometrics Conf. (IBC)*, 2004. 29

B. DeCann, B. Tan, and S. Schuckers. A novel region based liveness detection approach for fingerprint scanners. In *Proc. IAPR/IEEE Int. Conf. on Biometrics*, pages 627–636. Springer LNCS-5558, 2009. 30

R. Derakhshani, S. Schuckers, L. Hornak, and L. O'Gorman. Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition*, 36:383–396, 2003. 30

D. Dessimoz, J. Richiardi, C. Champod, and A. Drygajlo. Multimodal biometrics for identity documents (MBioID). *Forensic Science International*, 167:154–159, 2007. 47

M. Djioua, C. O'Reilly, and R. Plamondon. An interactive trajectory synthesizer to study outlier patterns in handwriting recognition and signature verification. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 1124–1127, 2006. 34

M. Djioua and R. Plamondon. A new algorithm and system for the characterization of handwriting strokes with delta-lognormal parameters. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2009. to appear. 35, 132, 182, 209

DoD. Biometrics Management Office, Department of Defense, USA, 2009. http://www.biometrics.dod.mil/. 1, 183

R. O. Duda, P. E. Hart, and D. G. Stork. *Pattern Classification*. Wiley, 2001. 13, 63, 64, 71, 199

B. Dumas, J. Hennebert, A. Humm, R. Ingold, D. Petrovska, C. Pugin, and D. V. Rotz. MyIdea - Sensors specifications and acquisition protocol. Computer Science Department Research Report DIUF-RR 2005.01, University de Fribourg in Switzerland, 2005. 47

T. Dutoit. *An introduction to text-to-speech synthesis*. Kluwer Academic Publishers, 2001. 33

EBF, 2009. European Biometrics Forum. (http://www.eubiometricforum.com/). 1, 183

A. Eriksson and P. Wretling. How flexible is the human voice? In *Proc. European Conf. on Speech Technologies (EUROSPEECH)*, pages 1043–1046, 1997. 21

M. Faundez-Zanuy, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. Multimodal biometric databases: An overview. *IEEE Aerospace and Electronic Systems Magazine*, 21:29–37, 2006. 44

J. Fierrez. *Adapted Fusion Schemes for Multimodal Biometric Authentication*. PhD thesis, Universidad Politecnica de Madrid, 2006. 45

J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. G. de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications*, 2009. To appear. 37, 43, 44, 80, 84, 133

J. Fierrez and J. Ortega-Garcia. *Handbook of biometrics*, chapter On-line signature verification, pages 189–209. Springer, 2008. 33, 87

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*, 8:2325–2334, 2007a. 88

J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez. BioSec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40:1389–1392, 2007b. 43, 44, 46, 98, 107, 111, 113, 129, 205

J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, and A. Jain. Incorporating image quality in multi-algorithm fingerprint verification. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 213–220. Springer LNCS-3832, 2006. 98, 103, 116

J. Fierrez-Aguilar, D. Garcia-Romero, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. Bayesian adaptation for user-dependent mulitmodal biometric authentication. *Pattern Recognition*, 38:1317–1319, 2005a. 64, 65

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. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 523–532. Springer LNCS-3546, 2005b. xxi, xxiii, xxvi, xxvii, 87, 131, 133, 134, 137, 139, 146, 149, 150, 151, 152

J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun. Discriminative multimodal biometric authentication based on quality measures. *Pattern Recognition*, 38(5):777–779, 2005c. 43, 61, 128, 130, 205

P. J. Flynn. *Handbook of Biometrics*, chapter Biometric Databases. Springer, 2007. 43

H. Fronthaler, K. Kollreider, J. Bigun, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. Fingerprint image quality estimation and its application to multi-algorithm verification. *Trans. on Information Forensics and Security*, 3(2):331–338, 2008. 98

K. Fukunaga. *Introduction to statistical pattern recognition*. Academic Press, 1990. 159

FVC. Fingerprint Verification Competition, 2006. (http://bias.csr.unibo.it/fvc2006). 117

J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. Fingerprint liveness detection based on quality measures. In *Proc. IEEE Int. Conf. on Biometrics, Identity and Security (BIdS)*, 2009a. 14, 19, 64, 94, 192, 204

J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters*, 2009b. to appear. 15, 94, 193, 204

J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez. Fake fingertip generation from a minutiae template. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 1–4, 2008a. 15, 94, 193, 204

J. Galbally, S. Carballo, J. Fierrez, and J. Ortega-Garcia. Vulnerability assessment of fingerprint matching based on time analysis. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BIOID)*. Springer LNCS-5707, 2009c. 27, 181, 208

J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Evaluation of brute-force attack to dynamic signature verification using synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Machine Intelligence (ICDAR)*, 2009d. 132, 206

J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Improving the enrollment in dynamic signature verification with synthetic samples. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, 2009e. 15, 64, 132, 194, 206

J. Galbally, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia. Synthetic generation of handwritten signatures based on spectral analysis. In *Proc. SPIE Biometric Technology for Human Identification VI (BTHI VI)*, 2009f. 14, 44, 64, 192

J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 386–395. Springer LNCS-4642, 2007. 15, 41, 60, 64, 132, 193, 196, 206

J. Galbally, J. Fierrez, and J. Ortega-Garcia. Performance and robustness: a trade-off in dynamic signature verification. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1697–1700, 2008b. xxi, 87, 88, 132, 206

J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador. On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, volume 1, pages 130–136, 2006. 14, 19, 60, 93, 94, 193, 204

J. Galbally, C. McCool, J. Fierrez, and S. Marcel. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, 2010. to appear. 14, 15, 19, 157, 192, 193, 207

J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia. Hill-climbing attack to an eigenface-based face verification system. In *Proc. IEEE Int. Conf. on Biometrics, Identity and Security (BIdS)*, 2009g. 157, 207

S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J. L. les Jardins, J. Lunter, Y. Ni, and D. Ptrovska-Delacretaz. BIOMET: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 845–853. Springer LNCS-2688, 2003. 44, 46

M. Garris, C. Watson, R. McCabe, and C. Wilson. *User's guide to NIST Fingerprint Image Software 2 (NFIS2)*. National Institute of Standards and Technology, 2004. 95, 118

Z. Geradts and P. Sommer. Forensic implications of identity systems. Technical report, Future of Identity in the Information Society (FIDIS) Consortium, 2006. 22, 181, 208

German Certification Body. Eal2 evaluation of fujitsu limited palmsecure SDK version 24 premium. Technical report, German Government, Federal Office for Information Security, 2008. Avilable on-line at http://www.commoncriteriaportal.org/files/epfiles/0511a.pdf. 3, 187

R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Prentice Hall, 2002. 13

V. A. Gronland, H. Hasli, and J. F. Pettersen. Challenging fingerprint scanner. Technical report, NISLAB Authentication Laboratory, Gjovik University College, 2005. 24

P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan. MINEX II, performance of fingerprint match-on-card algorithms, phase II report, NIST 7477. Technical report, Information Access Division, National Institute of Standards and Technology NIST, February 2008. 61, 117

P. J. Grother, R. J. Micheals, and P. J. Phillips. Face recognition vendor test 2002 performance metrics. In *Proc. IAPR Audio- and Video-based Person Authentication (AVBPA)*, pages 937–945. Springer LNCS-2688, 2003. 38

J. K. Guo, D. Doermann, and A. Rosenfeld. Off-line skilled forgery detection using stroke and sub-stroke properties. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 355–358, 2000. 32

K. Guo, D. Doermann, and A. Rosenfeld. Forgery detection by local correspondence. *Journal on Pattern Recognition and Artificial Intelligence*, 15:579–641, 2001. 32

I. Guyon. Handwriting synthesis from handwritten glyphs. In *Proc. IAPR Int. Workshop on Frontiers of Handwriting Recognition (IWFHR)*, pages 309–312, 1996. 34, 182, 209

J. Hennebert, R. Loeffel, A. Humm, and R. Ingold. A new forgery scenario based on regaining dynamics of signature. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 366–375. Springer LNCS-4642, 2007. 9, 21, 22, 24, 189

C. J. Hill. Risk of masquerade arising from the storage of biometrics. Master's thesis, Australian National University, 2001. 2, 9, 24, 26, 106, 186, 189

L. Hong, Y. Wan, and A. K. Jain. Fingerprint image enhancement: algorithm and performance evaluation. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 20(8):777–789, August 1998. 70, 104, 201

IBIA. International biometric industry association, 2009. (http://www.ibia.org/association/). 1, 183

ILO, 2006. ILO SID-0002, "Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents," Int'l Labour Organization. 107

International Biometric Group. Biometrics market and industry report 2009-2014. Technical report, 2009. http://www.biometricgroup.com. 1, 38, 183

ISO/IEC 17025. ISO/IEC 17025:2005, general requirements for the competence of testing and calibration laboratories., 2005. 38

ISO/IEC 19792. ISO/IEC 19792:2009, information technology - security techniques - security evaluation of biometrics., 2009. 2, 9, 41, 187, 189, 195

ISO/IEC 19794-2. ISO/IEC 19794-2:2005, information technology - biometric data interchange formats - part 2: Finger minutiae data., 2005. 107

ISO/IEC 29794-1. ISO/IEC 29794-1:2006 biometric quality framework standard, 2006. 182, 209

ISO/IEC JTC 1/SC 27 . IT security techniques, 2009. http://www.jtc1.org/sc27/. 1, 183

ISO/IEC JTC 1/SC 37 . Biometrics, 2009. http://www.jtc1.org/sc37/. 1, 183

A. K. Jain, R. P. W. Duin, and J. Mao. Statistical pattern recognition: a review. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(1):4–37, 2000. 40, 63

A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008a. 10, 20, 28, 182, 190, 209

A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38:2270–2285, 2005. 138

A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman. Biometrics: A grand challenge. In *in Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, volume 2, pages 935–942, 2004a. 183

A. K. Jain, A. Ross, and P. Flynn, editors. *Handbook of biometrics*. Springer, 2008b. 1, 60, 183

A. K. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. *IEEE Trans. on Information Forensics and Security*, 1(2):125–143, 2006. 1, 2, 3, 5, 13, 19, 182, 183, 191, 209

A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14(1):4–20, 2004b. 37

A. K. Jain and U. Uludag. Hiding biometric data. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 25:1494–1498, 2003. 28

A. K. Jain and D. Zongker. Feature selection: evaluation, application, and small sample performance. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 19:153–158, 1997. 150

J. Jia and L. Cai. Fake finger detection based on time-series fingerprint image analysis. In *Proc. IEEE Int. Conf. on Intelligent Computing (ICIC)*, pages 1140–1150. Springer LNCS-4681, 2007. 32

C. Jin, h. Kim, and s. Elliott. Liveness detection of fingerprint based on band-selective fourier spectrum. In *Proc. Int. Conf. on Information Security and Cryptology (ICISC)*, pages 168–179. Springer LNCS-4817, 2007. 32

M. Kakona. Biometrics: yes or no? Available on-line at http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm, 2001. 24

T. Kanade. *Picture processing system by computer complex and recognition of human faces.* PhD thesis, Kyoto University, 1973. 1, 37, 183

H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim. A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In *Proc. Knowledge-Based Intelligent Information and Engineering Systems (KES)*, pages 1245–1253. Springer LNAI-2774, 2003. 24

A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, 9:5–83, 1883. Available on-line at http://www.petitcolas.net/fabien/kerckhoffs/#english. 7, 10, 188, 190

A. Kholmatov and B. Yanikoglu. An individuality model for online signatures using global Fourier descriptors. In *Proc. SPIE Biometric Technology for Human Identification V (BTHI V)*, volume 6944, 2008. 20, 79

D. H. Klatt. Software for a cascade/parallel formant synthesizer. *Journal Acoustic Society of America*, 67:971–995, 1980. 35

P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Proc. Int. Cryptology Conf. on Advances in Cryptology*, pages 104–113. Springer LNCS-1109, 1995. 27, 181, 208

P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proc. Advances in Cryptology (Crypto 99)*, pages 388–397. Springer LNCS-1666, 1999. 27, 181, 208

P. Komarinski. *Automated Fingerprint Identification Systems (AFIS).* Elsevier, 2005. 4

K. Kryszczuk and A. Drygajlo. Improving classification with class-independent quality measures: Qstack in face verification. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 1124–1133. Springer LNCS-4642, 2007. 182, 209

M. Lane and L. Lordan. Practical techniques for defeating biometric devices. Master's thesis, Dublin City Universtity, 2005. 21

P. Lapsley, J. Lee, D. Pare, and N. Hoffman. Anti-fraud biometric sensor that accurately detects blood flow. US Patent, 1998. 30

S. Lee and S. Li, editors. *Proc. of Second International Conference on Biometrics (ICB)*, 2007. Springer LNCS-4642. 1, 183

M. Lewis and P. Statham. CESG biometric security capabilities programme: method, results and research challenges. In *Proc. Biometrics Consortium Conference (BCC)*, 2004. 22, 24

J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of fourier spectra. In *Proc. SPIE Biometric Technology for Human Identification (BTHI)*, pages 296–303, 2004. 29, 32

E. Lim, X. Jiang, and W. Yau. Fingerprint quality and validity analysis. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, volume 1, pages 469–472, 2002. 68, 69, 200, 201

A. Lin and L. Wang. Style-preserving english handwriting synthesis. *Pattern Recognition*, 40:2097–2109, 2007. xx, xx, 33, 34, 79, 182, 209

LivDet, 2009. http://prag.diee.unica.it/LivDet09/. 1, 32, 41, 66, 72, 90, 183, 196

D. Maio, D. Maltoni, R. Cappelli, J. Wayman, and A. Jain. FVC2002: Second Fingerprint Verification Competition. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 811–814. IEEE Press, 2002a. 112

D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2000: Fingerprint Verification Competition. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 24(3):402–412, 2002b. 40

D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2004: Third Fingerprint Verification Competition. In D. Zhang and A. K. Jain, editors, *Proc. of Int. Conf. on Biometric Authentication (ICBA)*, pages 1–7. Springer LNCS-3072, 2004. 38

D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2003. 22, 29

A. Mansfield, G. Kelly, D. Chandler, and J. Kane. Biometric product testing final report. Technical report, CESG Biometrics Working Group, March 2001. (http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf). 38

A. Mansfield and J. Wayman. Best practices in testing and reporting performance of biometric devices. Technical report, CESG Biometrics Working Group, August 2002. (http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf). 38, 39

G. Marcialis, A. Rattani, and F. Roli. Biometric template update: an experimental investigation on the relationship between update errors and performance degradation in face verification. In *Proc. IAPR Int. Workshop on Structural, Syntactic, and Statistical Pattern Recognition (SSSPR)*, pages 684–693. Springer LNCS-5342, 2008. 61

A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki. The DET curve in assessment of decision task performance. In *Proc. of ESCA Eur. Conf. on Speech Comm. and Tech., EUROSPEECH*, pages 1895–1898, 1997. 40, 185

M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Siguenza. Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, volume 1, pages 151–159, 2006. 64, 94, 132, 204

O. G. Martinsen, S. Clausen, J. B. Nysather, and S. Grimmes. Utilizing characteristic electrical properties of the epidermal skin layers to detect fake fingers in biometric fingerprint systems–a pilot study. *IEEE Trans. on Biomedical Engineering*, 54:891–894, 2007. 32

T. Matsumoto. Artificial irises: importance of vulnerability analysis. In *Proc. Asian Biometrics Workshop (AWB)*, volume 45, 2004. 181, 208

T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proc. SPIE Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677, pages 275–289, 2002. 2, 22, 23, 66, 93, 95, 186

A. Mayoue, B. Dorizzi, L. Allano, G. Chollet, J. Hennebert, D. Petrovska-Delacretaz, and F. Verdet. *Guide to biometric reference systems and performance evaluation*, chapter BioSecure multimodal evaluation campaign 2007 (BMEC 2007), pages 327–372. Springer, 2009. 1, 38, 183

H. Meng, P. C. Ching, T. Lee, M. W. Mak, B. Mak, Y. S.Moon, M.-H. Siu, X. Tang, H. P. S. Hui, A. Lee, W.-K. Lo, and B. M. andE. K. T. Sio. The multi-biometric, multi-device and multilingual (M3) corpus. In *Proc. Workshop on Multimodal User Authentication (MMUA)*, 2006. 47

K. Messer, J. Matas, J. Kittler, J. Luettin, and G. Maitre. XM2VTSDB: The extended M2VTS database. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 72–77. Springer LNCS-2091, 1999. 44, 45, 46, 160

S. Modi, S. J. Elliott, H. Kim, and J. Whetstone. Impact of age groups on fingerprint recognition. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2007. 61

B. Moghaddam and M.-H. Yang. Learning gender with support faces. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 24:707–711, 2002. 61

P. Mohanty, S. sarkar, and R. Kasturi. From scores to face templates: a model-based approach. *Pattern Analysis and Machine Intelligence*, 29:2065–2078, 2007. 25, 157

Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo. Wavelet based fingerprint liveness detection. *Electronic Letters*, 41, 2005. 32

M. Mori, A. Suzuki, A. Shio, and S. Ohtsuka. Generating new samples from handwritten numerals based on point correspondence. In *Proc. IAPR Int. Workshop on Frontiers in Handwriting Recognition (IWFHR)*, pages 281–290, 2000. 34

H. Mouchere, S. Bayoudh, E. Anquetil, and L. Miclet. Synthetic on-line handwriting generation by distortions and analogy. In *Proc. Conference International Graphonomics Society (IGS)*, pages 10–13, 2007. 34

MTIT. Minutiae Template Interoperability Testing, FP6-2004-IST-4, 2009. http://www.mtitproject.com/index.html. 1, 183

R. Mueller and U. Martini. Decision level fusion in standardized fingerprint match-on-card. In *Proc. IEEE Int. Conf. on Control Automation Robotics and Vision (ICARCV)*, pages 185–190, 2006. 117

M. E. Munich and P. Perona. Visual identification by signature tracking. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 25:200–217, 2003. 34, 83, 204

D. Muramatsu. Online signature verification algorithm using hill-climbing method. In *Proc. IEEE Int. Conf. on Embedded and Ubiquitous Computing (ICEUC)*, pages 133–138, 2008. 26

R. Nagel and A. Rosenfeld. Computer detection of freehand forgeries. *IEEE Trans. on Computers*, 26(9):895–905, 1977. 37, 183

A. M. Namboodiri, S. Saini, X. Lu, and A. K. Jain. Skilled forgery detection in on-line signatures: a mutimodal approach. In *Proc. Int. Conf. on Biometric Authentication (ICBA)*, 2004. 28

NBSP. National Biometric Security Project, 2009. http://www.nationalbiometric.org/. 38

W. Nelson and E. Kishon. Use of dynamic features for signature verification. In *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics (ICSMC)*, pages 201–205, 1991. 32

NIST. NIST special publication 800-76, biometric data specification for personal identity verification, 2005. 107

NIST. NIST biometric quality workshop (BWQ), 2006. http://www.itl.nist.gov/iad/894.03/quality/workshop/. 182, 209

K. A. Nixon, V. Animale, and R. K. Rowe. *Handbook of biometrics*, chapter Spoof detection schemes, pages 403–423. Springer, 2008. 19

C. Oliveira, C. A. Kaestner, F. Bortolozzi, and R. Sabourin. Generation of signatures by deformations. In *Proc. IAPR Int. Conf. on Advances in Document Image Analysis (ICADIA)*, pages 283–298. Springer LNCS-1339, 1997. 34

Optel, 2009. http://www.optel.pl/index_en.htm. 32

N. M. Orlans, D. J. Buettner, and J. Marques. A survey of synthetic biometrics: capabilities and benefits. In *Proc. Int. Conf. on Artificial Intelligence (ICAI)*, pages 499–505, 2004. 33

J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez. Authentication gets personal with biometrics. *IEEE Signal Processing Magazine*, 21(2):50–62, 2004. 39

J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. W. R. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran. The multi-scenario multi-environment BioSecure multimodal database (BMDB). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2009. to appear. 16, 43, 44, 46, 194

J. Ortega-Garcia, J. Fierrez, D. Simon, M. F. Gonzalez, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. I. Moro. MCYT baseline corpus: a bimodal biometric database. *IEE Proc. Vision, Image and Signal Processing*, 150(6):391–401, 2003. 45, 57, 85, 119, 134, 138, 204, 205

J. Ortega-Garcia, J. Gonzalez-Rodriguez, and V. Marrero-Aguilar. AHUMADA: A large speech corpus in spanish for speaker characterization and identification. *Speech Communication*, 31:255–264, 2000. 54

A. Pacut and A. Czajka. Aliveness detection for iris biometrics. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, pages 122–129, 2006. 30

B. Paltridge. Thesis and dissertation writing: An examination of published advice and actual practice. *English for Scientific Purposes*, 21:125–143, 2002. 11

G. Pan, Z. Wu, and L. Sun. *Recent advances in face recognition*, chapter Liveness detection for face recognition, pages 109–124. I-Tech, 2008. 29, 32

S. Pankanti, S. Prabhakar, and A. K. Jain. On the individuality of fingerprints. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 24:1010–1025, 2002. 20

D. Petrovska-Delacretaz, A. Mayoue, and B. Dorizzi. *Guide to biometric reference systems and performance evaluation*, chapter The BioSecure benchmarking methodology for biometric performance evaluation, pages 11–25. Springer, 2009. 38

J. Phillips, P. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. In *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition (ICCVPR)*, pages 947–954, 2005. 38, 47, 159

P. Phillips, A. Martin, C. Wilson, and M. Przybocki. An introduction to evaluating biometric systems. *IEEE Computer*, 33(2):56–63, 2000a. 38

P. J. Phillips. Face and iris evaluations at NIST. In *CardTech/SecurTech*, May 2006. 38

P. J. Phillips, H. Moon, P. J. Rauss, and S. Rizvi. The FERET evaluation methodology for face recognition algorithms. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, 2000b. 37, 38

N. B. Pinto, D. G. Childers, and A. L. Lalwani. Formant speech synthesis: improving production quality. *IEEE Trans. on Acoustics, Speech and Signal Processing*, 37:1870–1887, 1989. 35

N. Poh, S. Marcel, and S. Bengio. Improving face authentication using virtual samples. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, 2003. 33, 34

D. V. Popel. *Synthesis and analysis in biometrics*, chapter Signature analysis, verification and synthesis in pervasive environments, pages 31–63. World Scientific, 2007. xx, xx, 33, 35, 132

PosID, 2009. http://www.posid.co.uk/. 32

S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: security and privacy concerns. *IEEE Security and Privacy*, 1:33–42, 2003. 28, 182, 209

F. J. Prokoski and R. B. Biel. *Biometrics: personal identification in networked society*, chapter Infrared identification of faces and body parts, pages 191–212. Kluwer, 1999. 32

M. Przybocki and A. Martin. NIST Speaker Recognition Evaluation chronicles. In J. Ortega-Garcia *et al.*, editors, *ISCA Workshop on Speaker and Language Recognition, ODYSSEY*, pages 15–22, 2004. 1, 38, 183

P. Pudil, J. Novovicova, and J. Kittler. Flotating search methods in feature selection. *Pattern Recognition Letters*, pages 1119–1125, 1994. 149, 150

C. Rabasse, R. M. Guest, and M. C. Fairhurst. A method for the synthesis of dynamic biometric signature data. In *Proc. IAPR Int. Conf. on Document Aanalysis and Recognition (ICDAR)*, 2007. 34, 79

N. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *Proc. IAPR Audio- and Video- Based Person Authentication (AVBPA)*, pages 223–228. Springer LNCS-2091, 2001a. xix, 20, 21, 22, 41, 196

N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007. 28, 130, 205

N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication sytems. *IBM Systems Journal*, 40:614–634, 2001b. 19, 21, 28

N. K. Ratha and V. Govindaraju, editors. *Advances in biometrics: Sensors, algorithms and systems*. Springer, 2008. 1, 183

J. Richiardi. Skilled and synthetic forgeries in signature verification: large-scale experiments. Technical report, Institute of Electrical Engineering, Swiss Federal Institute of Technology, Lausanne, 2008. 34, 79

A. Ross, K. Nandakumar, and A. Jain. *Handbook of Multibiometrics*. Springer, 2006. 1, 43, 128, 183

A. Ross, J. Shah, and A. K. Jain. From template to image: reconstructing fingerprints from minutiae points. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 29:544–560, 2007. 26, 106

V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management (BioID)*, 2008. 16, 66, 195

M. Saavides, B. V. Kumar, and P. K. Khosla. Cancelable biometric filter for face recognition. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, pages 922–925, 2004. 28

R. Sanchez-Reillo, L. Mengihar-Pozo, and C. Sanchez-Avila. Microprocessor smart cards with fingerprint user authentication. *IEEE AESS Systems Magazine*, 18(3):22–24, 2003. 117

B. Schneier. The uses and abuses of biometrics. *Communications of the ACM*, 48:136, 1999. 2, 8, 189

B. Schneier. *Secrets and lies*. Wiley, 2000. 7, 188

S. Schuckers. Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7:56–62, 2002. 10, 21, 190

S. Schuckers and A. Abhyankar. A wavelet based approach to detecting liveness in fingerprint scanners. In *Proc. Biometric Authentication Workshop (BioAW)*, pages 278–386. Springer LNCS-5404, 2004. 30

S. Shah and A. Ross. Generating synthetic irises by feature agglomeration. In *Proc. IEEE Int. Conf. on Image Processing (ICIP)*, pages 317–320, 2006. 35

L. Shen, A. Kot, and W. Koo. Quality measures of fingerprint images. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 266–271. Springer LNCS-2091, 2001. 67, 200

C. Soutar, R. Gilroy, and A. Stoianov. Biometric system performance and security. In *Proc. IEEE Automatic Identification Advanced Technologies (AIAT)*, 1999. 24, 64

S. Steininger, S. Rabold, O. Dioubina, and F. Schiel. Development of user-state conventions for the mulitmodal corpus in smartkom. In *Proc. Int. Conf. on Language Resources and Evaluation (ICLRE)*, pages 33–37, 2002. 47

K. Sumi, C. Liu, and T. Matsuyama. Study on synthetic face database for performance evaluation. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 598–604. Springer LNCS-3832, 2006. 34

B. Tan, A. Lewicke, and S. Schuckers. Novel methods for fingerprint image analysis detect fake fingers. *SPIE Newsroom*, 2008. 30

B. Tan and S. Schuckers. Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. In *Proc. SPIE Biometric Technology for Human Identification III (BTHI III)*, volume 6202, page 62020A, 2006. 28, 30, 130, 205

B. Tan and S. Schuckers. A new approach for liveness detection in fingerprint scanners based on valley noise analysis. *Journal of Electronic Imaging*, 17:011009, 2008. 30

L. Thalheim and J. Krissler. Body check: biometric access protection devices and their programs put to the test. *c´t magazine*, pages 114–121, November 2002. 9, 21, 22, 24, 95, 181, 189, 208

S. Theodoridis and K. Koutroumbas. *Pattern Recognition*. Academic Press, 2006. 13, 40, 63

M. Tistarelli and D. Maltoni, editors. *Proc. of Second IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2007. IEEE Press. 1, 183

T. Toda, H. Kawai, and K. Shikano. Unit selection algorithm for japanese speech synthesis based on both phoneme and diphone unit. In *Proc. IEEE Int. Conf. on Acousticas, Speech and Signal Processing (ICASSP)*, pages 465–468, 2002. 34

M. A. Turk and A. P. Pentland. Face recognition using eigenfaces. In *Proc. IEEE Int. Conf. on Computer Vision and Pattern Recognition (ICCVPR)*, pages 586–591, 1991. 159

P. Tuyls, A.Akkermans, T. A. Kevenaar, G. J. Schrijen, A. M. Bazen, and R. N. Veldhuis. Practical biometric authentication with template protection. In *Proc. IAPR Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 436–446. LNCS Springer-3546, 2005. 28

Ultra-Scan, 2009. http://www.ultra-scan.com/. 32

U. Uludag and A. Jain. Attacks on biometric systems: a case study in fingerprints. In *Proc. SPIE Seganography and Watermarking of Multimedia Contents VI*, volume 5306, pages 622–633, 2004. 25, 41, 64, 93, 117, 137, 196

U. Uludag, A. Ross, and A. K. Jain. Biometric template selection and update: a case study in fingerprints. *Pattern Recognition*, 37:1533–1542, 2003. 61

T. Van der Putte and J. Keuning. Biometrical fingerprint recognition: don't get your fingers burned. In *Proc. Conference on Smart Card Research and Advanced Applications (CARDIS)*, pages 289–303, 2000. 23, 93, 95

T. Varga, D. Kilchhofer, and H. Bunke. Template-based synthetic handwriting generation for the training of recognition systems. In *Proc. Conf. of the International Graphonomics Society (IGS)*, 2005. 34, 182, 209

B. Vijaya-Kumar, S. Prabhakar, and A. Ross, editors. *Proc. of Fifth Conference on Biometric Technology for Human Identification (BTHI V)*, 2008. SPIE. 1, 183

P. Vizcaya and L. Gerhardt. A nonlinear orientation model for global description of fingerprints. *Pattern Recognition*, 29:1221–1231, 1996. 107

H. Wang and L. Zhang. Linear generalization probe samples for face recognition. *Pattern Recognition Letters*, 25:829–840, 2004. 34

J. Wang, C. Wu, Y.-Q. Xu, H.-Y. Shum, and L. Ji. Learning-based cursive handwriting synthesis. In *Proc. IAPR Int. Workshop on Frontiers of Handwriting Recognition (IWFHR)*, pages 157–162, 2002. 34

J. Wayman, A. Jain, D. Maltoni, and D. Maio. *Biometric systems. Technology, design and performance evaluation.* Springer, 2005. 41, 43, 195

A. Wehde and J. N. Beffel. Finger-prints can be forged. *Tremonia Publish Co.*, 1924. 22, 23

Z. Wei, X. Qiu, Z. Sun, and T. Tan. Counterfeit iris detection based on texture analysis. In *Proc. IEEE Int. Conf. on Pattern Recognition (ICPR)*, 2008. 30

A. Wiehe, T. Sondrol, O. K. Olsen, and F. Skarderud. Attacking fingerprint sensors. Technical report, NISLAB Authentication Laboratory, Gjovik University College, 2004. xix, 23, 24

D. Willis and M. Lee. Biometrics under our thumb. *Network Computing*, 1998. Available on line at http://www.networkcomputing.com/. 23

C. Wilson, R. A. Hicklin, M. Bone, H. Korves, P. Grother, B. Ulery, R. Micheals, M. Zoepfl, S. Otto, and C. Watson. FpVTE2003: Fingerprint Vendor Technology Evaluation 2003, June 2004a. NIST Research Report NISTIR 7123 (http://fpvte.nist.gov/). 38

C. Wilson, R. A. Hicklin, H. Korves, B. Uler, M. Zoepfl, M. Bone, P. Grother, R. Micheals, S. Otto, and C. Watson. Fingerprint vendor technology evaluation 2003: summary of results and analysis report, nistir 7123. Technical report, National Institute of Standards and Technology, 2004b. 117

H. R. Wilson, G. Loffler, and F. Wilkinson. Synthetic faces, face cubes, and the geometry of face space. *Vision Research*, 42:2909–2923, 2002. 34

Y. Yamazaki, A. Nakashima, K. Tasaka, and N. Komatsu. A study on vulnerability in on-line writer verification system. In *Proc. IAPR Int. Conf. on Document Analysis and Recognition (ICDAR)*, volume 2, pages 640–644, 2005. 26

W. S. Yambor, B. A. Draper, and J. R. Beveridge. Analyzing PCA-based face recognition algorithms: eigenvector selection and distance measures. In *Proc. Workshop on Empirical Evaluation Methods in Computer Vision (WEEMCV)*, 2000. 159

S. N. Yanushkevich, P. S. P. Wang, M. L. Gavrilova, and S. N. Srihari, editors. *Image pattern recognition. Synthesis and analysis in biometrics.* World Scientific, 2007. 33

D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll. SVC2004: First International Signature Verification Competition. In D. Zhang and A. K. Jain, editors, *Proc. IAPR Int. Conf. on Biometric Authentication (ICBA)*, pages 16–22. Springer LNCS-3072, 2004. 1, 26, 38, 54, 133, 183

M. M. Yeung and S. Pankanti. Verification watermarks on fingerprint recognition and retrieval. *Journal of Electronic Imaging*, 9:468–476, 2000. 28

Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi. Fake finger detection based on thin-plate spline distortion model. In *Proc. IAPR Int. Conf. on Biometrics*, pages 742–749. Springer LNCS-4642, 2007. 31

J. Zuo, N. A. Schmid, and X. Chen. On generation and analysis of synthetic iris images. *IEEE Trans. on Information Forensics and Security*, 2:77–90, 2007. 33, 35, 79, 132