UNIVERSITÀ DEGLI STUDI ROMA TRE
DIPARTIMENTO DI INGEGNERIA
DOTTORATO DI RICERCA IN ELETTRONICA APPLICATA

ROMA TRE UNIVERSITY
ENGINEERING DEPARTMENT
DOCTORAL PROGRAMME IN APPLIED ELECTRONICS

ANONYMOUS BIOMETRICS

Doctoral Dissertation of:
Gabriel Emile Hine

Supervisor:
Prof. Patrizio Campisi

XXXI Cycle

February 2019

Abstract

In this thesis, we developed techniques that enable to use biometric traits for authentication in an anonymous manner. At first glance, the concept of anonymous biometrics seems quite odd since biometric traits are closely linked to our identity. Moreover, the widespread adoption of biometrics in forensics, border control, surveillance applications has biased the general vision that users have if asked to show their biometrics. The basic idea behind anonymous biometrics is to do not use biometrics themselves as identifiers, but rather bind the biometric trait with a secret key that acts as the authenticator. The biometric trait becomes a factor of the authentication protocol that let the user reproduce the identifier that has been previously assigned to him. In this way, the authentication service provider does not need to know the biometric sample itself, or any representation of it. Because of the intrinsic noisiness of biometrics, classical cryptographic techniques are not suitable, and specific techniques, known as biometric cryptosystems, have been developed.

In this context, we present a novel biometric cryptosystem obtaining perfect security, that is not leaking any information about the employed secret key from the knowledge of the data stored in the database. While similar methods have already been sought in the literature, the approaches proposed so far have been evaluated in terms of recognition performance under the unrealistic assumption of ideal statistical distributions for the considered biometric data. Conversely, in this thesis, we investigate the appli-

cability of the proposed framework to practical scenarios while managing a trade-off between privacy and recognition performance. This goal has been achieved by introducing a class of transformation functions enforcing zero-leakage secrecy, by designing an adaptive strategy for embedding the secret key bits into the selected features, and by developing a system parameters optimization strategy with respect to security, recognition performance, and privacy. Experimental tests conducted on real fingerprint data prove the effectiveness of the proposed scheme.

Another important aspect is to ensure the untraceability along different services. That means that we should be able to produce different identifiers starting from the same biometric trait, but these should be indistinguishable from identifiers originated by independent users. The vulnerability of our system to the linkability attack has been analysed and an enhanced system is proposed in order to counteract it.

A frequently neglected aspect in cryptosystem design proposals and analysis is the impossibility to synchronise signals once they are encrypted. Any kind of biometric should be aligned before doing any comparison. That means that further auxiliary data must be stored as a reference. This could leak too much information making the cryptosystem design useless. In this context, we propose a novel translation-invariant representation for fingerprint minutiae.

Author's contributions

Journals

J.1 **Hine GE**, Maiorana E and Campisi P (2017),
"A Zero-Leakage Fuzzy Embedder From the Theoretical Formulation to Real Data",
in IEEE Transactions on Information Forensics and Security, July, 2017. Vol. 12(7), pp. 1724-1734.

J.2 Maiorana E, **Hine GE** and Campisi P (2015),
"Hill-Climbing Attacks on Multibiometrics Recognition Systems",
IEEE Transactions on Information Forensics and Security, Vol. 10, pp. 900-915.

J.3 Iula A, **Hine GE**, Ramalli A and Guidi F (2014),
"An Improved Ultrasound System for Biometric Recognition Based on Hand Geometry and Palmprint",
in Procedia Engineering. Vol. 87, pp. 1338-1341. Elsevier.

Conferences

C.1 **Hine GE**, Maiorana E and Campisi P (2018),
"Fingerprint Minutiae Matching Through Sparse Cross-correlation",
in the 26th European Signal Processing Conference (EUSIPCO).

C.2 **Hine GE**, Maiorana E and Campisi P (2017),
"Resting-state EEG: A Study on its non-Stationarity for Biometric Applications",
in 2017 International Conference of the Biometrics Special Interest Group (BIOSIG).

C.3 Ramalli A, Dallai A, Bassi L, Scaringella M, Boni E, **Hine GE**, Matrone G, Savoia AS and Tortoli P (2017),
"High Dynamic Range Ultrasound Imaging With Real-Time Filtered-Delay Multiply and Sum Beamforming",
in 2017 IEEE International Ultrasonics Symposium (IUS).

C.4 **Hine GE**, Onaolapo J, Cristofaro ED, Kourtellis N, Leontiadis I, Samaras R, Stringhini G and Blackburn J (2017),
"Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web",
in the 11TH International AAAI Conference on Web and Social Media (ICWSM-17).
Best Paper Runner-Up (awarded to 3 of 50 papers)
Media Coverage: Nature, Motherboard, The Independent, The Conversation, MIT Technology Review, Vice, La Stampa , La Repubblica, BoingBoing, Pacific Standard

C.5 Iula A, **Hine GE**, Ramalli A and Guidi F (2014),
"Wide 3D ultrasound palmprint for biometric recognition",
in 2014 IEEE International Ultrasonics Symposium (IUS), pp. 1388-1391.

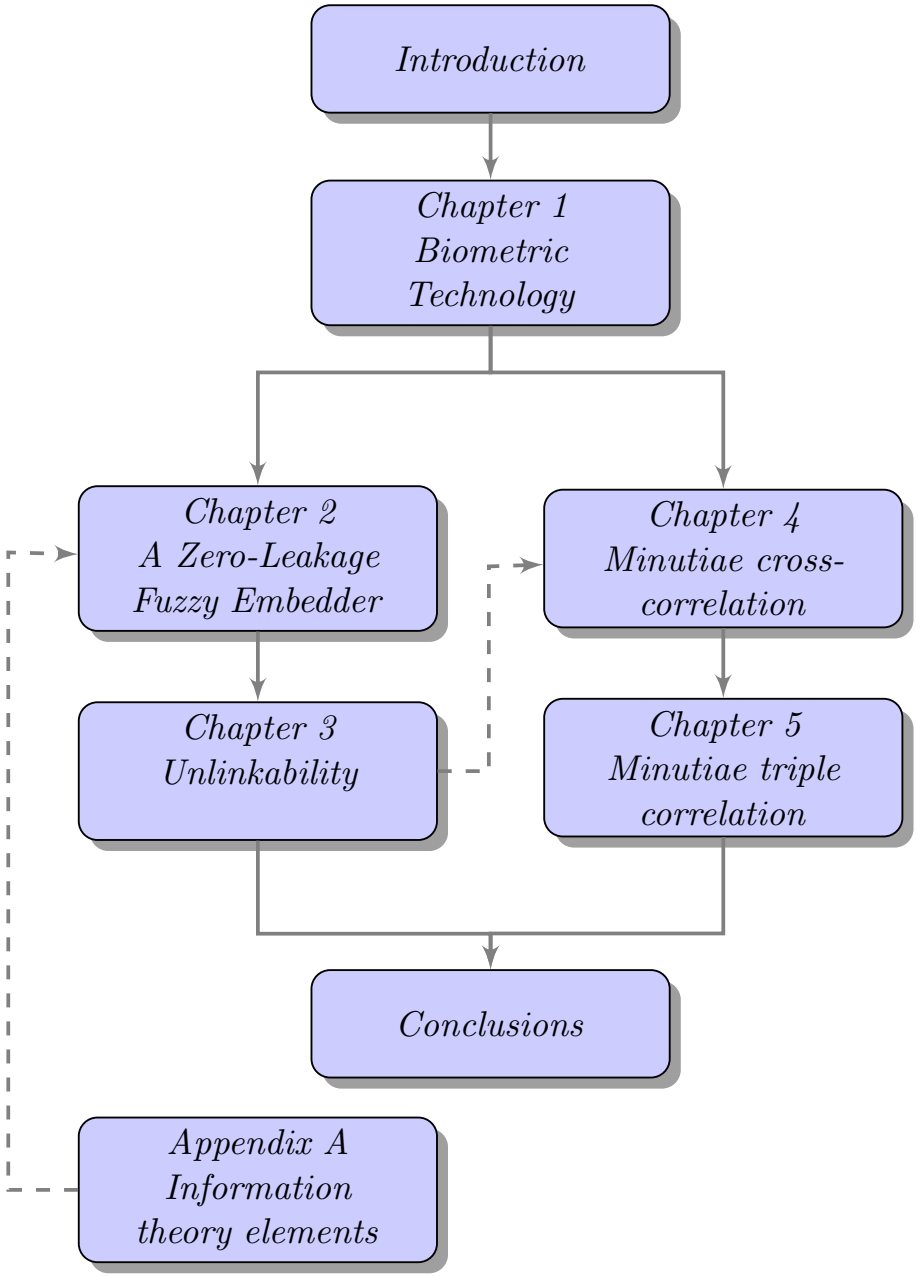
C.6 Iula A, **Hine GE**, Ramalli A, Guidi F, Boni E, Savoia AS, and Caliano G (2013),
"An enhanced Ultrasound technique for 3D Palmprint Recognition",
in 2013 IEEE International Ultrasonics Symposium (IUS), pp. 978-981.

C.7 Maiorana E,**Hine GE** and Campisi P (2013),
"Hill-climbing attack: Parametric optimization and possible countermeasures. An application to on-line signature recognition",
in Proceedings of the International Conference on Biometrics (ICB), 2013.

C.8 Maiorana E, **Hine GE** and Campisi P (2013),
"On the vulnerability of an EEG-based biometric system to hill-climbing attacks",
in Proceedings of the IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013.

Book Chapters

Iula A, **Hine GE**, Ramalli A, Guidi F and Boni E (2016),
"2D and 3D Palmprint Extraction by an Automated Ultrasound System",
in Applications in Electronics Pervading Industry, Environment and Society, pp. 83-89. Springer International Publishing.



The flow-chart shows the dependencies between chapters. Thick lines indicate strict dependencies; dashed lines indicate weak dependencies, i.e., the reader should read appendix A only if does not have a sufficient information theory background. Chapters 4 and 5 may be read independently from Chapters 2 and 3.

Contents

Introduction

Biometric template protection has recently triggered the attention of both the research and the industrial communities, due to the widespread social perception of the potential damages which could derive from the loss of secrecy and control over biometric traits [Nandakumar and Jain, 2015].

As well known, the use of biometric data raises many security issues which are peculiar of biometrics-based recognition systems, not affecting other approaches employed for automatic people authentication. In fact, some biometrics such as voice, face, fingerprints and many others are exposed traits, they are not secret and therefore they can be covertly acquired or stolen by an attacker and misused. This can lead for example to identity theft. Moreover, raw biometrics cannot be revoked, cancelled, or reissued if compromised, since they are user's intrinsic characteristics and they are in limited number. Therefore, if a biometric is compromised, all the applications making use of that biometrics are compromised, and, since biometric identifiers are permanent, an issue is raised when it is needed to change them. The use of biometrics poses also many privacy concerns. In fact, when an individual gives out his biometrics, either willingly or unwillingly, he discloses unique information about himself. It has also been demonstrated that biometric data can contain relevant information regarding people health. This information can be used, for instance, to discriminate people for hiring or to deny insurance to those with latent health problems. The use of biometrics can also raise cultural-, religious- as well as

ethnicity-related concerns. To some extent, the loss of anonymity can be directly perceived by users as a loss of autonomy.

Several schemes have been proposed in recent years with the aim of protecting the templates stored in biometric databases, guaranteeing the properties of renewability, security and performance [Tuyls et al., 2004], [Campisi, 2013]. Such approaches have been typically categorized into two major classes: cancelable biometrics and biometric cryptosystems [Rathgeb and Uhl, 2011].

The former kind of approach is based on the adoption of non-invertible transformation functions, whose defining parameters may be made publicly available or not [Patel et al., 2015]. Typically, in these cases the robustness analysis, that is the possibility of reverting the employed transformations, are not dealt with many details, due to both the difficulty in quantitatively evaluating the actual non-invertibility, and to the heterogeneity of the proposed approaches, which makes arduous to define general metrics upon which evaluating the provided security.

Conversely, biometric cryptosystems [Uludag et al., 2004a], where cryptographic protocols encounter biometrics, have been the object of extensive study, and metrics for assessing security, and privacy have been proposed in the literature. Specifically, several peculiar attacks against such template protection approaches have been described in [Simoens et al., 2009] and [Stoianov, 2009]. Among them, one of the most threatening consists of the non-randomness attack, where the knowledge about the global statistics of the employed biometric data is exploited to obtain information about the secrets protected by the system. In more details, different information theoretic studies have deeply analysed key-binding approaches, based on the combination of biometric information with secret cryptographic keys, trying to evaluate which amount of information is leaked by the resulting helper data regarding the original secret sources.

A fundamental trade-off between reliability, privacy, intended as the hardness of retrieving the original biometric information from the stored helper data, and security, measured by the uncertainty about the adopted cryptographic key, has been given in [Ignatenko and Willems, 2009] and [Lai et al., 2015]. Further insights about the trade-off existing among security, privacy, and achievable recognition rates have been also discussed in [Ignatenko and Willems, 2015], where it has been demonstrated that a

system can obtain better recognition performance at the expenses of an increased leakage about the employed secret key and the adopted biometric data. The aforementioned theoretical investigations have also proven that, although privacy leakage is unavoidable, perfect security may be possible from an information-theoretical point of view. Nonetheless, this can be achieved only assuming some unrealistic requirements for practical biometric representations, such as the use of uncorrelated features with uniform distributions, as in [Tuyls et al., 2005] for fingerprint data.

The few attempts that have tried to empirically evaluate the protection provided by key-binding approaches applied to real biometric data, such as signature in [Maiorana et al., 2012], face in [Sutcu et al., 2007] and [Zhou et al., 2011], iris in [Zhou and Busch, 2012] and [Maiorana et al., 2014], and electroencephalography in [Maiorana et al., 2015b], have shown that a very significant reduction of security and a notable increase of privacy leakage occur when biometric features with a non-ideal distribution are taken into account in practical scenarios.

Indeed, as further discussed in Section 2.1, in [Buhan et al., 2008a], [de Groot and Linnartz, 2011] and [de Groot et al., 2016] some procedures to map biometrics data distributions into ideal ones have been proposed. Nonetheless, also in the aforementioned scenarios, the analysis has been carried out employing only synthetic data modeled as independent features, thus preventing to draw general conclusions when dealing with real-world biometrics. To the best of our knowledge, a template protection scheme able to provide perfect security against non-randomness attacks and proved to be applicable to practical scenarios is still missing in literature.

Within this scenario, the goal of this thesis is the proposition of a novel approach which allows the construction of a zero-leakage template protection system, applicable to real-world biometric data, still able to guarantee satisfactory privacy and recognition performance. As detailed in Section 2.2.3, the proposed framework is also designed in order to endure attacks based on the exploitation of false acceptance rate (FAR) [Korte and Plaga, 2007], [Bringer et al., 2006], where a malicious user tries to get access to the system, by performing several recognition trails authentication.

Another very poorly covered and unsolved issue in the field of biometric protection is the linkability. Linkability refers to the ability to link together identifiers obtained from the same user In this context, both theo-

retical analysis and practical methods are missing. The theoretical analysis present in literature we mentioned before and the concept of zero-leakage are valid only in the scenario of a single identifier instance per user. Indeed, many works proved that most of the biometric cryptosystems have privacy weaknesses in the case of multiple instances [Buhan et al., 2010a, Simoens et al., 2009, Boyen, 2004]. Some general purpose attempt to avoid the issue have been proposed, such as in [Blanton and Aliasgari, 2011], where the authors proposed that the user should store one short secret string for all possible uses of his/her biometric. The problem is that, in many contexts, the use of secondary factors for authentication may let biometrics pointless. Other methods based public information have been proposed but they are system specific. For example, in [Kelkboom et al., 2011] the authors proposed a key-less method to avoid cross-matching in a fuzzy commitment scheme. Similarly, we propose an analogous method suited for our zero-leakage cryptosystem.
In order to apply the techniques introduced so far to real biometric data, some preprocessing steps are needed. Specifically, a crucial step consists in aligning the enrolled and the verification biometric probes [Nandakumar et al., 2007]. Since the enrolled reference is encrypted, the synchronization becomes an issue. In this context, further auxiliary data are usually considered, leading to further potential leakage that the designer has to manage. For this reason, in this framework, translation-invariant representations are appealing. Therefore, we propose a novel fingerprint minutiae representation that is invariant to rigid translation. The interesting characteristic of the proposed representation is that it is loss-less, in the sense that no information of the signal is lost, except for the absolute position in space.

The thesis is organized as follows. In Chapter 1, biometric technology is introduced, where particular emphasis is given to privacy and security issues. In Chapter 2, the proposed biometric zero-leakage cryptosystem is presented and deeply analysed. Lastly, in Chapter 3, an enhancement of the system is suggested in order to overcome the weakness to linkability attack. In Chapter 4, a novel minutiae matching algorithm is presented, thus posing the bases for Chapter 5 where we propose a translation-invariant minutiae representation. In Appendix A, some basic elements of information theory are given.

Some Key Terms Definitions

In this Section, some key terms are defined. The definitions are taken from the [ISO/IEC 2382-37, 2017] − Information technology − Vocabulary − Part 37: Biometrics and [ISO/IEC 30136, 2018] − Information technology − Performance testing of biometric template protection schemes.

- *biometric recognition (biometrics)*: automated recognition of individuals based on their biological and behavioural characteristics;
- *biometric system*: system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics;
- *biometric feature*: numbers or labels extracted from biometric samples and used for comparison;
- *biometric template*: set of stored biometric features comparable directly to probe biometric features;
- *biometric reference*: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison;
- *biometric probe*: biometric query biometric sample or biometric feature set input to an algorithm for biometricc omparison to a biometric reference(s);
- *biometric enrolment*: act of creating and storing a biometric enrolment data record in accordance with an enrolment policy;
- *biometric identification*: process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual;
- *biometric verification*: process of confirming a biometric claim through biometric comparison;
- *false match*: comparison decision of match for a biometric probe and a biometric reference that are from different biometric capture subjects;
- *false match rate (FMR)*: proportion of the completed biometric nonmated comparison trials that result in a false match;

- *false non-match*: comparison decision of "non-match" for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic;
- *false non-match rate (FNMR)*: proportion of the completed biometric mated comparisontrials that result in a falsenon-match;
- *mated (adjective)*: of or having to do with a paired biometric probe and biometric reference that are from the same biometric characteristic of the same biometric data subject;
- *non-mated (adjective)*: of or having to do with a paired biometric probe and biometric reference that are not from the same biometric characteristic of the same biometric data subject;
- *biometric information privacy*: right to control the collection, transfer, use, storage, archiving, disposal and renewal of one's own biometric information throughout its lifecycle;
- *biometric sample*: analog or digital representation of biometric characteristics obtained from a biometric capture device or biometric capture subsystem prior to biometric feature extraction;
- *identifier*: one or more attributes that uniquely characterize an entity in a specific domain;
- *authentication*: the act of proving or showing to be of undisputed origin or veracity identity is genuine;
- *accuracy degradation*: difference in FNMR/FMR for a biometric system tested both with and without template protection schemes;
- *adversary*: one who compromises an enrolment database and may gain access to the generative biometric data of the individuals enrolled therein;
- *biometric template protection*: protection of biometric references under various requirements for secrecy, irreversibility, and renewability during storage and transfer

- *irreversibility*: property of a transform that creates a biometric reference from generative biometric data such that knowledge of the transformed biometric reference cannot be used to determine any information about the generative biometric data;

- *auxiliary data*: subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general;

- *pseudonymous identifier (PI)*: part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any);

- *renewability*: property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference;

- *revocability*: ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference;

- *irreversibility*: property of a transform that creates a biometric reference from generative biometric data such that knowledge of the transformed biometric reference cannot be used to determine any information about the generative biometric data;

- *privacy compromise*: event in which an adversary discovers part of the generative biometric data of an individual enrolled in the database of a biometric verification or identification system;

- *privacy leakage*: <template protection scheme> amount of information about an individual's generative biometric data which an adversary can learn from the stored reference data;

- *unlinkability*: property of two or more biometric references that they cannot be linked to each other or to the subject(s) from which they were derived;

- *successful attack rate*: probability that an informed adversary can obtain a false accept result in a biometric system;

CHAPTER 1

Biometric Technology

Biometric technology has the aim of identifying or verifying a user identity based on his or her physiological characteristics (such as fingerprints or irises) or behavioural characteristics (such as the signature or keystroke). The technology was born with the purpose of supporting forensic investigations. Subsequently, it had his main application in border control. The majority of modern passports store biometric information, such as fingerprints and, obviously, face images. Although it has been a long time since biometric devices have been commercialized without great success, nowadays biometrics is gaining a popularity thanks to its adoption in many mainstream mobile devices (like smart-phones tablets) and personal computers. Besides unlocking a personal device, that is the main commercial application nowadays, many companies are pushing to use biometrics for on-line authentication, such as e-banking services. Although such a scenario is very appealing, biometric data are too sensitive to distribute them to whatever service provider in the web. It is in this context that the biometric protection technologies may have their main application.

1.1 Biometric as Authentication Factor

Biometric traits, such as fingerprints, are permanent and unique identifiers. That's why they should be considered private and sensitive data. On the other hand, some biometric traits are semi-public. Our faces can be captured at any moment and our fingerprints can be retrieved from everything we touch. This duality makes inappropriate the use of biometrics in authentication systems with centralized storage. With the spread of the use of biometrics in our society, the privacy and security threads grow further. These threads include:

- lost of the control regarding our personal data;
- cross-database correlations;
- user profiling and discrimination;
- biometric information theft and subsequent frauds.

Biometric cryptosystems have the aim to solve upstream the majority of the aforementioned threads since they require that the biometric signal is never shared, transmitted, or memorized. In this way biometric cryptosystems let embody some of the most fundamental good practice privacy policies:

- data minimization: no biometric data is stored, minimizing the risk of misuse;
- user control maximization: the user can narrow the use of his data to what they are meant to, thus preventing the so-called function-creep.

The main idea of biometric cryptosystems is to extract from the biometric signal reproducible and noiseless strings that can be used as cryptographic keys or identifiers in an authentication system. Ideally, one should be able to extract an unlimited number of uncorrelated single-purpose identifiers from the same biometric, in order to use each of them in a different application. If any of these identifiers is compromised, this should be easily revoked and substituted as, in the same way, we would do with a password. Obviously, such a scenario is not possible with conventional biometric systems that make use of biometric templates direct match.

1.2 Conventional Biometric System

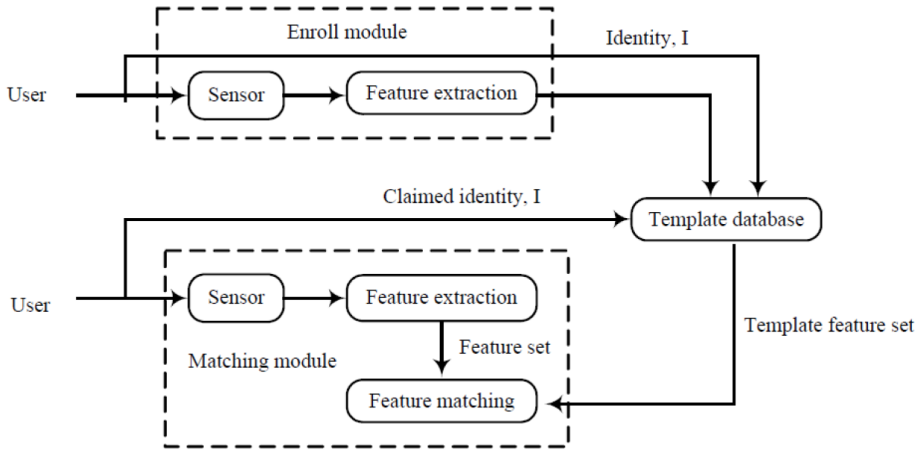


Figure 1.1: *Conventional Biometric System*

In figure 1.1 a conventional biometric system is shown. In its basic configuration, this is made up of:

- a sensor that acquires the biometric trait of the user;
- a feature extractor that extracts useful information for recognition from the raw data, building the so-called template;
- a database where the template is stored during the enrolment stage;
- a matching algorithm that compares the fresh template extracted during verification with the stored one and decides whether they both belong to the same user or not.

Since the biometric signal is noisy by nature, the comparison between template is done by means of some sort of distance. A binary decision is then taken comparing the score with a predefined threshold. It is clear that the problem with this scheme is that the matching algorithm must be able to access the plain-text version of the templates.

1.3 Secure Biometric Systems

Although the industry and scientific communities had been arguing for many years that the knowledge of the biometric template does not leak

information about the original biometric signal, such belief turned out to be wrong. In fact, many reverse engineering techniques, such as hill climbing algorithms, have been proposed. This means that if the biometric template is compromised, many privacy threats arise. Since the biometric trait is intimately linked to its owner, its theft would be irretrievable. Standard cryptographic techniques alone do not solve the problem. The major difficulty is due to the intrinsic noise that characterises biometric data. On the other hand, cryptographic primitives work only with noiseless data. Indeed, one of the most fundamental requirements of any cryptographic primitive is that any minimal variation of the input data should cause an upheaval of the output. In other words, no similarity notion should be preserved after the transformation.

1.4 Template Protection Techniques

Although many different paradigms for template protection exist, they are all subject to the following requirements:

- *Irreversibility*: it should be computationally difficult to retrieve the original template from the data stored in the database (i.e. the protected template, helper data), while it should be easy to generate them from the input template.
- *Renewability*: it should be possible to generate many identifiers from the same biometric in order to use each of them for different applications, and, if necessary, replace them if compromised.
- *Unlinkability*: given a couple of identifiers, it should be computationally difficult to establish whether or not they were generated from the same biometrics. This property is also referred as *indistinguishability.*
- *Recognition performance*: the protection system should not affect too much the recognition performance in terms of False Match Rate and False Non-Match Rate. Unfortunately, it turns out that there is a clear trade-off between security/privacy properties and recognition performance.

The template protection techniques are commonly classified as:

- cancellable templates;

- biometric cryptosystem;
- Secure multiparty computation-based.

Cancellable template systems are based on some kind of transformation of the biometric template, and the matching is done in the transformed domain. The transformation should be such that it should be computationally difficult to invert. The transformation parameters are typically dependent on a key or password that should, therefore, be used during both enrolment and authentication.

Biometric crypto-systems are systems that mate the biometric trait with a key. The key can be extracted directly from the signal or can be chosen independently. We refer to the two cases respectively as fuzzy extractors and fuzzy embedders. In both cases, usually, during the enrolment, additional information are stored, commonly known as helper data. These data are used to support the verification stage and help the system to generate the same key embedded/extracted during enrolment. The helper data are usually considered public information, so they should not reveal any information about the original biometric or the associated key. The biometric recognition is done indirectly by comparing the key extracted during authentication and the stored one. The use of a fixed string as authenticator allows integrating easily many cryptography protocols that are normally used with password- or pin-based authentication systems. As a simple example, it is straightforward to implement a hash-based protocol.

Secure multiparty computation-based biometric systems exploit homomorphic encryption to compute the distance (or similarity) between biometric samples in the encrypted domain. The basic idea is that the server can store and process only the encrypted version of biometric data. Thanks to homomorphic encryption techniques, the server can compute the encrypted version of some specific operators applied to original data. For example, Paillier cryptosystem [Paillier, 1999] is additively homomorphic since $E(a)\,E(b) = E(a+b)$. The plain-text version of the result of the operator can be obtained only with a private key that is usually owned by the user. Thus, multiparty computation-based biometric systems are intrinsically double-factor systems.
In this thesis, we focus on techniques only on single factor techniques since our vision is that biometrics should completely substitute pins, tokens etc. At most, if secondary factors are used, these should be considered as sup-

plementary levels of security. The biometric system should be constructed in order to be intrinsically secure, independently to other authentication factors. For this reason, the system should be analysed by means of strong theoretical reasoning.
In next section, the most relevant works in the field of biometric cryptosystems are reported.

Biometric Cryptosystems

The most influential contributions in the field of security with noisy data are probably due to Ari Juels who introduced the most famous error tolerant cryptographic primitives: *fuzzy commitment* [Juels and Wattenberg, 1999] and *fuzzy vault* [Juels and Sudan, 2006]. Fuzzy commitment is the first method that combines cryptographic techniques with error correction codes (ECC).

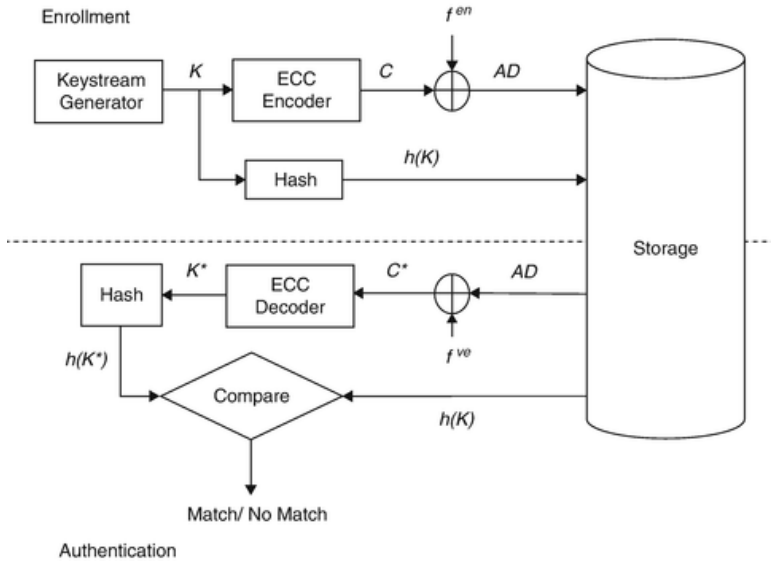


Figure 1.2: *The fuzzy-commitment scheme*

As we can see in figure 1.2, the scheme is very simple. During enrolment, a secret message K is encoded with ECC and codeword C is XORed with the so-called witness f^{en}, producing the auxiliary data, also known as helper data:

$$AD = C \oplus f^{en}. \tag{1.1}$$

The witneses is usually the quantized version of a noisy reference signal, for example a biometric trait. That means that, during the verification stage, the witness may contain some errors, i.e. $f^{ve} = f^{en} \oplus e$. By XORing it with the helper data AD, the error pattern e is transferred on the codeword:

$$f^{ve} \oplus AD = (C \oplus f^{en}) \oplus (f^{en} \oplus e) = C \oplus e = C'. \tag{1.2}$$

If the number of errors is below a certain threshold, the ECC decoder is able to retrieve the secret message K. Basically, fuzzy commitment is XOR-based encryption scheme in which the decryption key (the witness) may slightly differ from the encryption one. The interesting fact of the scheme is that it allows protecting biometrics with conventional cryptographic techniques, like hash functions, that are commonly used to protect alphanumeric passwords. The fuzzy commitment scheme has been tested and analysed deeply in the literature. In [Zhou et al., 2011] the privacy and security of the scheme are analysed. A deeper analysis of the leakage of information with different kinds of biometric source can be found in [Ignatenko and Willems, 2010]. In [Simoens et al., 2009], the authors demonstrated the non-re-usability of the scheme. In fact, two sketches obtained with the same witness can be easily linked together. The weakness is due to the linearity of error correcting codes. In [Kelkboom et al., 2011], the author proposed to use a record specific perturbation matrix to avoid the linkability, but in [Tams, 2014], the author demonstrated the ineffectiveness of the method.

Many systems have been inspired by the fuzzy commitment idea. They are known with different names in the literature such as fuzzy embedders [Buhan et al., 2008b] or fuzzy sketch [Sutcu et al., 2007] but the concept is the same. The architecture is the same of the fuzzy commitment in figure 1.2 where, instead of the XOR module, a generic key binding technique is placed. For example, a well known key binding technique is the Quantization Index Modulation(QIM) -based cryptosystem [Bui et al., 2010], where the helper data coincide with the quantization error of key controlled quantizer. Actually, as we will see in Section 2.1.1, the QIM scheme can be seen as a modular shift-based embedder, making it an extension of the fuzzy commitment scheme.

Fuzzy vault primitive [Juels and Wattenberg, 1999] is very similar to fuzzy commitment with the difference that the secret message is bind to a set of unordered elements. During verification, the secret is extracted only if a set

sufficiently overlapping with the original witness is provided. The order invariance and the not fixed length characteristics make the method perfectly suitable for minutiae-based biometric verification systems [Nandakumar et al., 2007]. Unfortunately, also this scheme suffers the linkability of multiple instances because of the correlation attack [Kholmatov and Yanikoglu, 2008], therefore some improvements have been proposed [Tams, 2016].
Besides the various techniques proposed in the literature, a big effort has been done to define the intrinsic theoretical limits of biometric cryptosystems in terms of security, privacy, and reliability. Theoretical investigations of the trade-off existing among security, privacy, and achievable recognition rates can be found in [Ignatenko and Willems, 2009], [Lai et al., 2015], and [Ignatenko and Willems, 2015]. Although the importance of these works is undoubted, the assumptions that they make are generally unrealistic. In fact, in order to carry out generic and universal conclusions in an elegant mathematical manner, the biometric signals are described through very simple models. A typical model is the independent and identically distributed (IID) source with additive Gaussian noise. The problem with these models is that they are not data-driven, but they are chosen just for the sake of simplicity. Simplicity is crucial to build models, but as we will see in chapters 2 and 3, entrusting on these models may cause wrong conclusions, and most importantly bad design choices.

1.4.1 The Alignment Requirement

A crucial requirement of any cryptosystem we have introduced so far is the alignment issue. Let us consider the fuzzy commitment scheme. Features vectors are binarised and XOR operations are applied. The system would never work with features that are translation-dependent. Most of the template protection techniques that have been proposed in literature assume that the data are pre-aligned which is rarely the case in practice [Rathgeb and Uhl, 2011]. In fact, features alignment is a fundamental processing step in any biometric system. That means that some reference data should be stored in the system in order to register the sample. The additional data have to be considered as integral part of the Auxiliary Data (or Helper Data), meaning that it should not leak relevant information about the original biometrics. Such requirements are highly non-trivial.

A biometric trait that heavily suffers the alignment requirement is fin-

gerprint. In this context, [Nandakumar et al., 2007] suggest to utilize high curvature points derived from the orientation field of a fingerprint as helper data to assist the process of alignment, although, the alignment performances are not as having the entire reference. In order to overcome the alignment difficulties, translation- and rotation-invariant representations of minutiae have been proposed [Jeffers and Arakala, 2006].

1.5 Standardization of Biometric Template Protection

Besides the technical difficulties that we have described so far, one of the major obstacles to the deployment of privacy protection techniques is the lack of interoperability among biometric modules, such as sensors, feature extractors, storage formats [Rane, 2014]. As well as the standardization of the protocols between modules, common criteria to evaluate and report performances are needed. This aspect is particularly hard because of the many different approaches that have been proposed in the literature. The first step is to define "implementation-agnostic" vocabulary for security and privacy aspects in the context of biometric protection systems. Once these concepts are well defined, metrics to evaluate privacy and security must be defined. Although it would be great to have only architecture-independent metrics, some of them may be defined specifically for a considered scheme.
One of the first notable attempts to give standard guidelines and requirements on secure and privacy-compliant administration and processing of biometric data is provided in ISO/IEC 24745 standard on Biometric Information Protection [JTC1 SC27 IT Security Techniques ISO/IEC 24745, 2011]. First of all, the standard specifies that, during enrolment stage, two kind of information are stored in the biometric database:

- Auxiliary Data (AD),
- Pseudonymous Identifier (PI),

that together constitute the template. To make an example, in the fuzzy commitment scheme we discussed before, the Pseudonymous Identifier is the hash version of the secret key, while the Auxiliary Data is the XOR between the key and witness extracted from the biometric trait. In general, auxiliary data, also known as helper data, include all those information that are needed to reconstruct the pseudonymous identifier ones the verification

biometric sample is provided. These may also include references point for the signal alignment. On the other hand, the pseudonymous identifier is the part of a biometric reference that uniquely represents an individual and can be verified by means of a captured biometric sample and the auxiliary data. In many cases, the identifier is completely interdependent from the biometric sample, and, alone, it cannot (or at least should not) provide any information about the enrolled biometric sample. The choice of the information to store and process in the authentication server is crucial to preserve security and privacy. Although these terms are commonly confused each other, they refer to different concepts. Privacy refers to the difficulty of retrieving the biometrics of enrolled users or any other personal information that may be somehow encoded in the biometric trait, such as gender, skin colour, etc. Security refers to the hardness of obtaining access to the service or the data that are protected through the biometric trait, e.g. discovering the pseudonymous identifier. Actually, sometimes the two concepts are linked together since, for example, knowing the biometric trait may allow accessing the system. In order to clarify the differences between the two concepts, the ISO/IEC 24745 defines three aspects for each of them. Regarding privacy, it defines:

- *Irreversibility:* refers to the hardness to recover the biometric trait from the stored template.
- *Unlinkability:* multiple instances of biometric templates, i.e. (PI, AD) pairs, may not be linked together.
- *Confidentiality*: enrolled data may not be disclosed by unauthorized people.

Regarding security it defines:

- *Confidentiality*: this aspect has both privacy and security implications since the adversary may use the disclosed data to obtain unauthorized access to data or services.
- *Integrity*: it should be guarantee that the stored template has not been corrupted, intentionally or not.
- *Renewability and revocability*: if a template is compromised, the system should be able to define a new (PI, AD) pair from the same bio-

metric trait.[1]

The ISO/IEC 24745 standard defines the aforementioned requirements but does not specify the metrics to evaluate them. In this context, the WD 30136 standard on Performance Testing of Biometric Template Protection Schemes [WD 30136, 2014] plays an important role. The aim of the standard is to define "implementation-agnostic" metrics, i.e. metrics that are as much independent as possible from the specific architecture. One of the metrics that the standard defines is the *Successful Attack Rate* (SAR). SAR is defined as the "probability that an informed adversary can obtain a false accept result in a biometric system". An *informed attacker* is someone that, somehow, gained access to any enrolled information or secret parameters associated with one or more biometric recognition systems in which common individuals are enrolled. SAR concept is broader than False Match Rate (FMR) since it does not refer to simply guessing the biometric trait but to any kind of attack that may let someone being authenticated. Consequently, SAR is greater or equal to FMR (usually greater). Regarding privacy, the standard defines the *privacy leakage* as the "amount of information about an individual's generative biometric data which an adversary can learn from the stored reference data". The standard suggests measuring the amount of information leaked as the number of bits. As it will be explained in chapter 2, the author of this thesis does not consider it the right choice. Or at least, since biometric traits are noisy, and so the bits are not equally significant, one should consider the number of bits in terms of accuracy, not in terms of entropy. The attacker may be interested in estimating the biometric trait, rather than guessing the exact value. We will elaborate this concept in chapter 2. The standard defines other performance properties, some of them straightforward to evaluate, such as the *template size*, and others whose metric definition and evaluation test are not well defined, such as *unlinkability*. Actually, the unlinkability is one of the most dissimilarly evaluated parameters in the literature. Recently, in [Gomez-Barrero et al., 2018] the authors proposed a general framework to evaluate unlinkability. A drawback of the metric is that it should be evaluated for every "linkage function" that could be used to match two templates. A nice characteristic is that no assumptions are made on the data on biometric

[1] In this thesis, we will consider only irreversibility, unlinkability, and renewability aspects. The other aspects are associated to administration policies and the general security of the system as a whole, and not to specific biometric protection primitive used to generate the template.

statistics and the metric can be evaluated directly on data. In conclusion, despite the huge effort of the community, standardization of the testing of biometric protection is still an open issue. Its closure would be essential for both academia and industrial deployment. It would help us to have a common benchmark to compare algorithms, just like it is already done with standardised testing of the accuracy of recognition systems. Also, it would essential for biometric service providers and vendors in order to better describe what they provide. Especially regarding privacy, since, for example, regulations like GDPR [European Union, 2016] impose a series of data protection principles, it would be great to eventually have standard privacy level descriptors.

CHAPTER 2

A Zero-Leakage Fuzzy Embedder

The chapter is organized as follows. A summary of the fundamental concepts regarding zero-leakage template protection schemes is given in Section 2.1, where the approach proposed for achieving the desired perfect security, generalizing the method employed in [de Groot and Linnartz, 2011], is also introduced. The proposed secure framework is presented in Section 2.2, where the elements designed in order to allow the system achieving proper privacy and recognition performance are discussed in detail. The performed experimental tests, carried out on a large real world fingerprint database, are then described in Section 2.3, while conclusions regarding the proposed method are eventually given in Section 2.4.

2.1 Zero-Leakage Template Protection: preliminaries

In this section, we first introduce the conditions under which a zero-leakage biometric cryptosystem can be designed and then we sketch the rationale behind the proposed template protection scheme, detailed in Section 2.2.

Specifically, the proposed secure system relies on quantization index modulation (QIM) [Chen and Wornell, 2001], often employed to describe how to bind a generic biometric feature-based representation with a randomly generated secret key [Bui et al., 2010], and briefly summarized in Section 2.1.1. The information leakage analysis is discussed in Section 2.1.2, where it is also outlined how the proposed solution generalizes the state-of-the-art zero-leakage protection schemes.

2.1.1 Quantization Index Modulation

In its general exploitation, QIM allows embedding a secret key into a noisy signal. This is achieved by exploiting a set of A quantizers, being A the number of alphabet symbols, each employing different quantization levels. Assuming that the host signal x is scalar, the A quantizers can be defined by means of one uniform quantizer. Specifically, a uniform scalar quantizer $Q(x)$ with step Δ is defined as $Q(x) = \Delta \left\lfloor \frac{x}{\Delta} \right\rfloor$, with the $\lfloor \cdot \rfloor$ operator mapping its argument to the largest previous integer. The function $Q(x)$ can be used to generate A different quantizers as:

$$Q_m(x) = Q\left(x - m\frac{\Delta}{A}\right) + m\frac{\Delta}{A}, \tag{2.1}$$

where $m = 0, 1, 2, \ldots, A-1$. Storing $Q_m(x)$ instead of x for a given application allows to carry information on both the original signal as well as on the considered secret key m. An example of the reproduction levels of the quantizers set $\{Q_0, Q_1, \ldots, Q_{A-1}\}$ when $A = 3$ is given in Figure 2.1.

When applied for the purpose of protecting a biometric information x extracted during the user enrolment, the QIM approach can be exploited to generate a helper data z as the difference between the original signal x and its quantized version $Q_m(x)$ obtained through the $m - th$ quantizer, often also indicated as code-offset, that is,

$$z = x - Q_m(x). \tag{2.2}$$

For our purposes (2.2) can be written as:

$$z = \left[x - m\frac{\Delta}{A}\right]_\Delta = \left[[x]_\Delta - m\frac{\Delta}{A}\right]_\Delta, \tag{2.3}$$

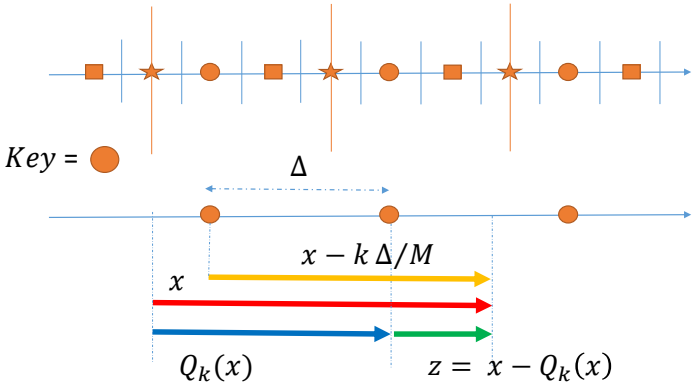


Figure 2.1: *QIM Principle.*

being $[\cdot]_\Delta$ the modulo Δ operation. Ideally, the storage of z should not reveal any information regarding either x or m, while allowing to perform recognition when a fresh template $\tilde{x}$ is made available, by retrieving the embedded key as:

$$\hat{m} = \arg\min_{\tilde{m}} \left| \tilde{m}\frac{\Delta}{A} - [\tilde{x} - z]_\Delta \right|. \tag{2.4}$$

If $\tilde{x}$ and x were identical, then $[\tilde{x} - z]_\Delta$ will be equal to $m\frac{\Delta}{A}$, and the extracted key $\hat{m}$ will be equal to m. More likely, $\tilde{x}$ is a noisy version of x, and the quantization step Δ has to be chosen accordingly to allow the retrieval of the original key.

2.1.2 Information Leakage

The main issue of a QIM-based biometric template protection scheme is the possible information leakage of the helper data z about both the adopted key m and the biometric template x in a non-randomness attack, which exploits the knowledge of the global statistics of the signal x and of the employed quantization step Δ [Linnartz and Tuyls, 2003]. Specifically, in this scenario, if we consider mutually independent template coefficients, the amount of information revealed by the helper data z about the secret key

m can be quantified by the mutual information between the two variables:

$$\begin{aligned} I(M,Z) &= h(Z) - h(Z|M) = \\ &= h(Z) - h\left([X - M\tfrac{\Delta}{A}]_\Delta | M\right) = \\ &= h(Z) - h([X]_\Delta | M) = \\ &= h(Z) - h([X]_\Delta), \end{aligned} \tag{2.5}$$

where $h(\cdot)$ denotes the differential entropy operator. It can be observed that, in case $[X]_\Delta$ has a uniform distribution in $[0; \Delta]$, the mutual information between Z and M would be zero:

$$I(M,Z) = \log \Delta - \log \Delta = 0. \tag{2.6}$$

The above condition would, therefore, guarantee a zero-leakage template protection system, in which the stored helper data z would not reveal any information about the employed secret m. In this regard, it has been demonstrated [Sripad and Snyder, 1977] that the necessary and sufficient condition to have $[X]_\Delta$ uniformly distributed is that the characteristic function (CF) of X, defined as the Fourier transform of its probability density function (PDF), satisfies the condition:

$$\varphi_X\left(\frac{2\pi l}{\Delta}\right) = 0, \quad \forall l \neq 0. \tag{2.7}$$

Unfortunately, it is unlikely to deal with real-world biometric data characterized by such property. It is therefore hard to implement practical zero-leakage biometric protected systems. Nonetheless, it is possible to apply some preprocessing to the extracted features in order to generate variables X having the desired characteristic as in (2.7).

Specifically, the addition of noise, with a uniform distribution in $[-\frac{\Delta}{2}; \frac{\Delta}{2}]$, to the original values in x, before applying quantization, has been suggested in [Buhan et al., 2008a]. According to this approach, since the PDF of the sum of two independent random variables is given by the convolution of the two PDFs, the CF of the resulting variable is given by the product of the respective CFs. In general, any random variable satisfying the condition (2.7) can be therefore employed as additive noise. However, this approach suffers from a severe drawback since it requires the presence of another key that must be kept secret. The key is in fact required during the verification phase to let the system generate the same noisy signal.

Therefore, the need to store this additional information is not of practical use in many contexts.

A preferable solution has been proposed in [de Groot and Linnartz, 2011] and in its extension [de Groot et al., 2016], where a fuzzy extractor framework [Dodis et al., 2004] is defined on the basis of a punctual transformation applied to the originally extracted features W in order to make their distribution uniform. This goal is achieved by applying to the data w a monotonic increasing function given by the cumulative distribution function (CDF) of W itself, that is:

$$x = f(w) = CDF_W(w), \tag{2.8}$$

thus generating a uniformly distributed variable X. It is worth pointing out that although this approach satisfies (2.7), it is not the only possible solution to the above mentioned goal.

In fact, in this thesis we propose a generalization of (2.8) as follows:

$$x = f(w) = {CDF_X}^{-1}\left[CDF_W(w)\right], \tag{2.9}$$

where CDF_X can be selected as any function representing the cumulative distribution function of a variable whose CF satisfies (2.7). The here proposed generalization (2.9) introduces a higher degree of freedom which we will exploit for selecting a transformation function that, while guaranteeing the needed zero-leakage requirements, could allow us to optimize other performance metrics of the proposed system, such as achievable recognition rate, security, or template irreversibility.

The proposed zero-leakage biometric cryptosystem, based on the use of the approach described in (2.9), is presented in Section 2.2, where a family of transformation functions able to satisfy the property in (2.7) is introduced, and the practical implementation strategies designed to achieve the desired performance when using real biometric data are presented. It is worth specifying that, given the above considerations, the biometric cryptosystem here presented is able to provide zero-leakage security against non-randomness attacks, which assume potential attackers possess the knowledge regarding global statistics of the employed biometrics. More treacherous attacks, such as those where the attacker already knows specific information regarding the biometrics of the interested user [de Groot et al., 2013], are not taken into account in the following discussion.

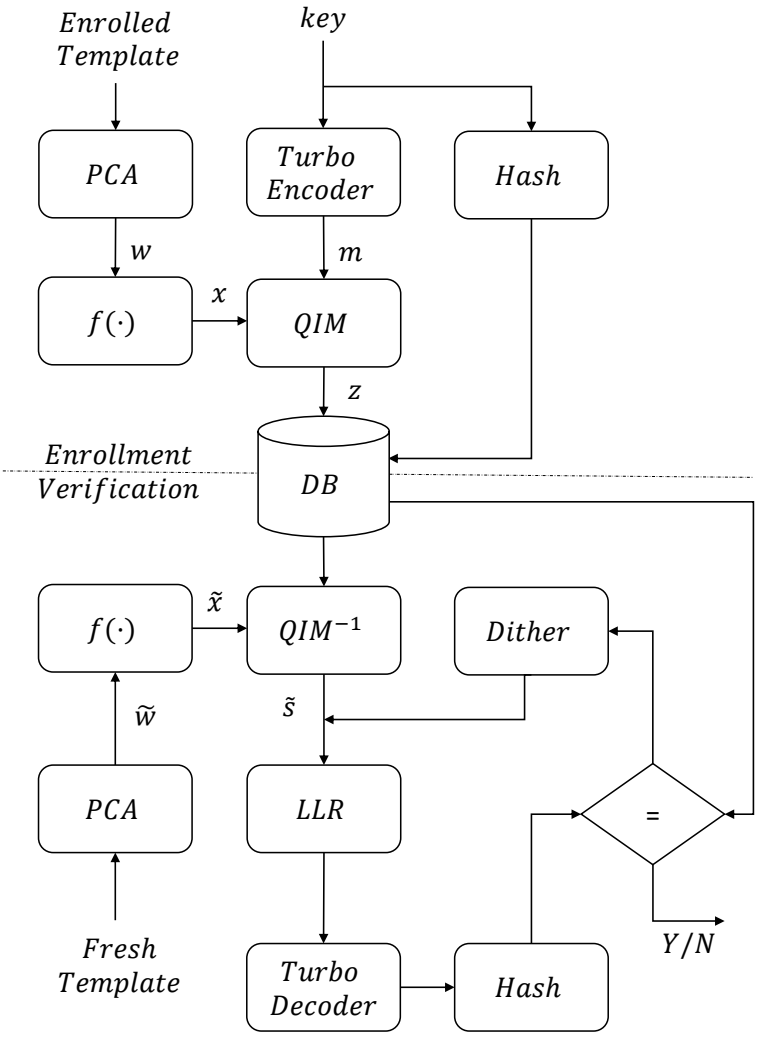


Figure 2.2: *Proposed biometric template protection scheme.*

2.2 The Proposed Biometric Cryptosystem

The proposed template protection scheme, described in Figure 2.2, besides not leaking any information about the employed secret through the stored helper data (see [Buhan et al., 2008a], [de Groot and Linnartz, 2011]), leverages on the generalization presented in (2.9) to guarantee proper per-

formance in terms of recognition rate, security, and template irreversibility, when applied to actual biometric scenarios.

In details, the preprocessing performed on the features extracted from a given biometrics is described in Section 2.2.1. The class of transformation functions proposed for the generation of templates satisfying (2.7) is introduced in Section 2.2.2. The effects resulting from the selection of a specific transformation family on the achievable recognition rates, as well as on the level of security of the proposed system, are discussed in Section 2.2.3 through the analysis of the embedding capacity per template coefficient. An evaluation of guaranteed template irreversibility, handled in terms of system privacy leakage, is provided in Section 2.2.4. In Section 2.2.5 a procedure to determine the system configuration to trade-off between security and privacy is then described. Eventually, in Section 2.2.6 we introduce a method to improve the recognition capability of the proposed protected system in terms of false recognition rate (FNMR), while keeping unaltered the other performance metrics. It is worth pointing out the proposed method, differently from zero-leakage state of the art approaches, is validated through an analysis conducted on real biometric data.

2.2.1 Template Preprocessing

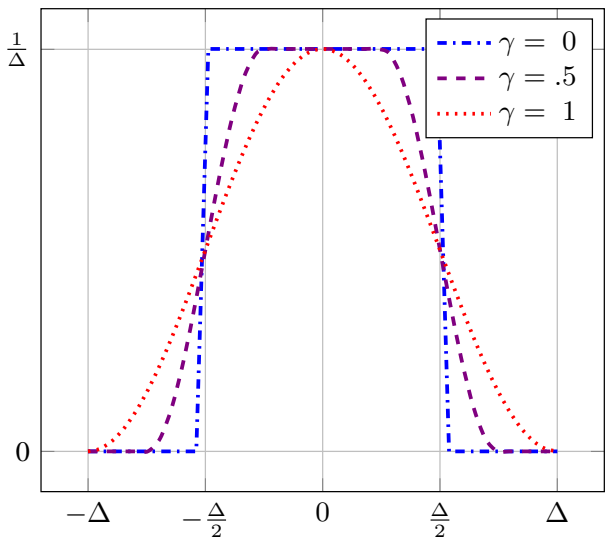


Figure 2.3: *Raised Cosine Probability Density Function.*

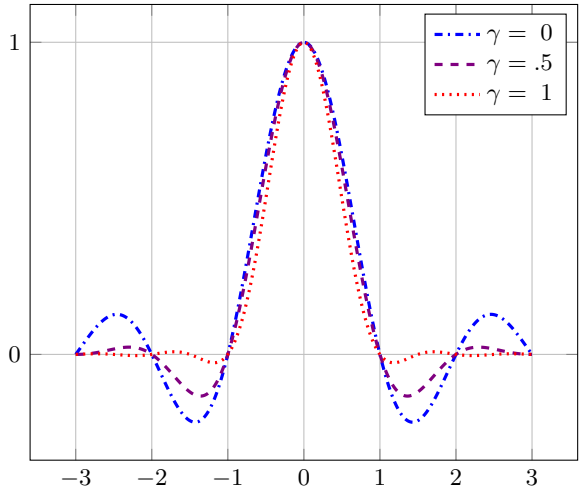


Figure 2.4: *Raised Cosine Characteristic Function.*

The description of QIM in Section 2.1.1, as well as the discussion about its information leakage when used for data protection in Section 2.1.2, has been conducted considering biometric information represented through mutually independent coefficients. Conversely, commonly employed feature-based template representations comprise a large number of strongly correlated coefficients. Nonetheless, the approaches described in Section 2.1 are still applicable to real biometric scenarios by performing a decorrelation process over the available data as a preliminary step of both the enrolment and verification stages. This goal can be achieved resorting to techniques such as principal component analysis (PCA) or linear discriminant analysis (LDA), given that the statistics of the target population's biometrics can be considered known. The following discussions are therefore carried out by describing the proposed operations as being applied in a coefficient-wise manner, having assumed that the treated biometric templates w are composed by a collection of practically independent scalar components.

It is, however, worth remarking that, even if the application of PCA or analogous transformations to the considered biometric data is needed in the proposed approach to achieve the desired zero-leakage property, such operation usually produces features with an increased intra-class variability with respect to the original ones, which makes often difficult to keep low

the FNMR in a protected system. In more detail, due to the PCA energy compaction property, the generated components are typically characterized by significantly different statistical properties. Therefore, in order to exploit such property, we propose an adaptive modulation technique described in Section 2.2.3, and a dithering-based performance improvement method in Section 2.2.6, meant to guarantee proper recognition rates when the aforementioned preprocessing is adopted.

2.2.2 Proposed Class of Transformations

After the decorrelation process described in Section 2.2.1 (see Figure 2.2) each generated component is transformed so that the distribution of the obtained coefficient satisfies the condition in (2.7). To this aim, the CDF_X function in (2.9) is here defined through the cumulative distribution function of the raised cosine class of functions as:

$$rc_{\gamma}^{\Delta}(x) = \begin{cases} \frac{1}{\Delta} & |x| < \frac{\Delta}{2}(1-\gamma) \\ \frac{1}{2\Delta}\left(1-\sin\frac{\pi(x-\frac{\Delta}{2})}{\Delta\gamma}\right) & \frac{\Delta}{2}(1-\gamma) < x < \frac{\Delta}{2}(1+\gamma) \\ \frac{1}{2\Delta}\left(1+\sin\frac{\pi(x+\frac{\Delta}{2})}{\Delta\gamma}\right) & -\frac{\Delta}{2}(1+\gamma) < x < -\frac{\Delta}{2}(1-\gamma) \\ 0 & \text{otherwise} \end{cases} \tag{2.10}$$

where $0 \leq \gamma \leq 1$. Figure 2.3 shows the PDFs associated with different values of γ. It can be observed that the approach employed in [de Groot and Linnartz, 2011] and [de Groot et al., 2016] can be considered as a particular case of the proposed method for $\gamma = 0$. On the contrary, in our approach, by varying γ in (2.9), we are able to trade-off between recognition, security and privacy performance, as detailed in the next sections.

2.2.3 Embedding Capacity Estimation: Adaptive Modulation

With reference to Figure 2.2, after the template w has been processed according to (2.7) in order guarantee zero-leakage, the QIM technique described in Section 2.1.1 is employed to embed $B = \log_2(A)$ secret bits into each template coefficient x, thus generating the stored helper data z. Specifically, the embedding can be performed by resorting to the digital modulation paradigm described in [Maiorana et al., 2012], where an original secret key of length k is fed to a n/k turbo encoder, in order to generate

symbols s belonging to a phase-shift keying (PSK) constellation of size A. Once a fresh biometric is acquired during the verification stage, a possibly corrupted codeword is retrieved by combining the available information with the stored helper data, and turbo codes are employed as in [Maiorana et al., 2012] to perform soft demodulation. This allows to fully exploiting the error correction capacity of the adopted codes.

It has to be remarked that the size of the employed constellations can be chosen adaptively with respect to each symbol. In fact, according to the proposed approach, the number of bits embedded into each coefficient x depends on its discriminative power, as well as on the parameter γ employed in the associated raised cosine transformation function. In order to gain

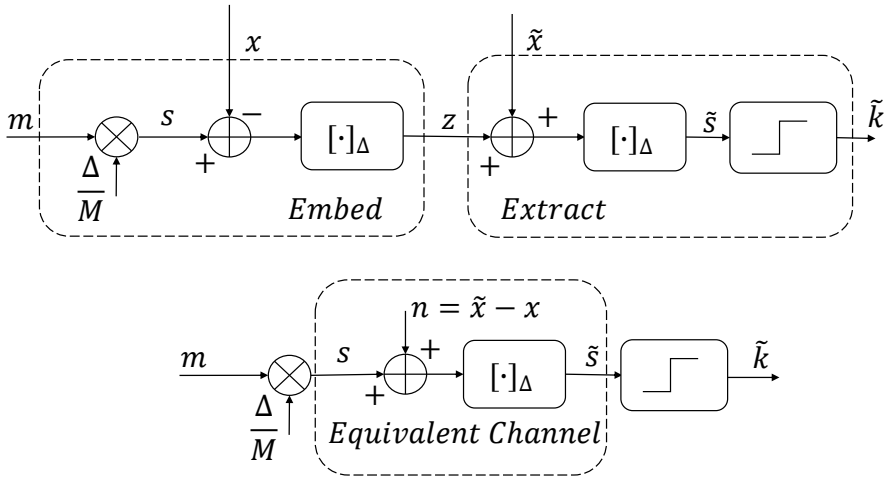


Figure 2.5: *Channel seen by the encoded secret key.*

more insights about the proposed approach, let us consider the equivalent channel, depicted in Figure 2.5, seen by the encoded secret m from its embedding (during enrolment) to its extraction (during verification) [Linnartz et al., 2007]. It can be in fact modeled through the introduction of an additive independent phase noise, given by the difference between the enrolled template x and the one presented during the verification phase $\tilde{x}$. Having indicated with s the PSK transmitted symbol, $s = m\frac{\Delta}{A}$ with $\Delta = 2\pi$, and with r the equivalent noise given by the difference between the enrolled template x and the fresh one $\tilde{x}$, the received noisy PSK symbol $\tilde{s}$ is ob-

tained as:

$$\begin{aligned}\tilde{s} = [\tilde{x} - z]_\Delta = [\tilde{x} - [x - s]_\Delta]_\Delta = \\ = [s + (\tilde{x} - x)]_\Delta = [s + r]_\Delta.\end{aligned} \tag{2.11}$$

In the genuine hypothesis (H_0) case, the characteristics of the phase noise r depend on the intra-class variability of the considered biometric representation, while in the impostor hypothesis (H_1) case, its statistics depend on the inter-class variability. We can therefore define two distinct channel capacities, giving the theoretical upper bounds on the rate at which information can be reliably transmitted over the equivalent channels under the two hypotheses, according to Shannon's definition: the genuine capacity C_{H_0} and the impostor capacity C_{H_1}, depending on the user typology at the verification stage. In the considered scenario, such capacities give us respectively the upper and lower boundaries for the information on the secret key which can be reliably transmitted over the equivalent channel:

$$C_{H_1} < \frac{k}{n} B < C_{H_0}, \tag{2.12}$$

being $\frac{k}{n}B$ the portion of the secret key entropy conveyed through the B bits embedded into the considered coefficient. Such percentage cannot exceed the genuine capacity C_{H_0}, since, otherwise, genuine users would not have any chance to correctly decode the secret. On the other hand, if such percentage is considerably lower than the non-genuine capacity C_{H_1}, the FMR would become unacceptable in practical applications. It has also to be remarked that, since the number of coefficients x in the available templates is usually limited, the employed error correcting codes won't be able to reach their best possible decoding performance, theoretically close to Shannon's limit [Berrou and Glavieux, 1996]. Therefore, it is recommended to have an adequate margin from the upper bound, while this is not required for the lower bound. Being possible for the considered coefficients x to significantly vary statistically-wise, and therefore in the associated capacity as a consequence, the number of bits to be allocated to each component should be chosen in an adaptive manner. In order to evaluate the channel capacities C_{H_0} and C_{H_1}, given (2.11) the former can be expressed

as:

$$\begin{aligned} C_{H_0} &= \max_{p_Z(z)} I(S, \tilde{S}) \\ I(S, \tilde{S}) &= h(\tilde{S}) - h(\tilde{S}|S) \\ &= h(\tilde{S}) - h([S+R]_\Delta|S) \\ &= h(\tilde{S}) - h([R]_\Delta) \\ \max\ h(\tilde{S}) &= -\int_0^\Delta \frac{1}{\Delta} log \frac{1}{\Delta} d\tilde{s} = log\Delta \\ \rightarrow C_{H_0} &= log\Delta - h([R]_\Delta), \end{aligned} \tag{2.13}$$

being the domain of $\tilde{S}$ bounded in $[0; \Delta]$, and being the differential entropy of limited domain random variable maximum when uniformly distributed.

The capacity C_{H_1} turns out to be equal to zero since, under the hypothesis of a non-genuine user during verification, the equivalent noise $[R]_\Delta$ is uniform in $[0,\ \Delta]$ due to the adoption of the proposed feature transformation in (2.9)[1]. This implies that the system operating point is implicitly set such that the FMR is next to zero, making the proposed protected system intrinsically robust against FMR-based attacks. The aforementioned property is a direct consequence of the design of the proposed system as a zero-leakage scheme, having a null mutual information between the key and the helper data.

Only the genuine capacity C_{H_0} has to be therefore evaluated in order to determine the number of bits B to be embedded into a given coefficient. Specifically, the assignable number of bits can be computed as:

$$B = \lfloor \frac{n}{k} \alpha\, C_{H_0} \rceil, \tag{2.14}$$

where the $\lfloor \cdot \rceil$ operator maps a real number to the closest integer value, while the parameter α is chosen within the interval $[0,\ 1]$ in order to let the sum of all the bits assigned to each coefficient being equal to the size n of the encoded secret key. Such bit allocation procedure implicitly selects the coefficients to be used in the system, since those with a very low capacity will have no associated bits and will be automatically discarded from the embedding process.

[1] The difference between two realization of a random variable uniform distributed in $[0; \Delta]$ has a triangular distribution in $[-\Delta; +\Delta]$. Thus, its modulo is uniform in $[0,\ \Delta]$

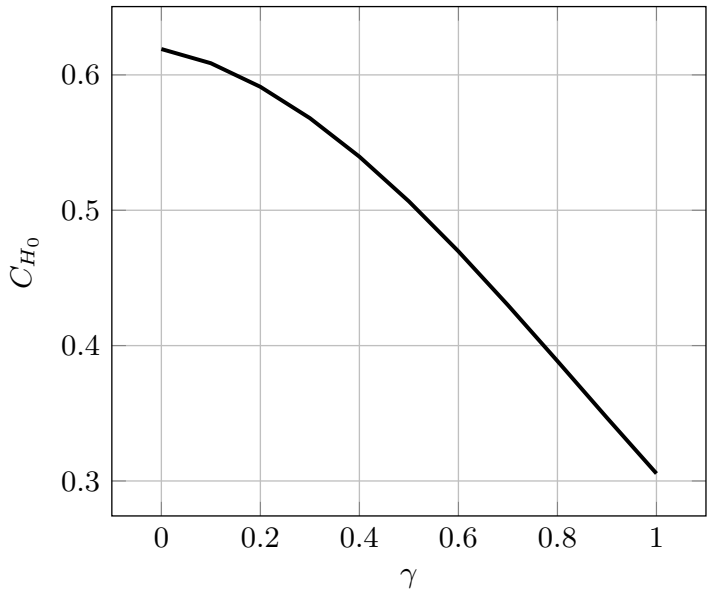


Figure 2.6: *Channel capacity C_{H_0} vs γ, for theoretic biometric distribution.*

It has to be pointed out that, in case the proposed class of transformations in (2.10) is employed to implement (2.9), C_{H_0} has a monotonically decreasing behavior with respect to the selection of the employed raised cosine parameter γ. As an example, Figure 2.6 shows the values obtained when considering the application of the proposed scheme to synthetic data generated with an equivalent channel having a signal-to-noise ratio (SNR) equal to $4.7dB$, suggested as characteristic of fingerprint templates in [Ignatenko and Willems, 2013]. Therefore, given a coefficient and its associated statistics, the number of bits that can be embedded into it also depends on the chosen parameter γ. Specifically, since using a lower γ would ensure higher capacity values, more bits can be embedded into the employed biometric representation, with a resulting improved security $H(M|Z) = H(M) = k$, for a given encoding ratio n/k and maintaining the condition in (2.12) for guaranteeing a proper FNMR. Likewise, for specific encoding ratio n/k and security k, achieving larger capacities C_{H_0} using lower γ parameters would result in improved FNMR, being the employed error correcting codes able to better deal with the considered intra-class variability. Although such observations would lead to choosing low

γ values for implementing the proposed zero-leakage cryptosystem, other performance metrics worsen because of this choice. Therefore, a proper trade-off strategy is described in Section 2.2.5.

2.2.4 Template Irreversibility: Privacy Evaluation

Together with the evaluation of the information leakage regarding the employed secret key $I(M, Z)$, a performance metric, commonly used for helper data based biometric cryptosystems, is the privacy leakage $I(X, Z)$ between the template X and the helper data Z. In this regard, this measure is not helpful when applied to a QIM approach since it diverges:

$$\begin{aligned} I(X, Z) = h(X) - h(X|Z) = \\ = h(X) - (-\infty) = +\infty. \end{aligned} \tag{2.15}$$

This happens because the random variable $X|Z$ is a discrete variable, while X is continuous. This fact does not imply that the knowledge of Z gives certain understanding of X. It is in fact due to the fact that the cardinality of X is reduced to be numerable.

Alternatively, since $X|Z$ is a discrete variable, we could measure the privacy of our scheme by means of the equivocation $H(X|Z)$ that describes the uncertainty about the template X given the knowledge of the helper data Z, commonly indicated as irreversibility:

$$\begin{aligned} H(X|Z) = H(X|[X]_\Delta) + H([X]_\Delta|Z) = \\ = H(X|[X]_\Delta) + H(M|Z) \end{aligned} \tag{2.16}$$

where $H(X|[X]_\Delta)$ represents the information loss about the template X after the modulo operation and $H(M|Z)$ relates to system security, expressing the uncertainty of the key once Z is known. It is worth pointing out that, in order to be authenticated by the system, the only required information is $[X]_\Delta$, whose equivocation related to Z is $H(M|Z)$. In fact, once m is known, $[x]_\Delta$ is univocally determined and vice versa. Nevertheless, the above-mentioned irreversibility measure only provides an indication of the possibility of retrieving the template X extracted during enrolment from the stored helped data Z. More practically, due to the noisy nature of the considered biometric data, an eventual attacker could be interested in getting just an estimate of X, rather than its exact value, since it would suffice in obtaining enough information about the biometrics of the targeted user.

In order to evaluate the privacy leakage associated with the proposed system in a broader sense, a more suitable index for the considered scenario can be defined as the mean root square error between the enrolled template x and its best estimation $\hat{x}(z)$ obtained from the helper data z, that is,

$$P = \frac{E_{X,M}\{(\hat{x}(z) - x)^2\}}{E_X\{x^2\}}. \tag{2.17}$$

Values of P range in $[0; 1]$, with larger values associated with a better privacy. The value $P = 1$ corresponds to a variance of the estimation error equal to the one of the original signal, with a consequent negligible privacy leakage. From the estimation theory, the minimum square error estimator is given by:

$$\hat{x}(z) = E_X(x|z) = \int x\, p_{X|Z}(x|z)\, dx, \tag{2.18}$$

which can be used for estimating the privacy metrics P in (2.17) for the proposed zero-leakage biometric cryptosystem.

Specifically, as it will be demonstrated in a while, the minimum square estimator of a variable X obtained through the application of raised cosine transforms, given the helper data Z, is:

$$\begin{aligned}\hat{x}(z) &= \int_X x p_{X|Z}(x|z)dx = \\ &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\left[m\frac{\Delta}{A} + z\right]_\Delta rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta\right) + \\ &+ \left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right) rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right)\end{aligned} \tag{2.19}$$

where $A = 2^B$ represents the number of possible symbols that can embedded in the considered coefficient using B bits. Given the aforementioned minimum square estimator, the behaviour of the considered privacy metrics P with respect to the parameter γ employed in the adopted raised cosine transform is shown in Figure 2.7. As it can be seen, the privacy of the proposed scheme increases with the use of larger values of γ, and embedding more bits in the considered coefficients. Comparing the plots in Figure 2.6 and 2.7, it can be seen that privacy and capacity are conflicting requirements for coefficients obtained through the employed raised cosine transform. A trade-off strategy is described in the next section.

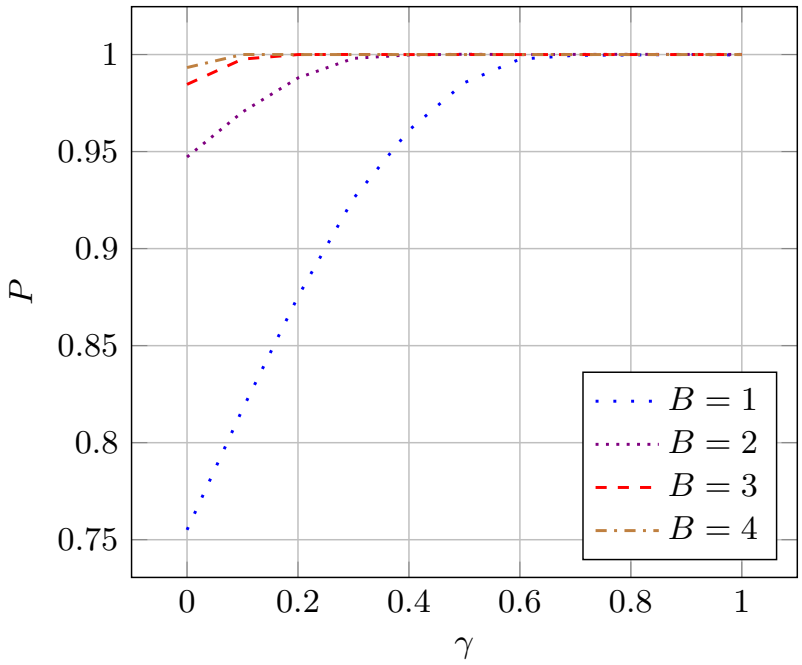


Figure 2.7: *Privacy leakage P vs γ, for different values of embedded bits B.*

Proof of equation 2.19

In this subsection, the biometric template minimum square estimator for the particular case of raised cosine distribution is demonstrated. Let us indicate:

- x the biometric template transformed by means of (2.9) so that its probability density function is characterized by (2.10);
- y the error of the quantized version of x, that is $y = [x]_\Delta$; $m = 0, 1, \ldots, A-1$ the symbol to embed in the coefficient;
- the helper data coefficient $z = [x - m\frac{\Delta}{A}]_\Delta = [y - m\frac{\Delta}{A}]_\Delta$.

Using the chain rule, it is straightforward to show that:

$$p_{X|Z}(x|z) = p_{Y|Z}(y|z)\frac{p_{X|Y}(x|y)}{p_{Y|Z}(y|z)} = p_{Y|Z}(y|z)\frac{p_X(x)}{p_Y(y)}. \tag{2.20}$$

Once z is set, y can be equal only to m equally likely values, depending on the embedded symbol:

$$p_{Y|Z}(y|z) = \frac{1}{A}\sum_{m=0}^{A-1}\delta_0\left(y - \left[m\frac{\Delta}{A} + z\right]_\Delta\right). \tag{2.21}$$

Replacing (2.21) into (2.20) and taking into account X and Y distributions, we have:

$$\begin{aligned} p_{X|Z}(x|z) &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\delta_0\left([x]_\Delta - \left[m\frac{\Delta}{A} + z\right]_\Delta\right) rc_\gamma^\Delta(x) \\ &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\left\{\delta_0\left(x - \left[m\frac{\Delta}{A} + z\right]_\Delta\right) + \right. \\ &\qquad \left. + \delta_0\left(x - \left[m\frac{\Delta}{A} + z\right]_\Delta + \Delta\right)\right\} rc_\gamma^\Delta(x) \end{aligned} \tag{2.22}$$

The minimum mean square estimator of x, known z, is thus given as follows:

$$\begin{aligned} \hat{x}(z) &= \int_X x p_{X|Z}(x|z)dx = \\ &= \frac{\Delta}{A}\sum_{m=0}^{A-1}\left[m\frac{\Delta}{A} + z\right]_\Delta rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta\right) + \\ &+ \left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right) rc_\gamma^\Delta\left(\left[m\frac{\Delta}{A} + z\right]_\Delta - \Delta\right) \end{aligned} \tag{2.23}$$

2.2.5 Transform Parameters (γ and B) Selection

As observed in the previous sections, the selection of the parameter γ of the raised cosine transform, here employed to satisfy (2.7), has hindering effects on the capacity and irreversibility of the associated coefficient. A proper strategy has to be therefore defined for selecting the γ parameter for each coefficient keeping both aspects into account. Specifically, we propose

to choose γ as the minimum value guaranteeing a desired level of privacy $\bar{P}$. This can be achieved by applying the following iterative procedure for each available coefficient:

1. $\gamma = 0$ is assigned at an initial stage;

2. the embedding capacity C_{H_0} in estimated through (2.13) and the number of bits to be embedded in the coefficient is set though (2.14);

3. the considered privacy level is estimated by means of (2.17);

4. if the evaluated privacy exceeds the target threshold level $\bar{P}$, the algorithm stops, otherwise, γ is increased and the procedure restarts from step 2.

The proposed γ-selection iterative procedure has to be performed for different values of α, till reaching the one for which the sum of the numbers of bits associated with each component is equal to n, once both the system security k and the desired encoding ratio n/k have been determined. It can be observed that the proposed strategy dynamically determines both the transformation to be applied, as well as the number of bits to be embedded into the coefficient, thus implementing the adaptive modulation approach presented in Section 2.2.3. As already remarked, and shown with the experimental results reported in Section 2.3, such adaptive modulation is especially relevant in case of coefficients decorrelated through techniques as PCA, which confine as much energy as possible in a few components, while leaving mostly noise in the remaining ones. Typically, a high γ value is assigned to these latter coefficients, whose statistics result in a low capacity which may imply the possibility of embedding a single bit, with the consequent requirement of a high γ value for guaranteeing high privacy levels, as shown in Figure 2.7. Low γ values are instead associated with coefficients characterized by a high capacity, having the possibility of embedding a large number of bits into them.

It is worth pointing out that, although the proposed γ and B adaptive selection strategy requires the storage of additional information in the system, this does not affect the privacy and security of the enrolled users, since the same parameters are employed for all of them.

2.2.6 Performance Improvement through Dithering

As already pointed out, the proposed system is characterized by construction by a very low FMR, that could lead to a high FNMR. In order to compromise between the two, an iterative process based on dithering is performed during the verification phase, as shown in Figure 2.2. Specifically, the proposed approach takes inspiration from real life when people are unable to open a door with the correct key: shaking a bit the key till all the gears of the lock are aligned often allows opening the door. Such operation typically increases the success rate of the genuine user, while having a negligible influence on the success rate of an impostor using the wrong key.

In case a match between the stored hash and the one retrieved during verification is not obtained, trying to slightly alter the template $\tilde{x}$ with an additive zero-mean uniformly distributed noise, and then attempting again to decode the resulting message, could be beneficial for improving the system recognition rate in terms of FNMR, without affecting notably the associated FMR. For each treated coefficient the width of the noise distribution can be defined as a fraction of the decision interval for a PSK symbol. In the practical implementation of the proposed approach, employed to obtain the results described in Section 2.3.2, such noise is defined in order to be kept in the range $[-0.3\frac{\Delta}{A}; 0.3\frac{\Delta}{A}]$. The number of iterations T the system can perform while trying to correctly decoding the original secret key is obviously limited by computational time constrains. An analysis of the effects of the proposed dithering approach on the achievable performance is reported in Section 2.3.2.

2.3 Experimental Analysis

The proposed system described in Section 2.2 is here analyzed when applied for a practical application involving fingerprint data. Section 2.3.1 introduces the adopted template representation, as well as the database providing the employed biometric data. The performance achieved by the proposed system when applied to the considered practical scenario are then reported in Section 2.3.2.

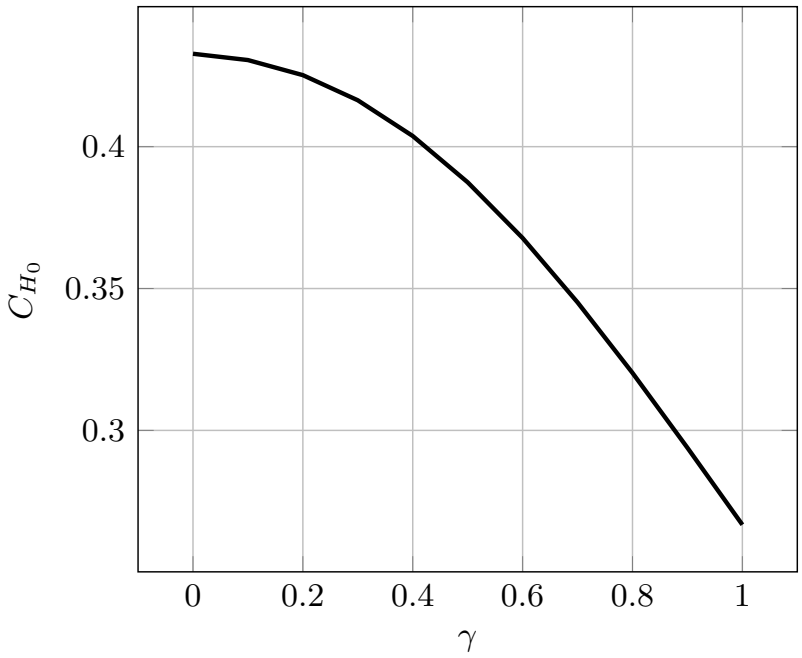


Figure 2.8: *Channel capacity C_{H_0} vs γ, for the considered fingerprints.*

2.3.1 Employed Template Representation

Without any loss of generality, we employ fingerprints to test the performance of the proposed system when applied to real data. More specifically, traditional fingerprint recognition approaches rely on the extraction of minutiae information from the analyzed traits, localizing ridge anomalies such as bifurcations or endings. Nevertheless, such technique produces templates composed by unordered sets of characteristics with variable sizes, while the proposed cryptosystem is designed to be applied to fixed-dimension ordered collections of parametric features. In order to obtain such template, the FingerCode representation proposed in [Jain et al., 2000] is here taken into account. According to this processing, a reference fingerprint point, characterized by the maximum curvature of the concave ridges, is first determined. The fingerprint region around this point is then divided into different sectors, each processed through a bank of Gabor filters used to capture both local and global fingerprint details. According to the processing described in [Jain et al., 2000], 640 features can be generated

for each fingerprint.

The employed biometric data are taken from the BiosecurID DB [Fierrez et al., 2010], comprising 16 optical impressions for each of the index and middle fingers from both right and left hands of 400 subjects. Such fingers have been acquired in the considered DB taking into account that they could be easily simultaneously captured at once, in a very fast and comfortable way, in practical recognition systems. Acquisition devices able to collect four fingerprints at one time are commercially available and widely used in real-life critical scenarios, like the border crossing US-Visit. Such acquisition modality could be therefore easily employed to replace knowledge-based authentication procedures relying on PINs or passwords with a biometric-based approach (e.g. cash withdrawal).

The impressions from all the four available fingers of a given person are considered altogether in generating a single template, making thus available for testing a set of 16 templates composed by $4 \cdot 640 = 2560$ coefficients for each of employed 400 users.

The available dataset is split into two disjoint subsets, comprising acquisitions coming from 100 and 300 subjects. The first subset is employed to test the performance of the proposed system, as reported in the following section. The remaining 300 users are exploited to train the considered protected cryptosystem, providing the data for estimating the needed PCA projection matrix, as well for evaluating the capacity associated with each transformed component. In this regard, Figure 2.8 reports the actual behavior of the capacity C_{H_0} with respect to the adopted parameter γ, evaluated as the mean curve over all the coefficients of the employed whitened template. It can be seen that the mean capacity estimated for the proposed fingerprint representation is significantly lower than the one reported in Figure 2.6, evaluated on the basis of the assumptions taken in [Ignatenko and Willems, 2013], testifying the difficulty of implementing a zero-leakage cryptosystem usable with real biometric data. It has to be remarked that, since the dimension of PCA projections is limited by the minimum between the number of classes employed for the training phase and the size of the original representation, template representations with only 299 coefficients are generated by the proposed approach, and used as templates for the method described in Section 2.2. Larger representations with more components could be processed in case larger training databases would be available in

practical applications.

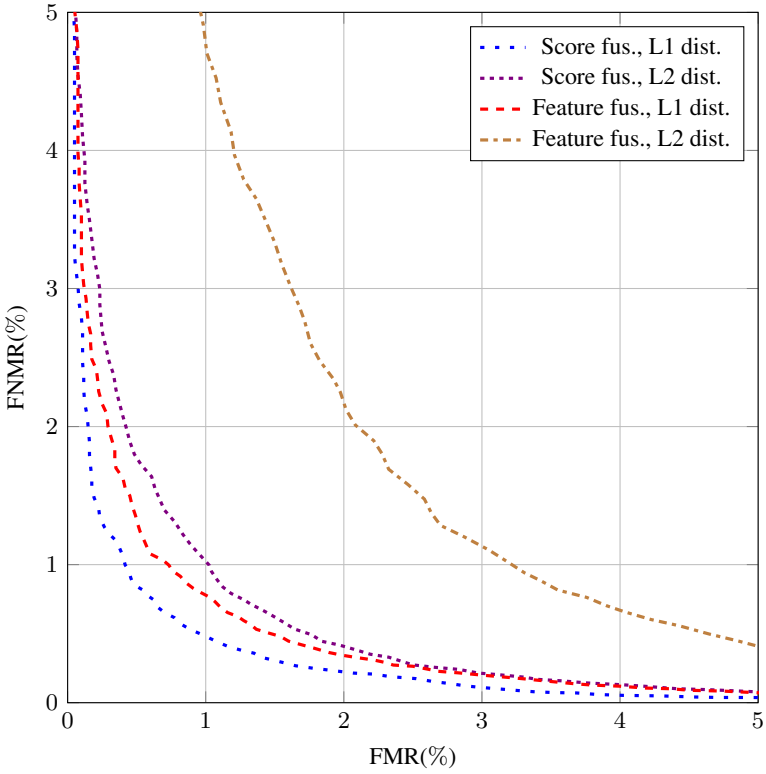


Figure 2.9: *Recognition performance of unprotected systems.*

2.3.2 Experimental Results

The recognition rates achievable with unprotected systems exploiting the features extracted from the considered fingerprint data are reported in Figure 2.9. Specifically, we have evaluated the performance reachable when fusing the information from the four available fingers of each subject at feature and score levels, using the inverse of both L1 and L2 distance metrics as matching scores. The best of the four classifiers gives an equal error rate (EER) of 0.67%.

Table 2.1 summarizes the results obtained when evaluating the performance of the considered protected biometric cryptosystems. Specifically, the required minimum level of privacy which has been employed in the iterative procedure described in Section 2.2.5 is $\bar{P} = 0.99$. We have

Table 2.1: *Performance of the proposed zero-leakage cryptosystem, with either static or dynamic bit allocation for QIM embedding.*

k	FNMR(%)		
	Static allocation	Dynamic allocation(DA)	DA + 100 dithering iterations
40	9.99	7.05	4.21
48	12.15	10.18	6.56
56	15.79	13.99	9.82
64	21.34	19.79	14.28

investigated the behaviors achievable when using secret keys of length $k = \{40, 48, 56, 64\}$, and compared the capabilities of systems based on either static or dynamic bit allocation. In the case of dynamic bit allocation, the rate of the employed error correcting turbo code has always been set to $\frac{n}{k} = 7$. When considering static bit allocation, the adopted rate has been chosen in the set $\frac{n}{k} = \{3, 5, 7\}$ as the one minimizing the FNMR, that is, selecting the largest ratio $\frac{n}{k}$ admissible once the length of the secret key k and the number of available coefficients has been fixed. In more detail, in case of static bit allocation, the n bits are embedded into the n most stable coefficients, *i.e.* the n coefficients with highest embedding capacity. Only the FNMR recognition rate is reported in Table 2.1 since, as already remarked, the proposed zero-leakage system is by construction set to an operating point with approximately null FMR, a condition which has been confirmed in the experimental tests. From the reported results it is evident that, for all the considered key lengths, the dynamic bit allocation strategy ensures better performance in comparison with static bit allocation.

It has to be remarked that the static bit allocation here considered guarantees recognition performance practically indistinguishable from those obtained when applying the approach in [de Groot and Linnartz, 2011] and [de Groot et al., 2016]. However, only transformations with $\gamma = 0$ are there considered, whereas in the proposed approach, larger γ values can be employed even when considering a static bit allocation method, thus resulting in a FMR lower privacy leakage. In fact, as shown in Figure 2.7, the required condition of minimum privacy equal to $\bar{P} = 0.99$ cannot be satisfied with a γ parameter equal to zero, regardless of the number of bits embedded in a given coefficient. It is also worth pointing out that, in case

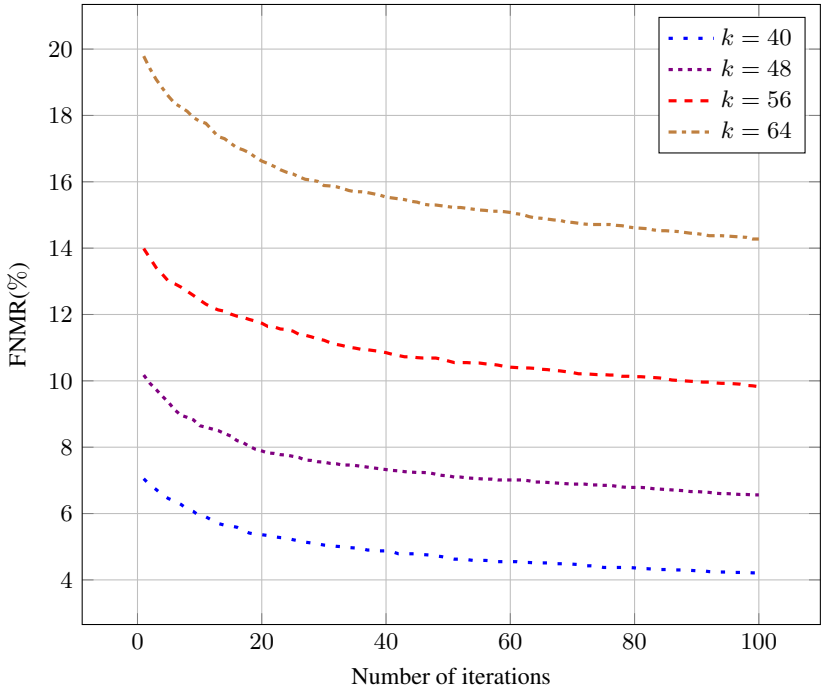


Figure 2.10: *FNMR improvement with respect to the number of iterations performed in the proposed dithering approach.*

a less strict requirement would have been taken into account for the minimum privacy level $\bar{P}$, the iterative procedure described in Section 2.2.5 would have led to the selection of lower γ values, with higher capacities therefore associated with each coefficient, and the consequent possibility of either embedding more bits increasing the security k of the system, or improving the achievable recognition performance in terms of FNMR.

The experimental results reported in Table 2.1 also show that a significant improvement in terms of FNMR can be achieved when the proposed dithering technique is exploited. Figure 2.10 shows the trend of the obtained FNMR with respect to the number of attempts performed in the proposed dithering technique. However, we would like to point out that the proposed dithering method, besides improving the achievable FNMR, also affects the security of the proposed cryptosystem with respect to FMR-based attacks. In fact, performing several recognition attempts for each presented biometrics may increase the probability of accepting a malicious user. Specifically, a loss of up to $log_2(T)$ bits against a FMR-based at-

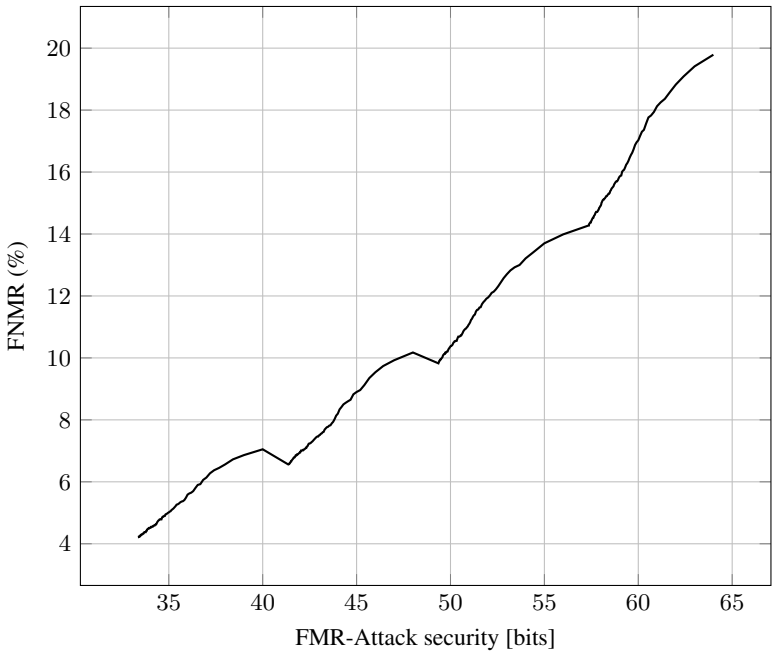


Figure 2.11: *FNMR behavior with respect to the associated security, expressed in terms of robustness against FMR-based attacks, when adopting the proposed dithering technique.*

tack, being T the number of performed iterations, can be assumed when the dithering process is carried out. In the performed experimental tests, a FMR greater than 0, and specifically equal to 0.0051%, has been registered only when considering secret keys with $k = 40$, reasonably due to the limited training resources that have been exploited to properly estimate the PCA projection matrix and the coefficients' capacities. Nevertheless, the behavior of the achievable FNMR with respect to the theoretic security against FMR-based attacks, when considering secret keys having length $k = \{40, 48, 56, 64\}$ bits, is depicted in Figure 2.11. This figure, as well as Figure 2.10, also illustrates that implementing a dithering approach allows tuning with improved degrees of freedom the recognition performance of the proposed cryptosystem. In fact, since standard implementations of error correcting codes, such as the turbo-codes we have employed, leave the possibility of choosing only a finite pre-defined set of key lengths to be encoded, the resulting number of feasible operational points may be signifi-

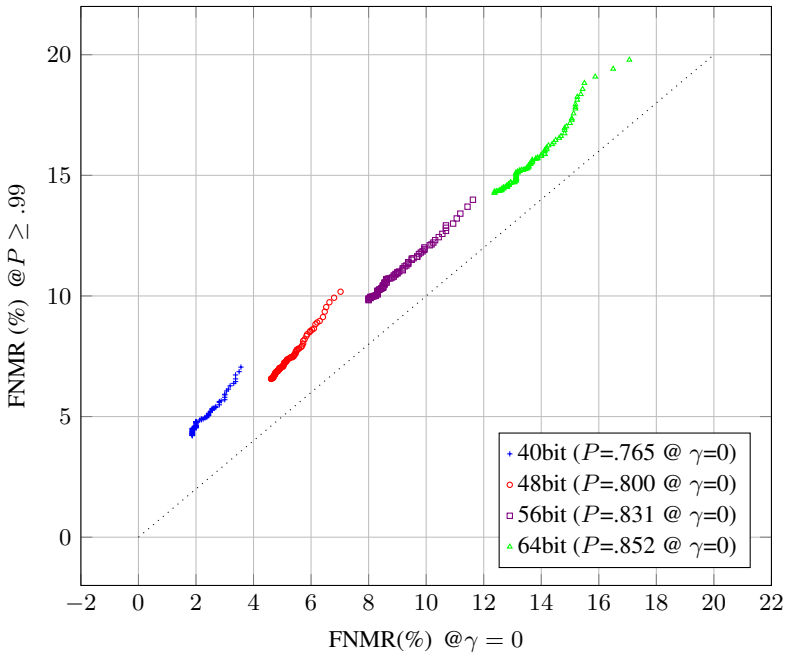


Figure 2.12: *Performance comparison between systems using γ = 0, and systems adopting the proposed adaptive γ selection procedure for guaranteeing a privacy level $P > 0.99$.*

cantly limited. Such limitation can be overcome by exploiting the proposed dithering technique, thus guaranteeing the capability of selecting the operating point providing the desired FNMR, even if the security associated with a FMR-based attack may be affected by the process. It is worth remarking that the security against brute-force and non-randomness attacks remain unaffected by the proposed dithering approach.

We eventually further outline in Figure 2.12 the existing trade-off between the achievable recognition rates, in terms of FNMR, and the possible privacy leakage P. Specifically, a comparison between the results which could be obtained when $\gamma = 0$ is adopted for each considered coefficient, and those achieved by our proposed system with adaptive γ selection is shown. Each plotted point represents the performance, in terms of FNMR, obtained when considering keys having length $k = \{40, 48, 56, 64\}$ bits, by applying up to 100 dithering iterations. As it can be seen, a system using $\gamma = 0$ always performs better in terms of recognition rates, even if at the cost of a reduced privacy P, reported as the average evaluated over all

the employed coefficients for each considered key length. Conversely, the proposed γ selection strategy always guarantee a minimum desired privacy level $P > 0.99$, at the cost of a slight reduction in FNMR.

2.4 Discussion

In this chapter, we have introduced a novel zero-leakage biometric cryptosystem. The proposed system guarantees no information leakage about the employed secret key from the stored helper data in case of non-randomness attacks, and it allows achieving a trade-off between privacy and recognition rates. Specifically, in our approach, we have introduced a class of transformation functions enforcing zero-leakage. In addition, we have proposed a strategy for adaptively embedding the bits of the secret key into the extracted template. Moreover, a system parameters optimization strategy with respect to security, recognition performance, and privacy has been proposed. As a proof-of-concept, and differently from state-of-the-art approaches, the proposed method has been tested on real fingerprint data. Experimental results show the effectiveness and the flexibility of the proposed system.

CHAPTER 3

Unlinkability

In this chapter, we show that the method that has been proposed in chapter 2 suffers the so-called linkability attack. We, therefore, propose an enhanced system resistant to the attack.
The chapter is organised as follow. First, we introduce the linkability concept and its threats to privacy and security. Then, after showing how easy it is to run the linkability attack on a QIM-based system, we describe the proposed solution. In section 3.3, the robustness versus two types of attacks are analysed. Lastly, in section 3.4, some design aspects related to the noise statistics of the biometric data are analysed.

3.1 The Linkability Issue

The problem of linkability (or traceability) is probably one of the hardest issues in biometric protection. Many techniques have been studied in order to obtain reliable identifiers from the biometric traits that cannot be easily reversed. As we have seen in the previous chapter, we can also find theoret-

ical guarantees of the impossibility of retrieving the original biometric. But that is not enough. Nowadays, we are asked to be authenticated to tens of services. Therefore, in an ideal password-less world, we should be able to extract from our biometric trait an independent identifier per each service we want to be authenticated to. We also should be able to renew the identifier if it is compromised. Ideally, it should not be possible to link together these identifiers. That is a pretty tricky matter to solve. It has been demonstrated that it is not possible to guarantee no information leakage about the original biometrics [Ignatenko and Willems, 2008]. That is because the helper data should contain at least a minimum amount of information to absorb the intraclass variability of the biometric signal and guarantee a reliable authentication. Even apparently negligible leakages of information may be enough to link together identifiers. Although we cannot guarantee theoretically provable unlinkability, we can settle computational complexity boundaries.

3.2 An Enhanced System to Prevent the Linkability Attack

In the previous chapter, the design of a zero leakage fuzzy embedder was analysed, i.e. a crypto-system whose helper data do not leak any information about the embedded key. One aspect that we have not analysed so far is the linkability. Given two identifiers, is it possible to determine whether these are linked to the same person or not? Actually, with the QIM system we described, the linkability attack is straightforward. In fact, as it has been shown in [Buhan et al., 2010a], given a couple of helper data z_1 and z_2 derived from the same user using different keys, we have:

$$[z_1 - z_2]_\Delta = [x - s_1]_\Delta - [x - s_2]_\Delta = [s_2 - s_1]_\Delta, \tag{3.1}$$

i.e., under the hypothesis of same user's helper data, their difference is bounded to a discrete set of values. On the other hand, when users are different, $[z_1 - z_2]_\Delta$ is uniformly distributed in $[0, \Delta]$. Even in the case that x_1 and x_2 are not exactly the same, but they slightly differ because of the intra-class variability, $[z_1 - z_2]_\Delta$ would be close to $[s_2 - s_1]_\Delta$ and the linkability attack would still success to couple the two identifiers.

The idea we had is to use a rotation matrix, as it is similarly done with bio-hashing [Jin et al., 2004]. Consider the scheme in figure 3.1. w is a

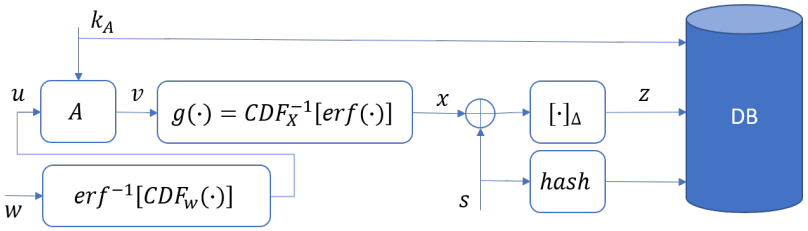


Figure 3.1: *Proposed scheme against linkability attack*

vector of mutually statistically independent features. The first transformation $\text{erf}^{-1}[CDF_W(\cdot)]$ makes u distribution Gaussian with zero mean and unitary variance. A is a record-specific rotation matrix. Since A is an orthonormal matrix, also v has the same characteristics as u. In this way, we can apply the same transformation $g(\cdot) = CFD_X^{-1}[\text{erf}(\cdot)]$ regardless the specific orthonormal transformation A.
Note that, when $A = I$, the just described scheme is equivalent to the one proposed in chapter 2:

$$CFD_X^{-1}\left[\text{erf}\left[\text{erf}^{-1}\left[CDF_W(w)\right]\right]\right] = CFD_X^{-1}\left[CDF_W(w)\right] \tag{3.2}$$

A very similar idea has been applied in [Kelkboom et al., 2011] in the context of fuzzy commitment. In that work, the authors proposed to apply a permutation matrix to the biometric bit-steam before the key binding. The idea is very similar since a permutation matrix itself is a rotation matrix. However, it is easy to see that in our scheme, a permutation matrix would be useless, since, if the matrix is known, it doesn't make the attack harder.

3.3 Attacking the System

If we consider two identifiers generated with the same biometric trait w but different transformation matrices A_1 and A_2, the linkability attack is not that straightforward. z is not any more a point-wise function of the input signal w, but each coefficient of z is a non linear function of all the coefficients of w.
With the following mathematical steps, we will try to reverse the system. We have that:

$$z = [g(Au) - s]_\Delta. \tag{3.3}$$

Let's isolate u:

$$[z + s]_\Delta = [g(Au)]_\Delta. \tag{3.4}$$

Since the $g(\cdot)$ codomain is limited at most to $[-\Delta, +\Delta]$ (since x is distributed as in 2.10), we can write:

$$[g(Au)]_\Delta = g(Au) + m\Delta \text{ with } m \in \{0, 1\} \tag{3.5}$$

so,

$$u = A^T g^{-1}([z + s]_\Delta - m\Delta). \tag{3.6}$$

So, if we take into account two helper data z_1 and z_2, generated respectively by the sets $\{x_1,\ s_1,\ A_1\}$ and $\{x_2,\ s_2,\ A_2\}$, and we assume $x_1 = x_2 = x$, we have:

$$A_1^T g^{-1}([z_1 + s_1]_\Delta - m_1\Delta) = A_2^T g^{-1}([z_2 + s_2]_\Delta - m_2\Delta). \tag{3.7}$$

With some mathematical steps we obtain:

$$\begin{aligned} g_2\left(A_2 A_1^T g^{-1}([z_1 + s_1]_\Delta - m_1\Delta)\right) &= [z_2 + s_2]_\Delta - m_2\Delta \\ \left[g_2\left(A_2 A_1^T g^{-1}([z_1 + s_1]_\Delta - m_1\Delta)\right)\right]_\Delta &= [z_2 + s_2]_\Delta \\ \left[g_2\left(A_2 A_1^T g^{-1}([z_1 + s_1]_\Delta - m_1\Delta)\right) - z_2\right]_\Delta &= [s_2]_\Delta = s_2 \\ \left[g_2\left(A_2 A_1^T g^{-1}([z_1 + s_1]_\Delta - m_1\Delta)\right) - z_2\right]_\Delta &= [s_2]_{\frac{\Delta}{M}} = 0. \end{aligned} \tag{3.8}$$

The last statement is a system of non linear equations whose unknowns are the coefficients of s_1 and m_1 vectors. Now, if one is able to find a couple of strings $\{s_1, m_1\}$ that satisfies equation 3.8, he would be able to link the two identifiers to the same user. The mixture of modulo, rotation, and non-linear operators makes the system of equations strongly non-smooth. Therefore, the author expects the system to be not solvable by means of some iterative algorithm. Consequently, guessing the correct string has a computational cost that is exponentially proportional to the entropy of the two strings. Note that the equivocation of m_1 grows with γ. In fact, when $\gamma = 0$, m has zero entropy since, in this case, no information are loss after applying the modulo operator. As γ grows, the uncertainty of m grows roughly linearly, as shown in figure 3.2.

An other way to run the linkability attack is by matching the estimations of the biometric templates from different helper data. Similarly to what we have seen in section 2.2.4, the template u can be estimated as:

$$\hat{u}(z) = E\left[A^T g^{-1}\left([z + s]_\Delta - m\Delta\right)\right], \tag{3.9}$$

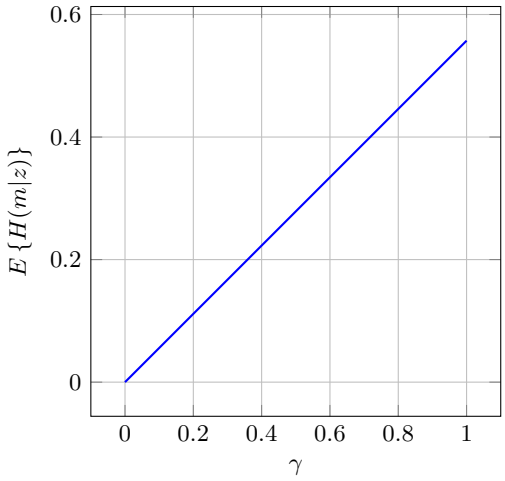


Figure 3.2: *Average entropy (per coefficient) of the auxiliary variable m*

where $E[\cdot]$ denotes the expected value. So, given two sets of helper data $\{z_1, A_1\}$ and $\{z_2, A_2\}$, an attacker can estimate $\hat{u}_1$ and $\hat{u}_2$ and compute their similarity, for example, by means of Euclidean distance. Since, in this case, the linkability attack is not deterministic, we should use some measure to evaluate its effectiveness. A nice linkability measure has been proposed in [Gomez-Barrero et al., 2018]. Suppose there is a "linkage function" $s = LS(T_1, T_2)$ that try to classify whether the identifiers T_1 and T_2 are mated, i.e. linked to the same user. The linkability $D_{\leftrightarrow}^{sys}$ is defined as:

$$D_{\leftrightarrow}^{sys} = \int p(s|H_m) D_{\leftrightarrow}(s) \mathrm{d}s \tag{3.10}$$

where

$$D_{\leftrightarrow}(s) = \begin{cases} 0 & \text{if } LR(s) \cdot \omega \leq 1 \\ 2\dfrac{LR(s) \cdot \omega}{1 + LR(s) \cdot \omega} - 1 & \text{if } LR(s) \cdot \omega > 1 \end{cases} \tag{3.11}$$

is the score specific linkability,

$$LR(s) = \frac{p(s|H_m)}{p(s|H_{nm})} \tag{3.12}$$

is the likelihood ratio between mated (H_m) and non-mated distributions (H_{nm}), and $\omega = p(H)/p(H_{nm})$ denotes the ratio between the unknown

prior probabilities of the mated samples and non-mated scores distributions. $D_{\leftrightarrow}^{sys}$ is bounded in $[0,\ 1]$ and the extreme values correspond respectively to fully separable and fully overlapping mated and non-mated distributions. I.e., $D_{\leftrightarrow}^{sys} = 1$ indicates that the biometric identifiers are fully linkable, while $D_{\leftrightarrow}^{sys} = 0$ that they are not, at least when considering the specific linkage function under examination. As we have seen in the previous chapter, the estimation accuracy can be made arbitrary small by increasing the value of γ of the proposed transformation function 2.10. As a matter of fact, we can choose a proper value of γ that lets the linkability attack through estimation totally ineffective. In figure 3.3, the linkability measure from [Gomez-Barrero et al., 2018] as a function of γ is shown. We assume as linkage function the Euclidean distance between estimations made through equation 3.9. As you can see, when $\gamma = 0$, $D_{\leftrightarrow}^{sys}$ is roughly equal to 1. This means the that the mated templates are fully linkable. As γ grows the accuracy of the estimation drops and the helper data of different users get indistinguishable each other. This fact validates our privacy analysis described in section 2.2.4.

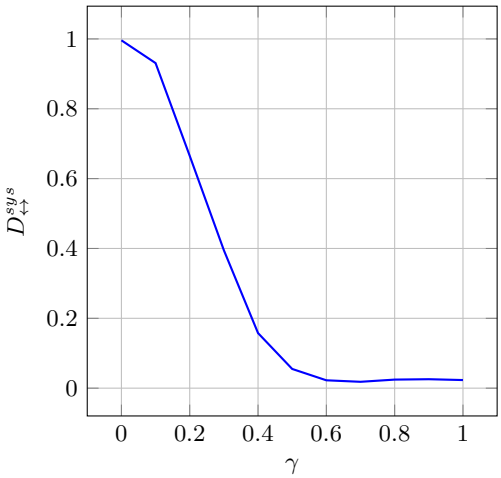


Figure 3.3: *Linkability vs* γ

An other important aspect when dealing with multiple instances is the gain that an attacker may achieve once he knows multiple helper data belonging to the same user [Simoens et al., 2009]. As we have seen in Section 2.2.4, it is possible to obtain a better-than-random estimation of the original biometric from the helper data. Therefore we can expect that we can obtain

more accurate estimation with multiple instances of helper data. Suppose we have several helper data sets $\{A_1, z_1\}$, $\{A_2, z_2\}$, .. $\{A_N, z_N\}$. The simplest way to estimate u is to average the estimations obtained from each set by means of equation 3.9:

$$\hat{u} = \frac{\hat{u}_1 + \hat{u}_2 + \cdots + \hat{u}_N}{N}. \tag{3.13}$$

In figure 3.4, the average normalized estimation error in the cases of $N = 1, 2, 3$ for different values of γ are shown. It turns out that, in the case that a small value γ is used, there is effectively a gain in the estimation accuracy with multiple helper data instances. For higher values of γ, no gain is obtained because the estimation accuracy is too low.

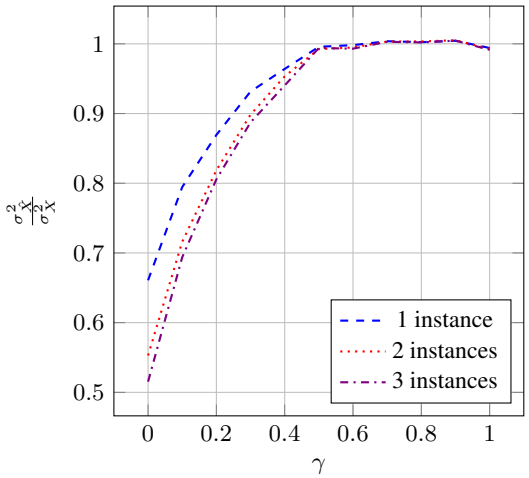


Figure 3.4: *Normalized estimation error of the biometric source with different numbers of known helper data instances*

3.4 Dealing With Non-IID data

As we have seen in chapter 2, when we deal with real data, many unexpected difficulties come out. The method we propose in this chapter works under the hypothesis of uncorrelated coefficients. As we have already discussed, in order to obtain quasi-uncorrelated coefficients, whitening techniques such as PCA must be used. It is well known that PCA has the side effect of letting the strength of the coefficients very unevenly distributed.

We will show in this section that, in this scenario, the rotation matrix can drastically downgrade the recognition performances.
Let us consider a toy example of a two-coefficients template (x_1, x_2) with unitary covariance matrix and Gaussian distribution. Let us suppose that the noise of the two coefficients have respectively energy σ_1^2 and σ_2^2, and that $\sigma_1^2 + \sigma_2^2 = 1$. In the extreme case $|\sigma_1^2 - \sigma_2^2| = 1$, all the energy is concentrated in one coefficient and the other is pure noise. In this case, the capacity is infinite. On the contrary, the more the noise is evenly distributed between coefficients, the more capacity decreases. This behaviour is shown in figure 3.5. The bad news is that any rotation of the matrix distributes the energy more evenly. Let's consider the transformation:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \leftarrow \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{3.14}$$

then we have:

$$\sigma_1^2 - \sigma_2^2 \leftarrow (\sigma_1^2 - \sigma_2^2)(2\cos^2\phi - 1). \tag{3.15}$$

Consequentially, the rotation decreases the overall capacity. [1]

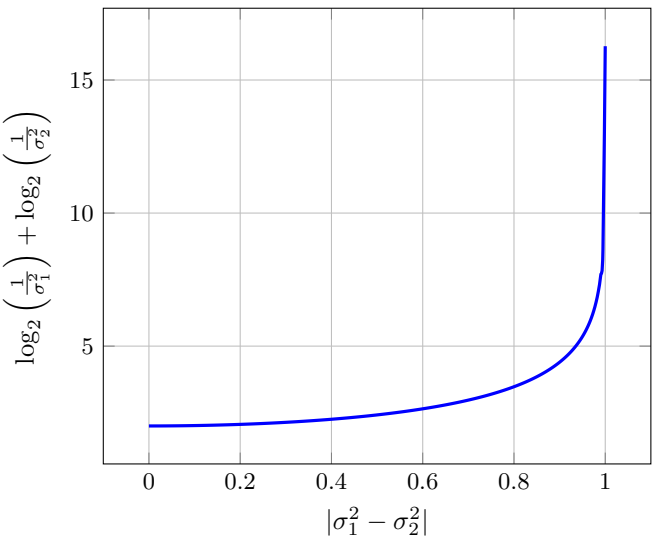


Figure 3.5: *Overall capacity of a 2-coefficients template vs SNR balance*

[1] Note that, in this example, we are not considering the capacity of the system we proposed, but rather the generic capacity of an additive gaussian noise channel.

In order to overcome this limitation, one should avoid as much as possible to combine together coefficients that are statistically different in terms of signal to noise ratio. As an example, in the extreme case in which one of the coefficients is noiseless, the capacity would be infinite. Any mixture between the noiseless coefficient and the others would make it noisy as well. Thus, the rotation matrix A should be designed so that only coefficients with similar SNR are combined. Obviously, this reflects in a trade-off between embedding capacity and unlinkability strength. In fact, in the extreme case, no coefficient is combined with each other and the scheme becomes equivalent to the one proposed in chapter 2. Also if we combine only a small group of coefficients together, the computational cost of finding the solution of the system of equations 3.8 would be computationally easy. The rotation matrix design is described as follow.
The basic idea is to combine each coefficient only with the W most noise-wise similar coefficients. If we sort the coefficients with respect to their SNR, this is equivalent to designing a banded rotation matrix. To construct such a matrix, we can use the following algorithm. We initialize A as a diagonal matrix with elements randomly chosen is $\{-1, +1\}$, i.e. a random reflection matrix. We rotate any couple of coefficients (i, j) such that $|i-j| \leq W$ by a random angle $0 \leq \theta_{ij} < \pi/2$. The order or the rotations is applied with random order. Mathematically, we define the rotation matrix as

$$\begin{aligned} A &= \left[\prod_{(i,j) \in S} G_{ij} \right] R \\ S &: \{(i,\, j) \mid |i-j| < W)\} \end{aligned} \tag{3.16}$$

where A_{ij} is a Givens rotation matrix, that is a rotation on the ij plane:

$$G_{ij} = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & c & \cdots & -s & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & s & \cdots & c & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{bmatrix} \tag{3.17}$$

i.e.

$$\begin{aligned} g_{kk} &= 1 \qquad \text{for } k \neq i,\ j \\ g_{kk} &= c \qquad \text{for } k = i,\ j \\ g_{ij} &= -g_{ji} = s \end{aligned} \tag{3.18}$$

where $c = \cos\theta$ and $s = \sin\theta$ appear at the intersections i_{th} and j_{th} rows and columns. Note that, with this procedure, the matrix A is not banded in the strict sense because the subsequent rotations may mix together also coefficients such that $|i - j| > W$. Anyway, since the weights of the combinations decrease with $|i - j|$, we can say that the matrix is banded in a fuzzy meaning. An example is shown in figure 3.6.

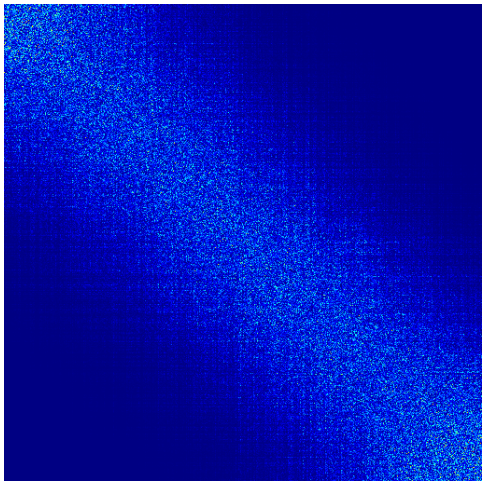


Figure 3.6: *Example of a Banded Rotation Matrix (Absolute Value) - Deep blue = 0 / Light blue = 1*

In order to have an idea on the effect W parameter, let's consider the following example. Let's consider a 512-coefficients whose capacities are shown in figure 3.7.

In figure 3.8 the trend of the total capacity of the vector when changing the W parameter is shown. As one can see, the capacity decreases drastically when W grows, until it reaches a plateau. The plateau is due to the fact that the effective bandwidth of the rotation matrix saturates. The bandwidth is the number of non-zero (or non-negligible) elements per raw of the rotation matrix, i.e. the size of the groups of coefficients that are combined together. This parameter is very important since it drives the complexity of

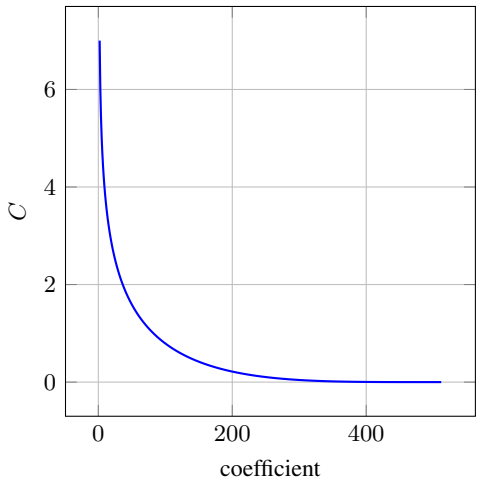


Figure 3.7: *Example of capacity per coefficient distribution.*

solving the linkability attack through the system of equations 3.8.

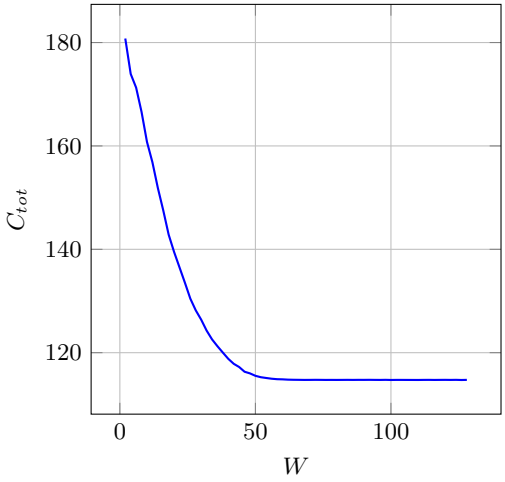


Figure 3.8: *Overall capacity vs W parameter of the banded rotation matrix construction*

3.5 Discussion

In this chapter, we improved the system presented in chapter 2 in order to make it immune to linkability attack. In contrast with other methods proposed in the literature, the unlinkability is achieved with the support of public parameters and no addition secret factor is required in the protocol.

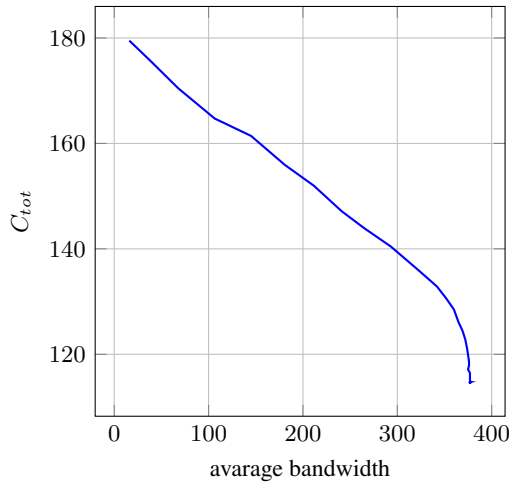


Figure 3.9: *Overall capacity vs the average bandwidth of* $A_2 A_1^T$

Even though the preliminary analysis we carried on suggests the effectiveness of the idea, further investigations are required. In contrast with the irreversibility analysis of chapter 2, here, no strong theoretical demonstration is provided regarding the linkability. The strength versus two different types of attacks has been evaluated. In one case, the unlinkability relies on the (unproven) computational hardness in solving a system of non-linear equations. In the other case, the untraceability is obtained by minimizing the accuracy that an attacker may achieve if he tries to estimate the employed biometrics. In both cases, the unlinkability is not really proven. It may exist an algorithm capable to solve the system of equations of the first attack in polynomial time. It may also exist a metric space for which the leaked information by the helper data are not indistinguishable. In fact, we minimized the estimation accuracy only with respect to the squared error rate, i.e. the Euclidean distance.

Besides the security analysis, following the same idea for the whole thesis, the repercussions on recognition performance are analysed and some design criteria are proposed in order to tune the trade-off between security and privacy. We showed again that using unrealistic models to represent biometrics brings to inaccurate conclusions. Specifically, we showed that the unlinkability building block must be accurately designed by taking into account the uneven distribution of noise among biometric coefficients, otherwise a significant drop of performances occurs.

CHAPTER 4

Fingerprint Minutiae Matching Through Sparse Cross-correlation

In this chapter, we introduce a novel minutiae-based matching algorithm for fingerprint recognition. The method is built on an elegant and straightforward mathematical formulation: the minutiae set is represented by a train of complex pulses and the matching algorithm is based on a simple cross-correlation. We propose two different implementations. The first one exploits the intrinsic sparsity of the signal representing the minutiae set in order to construct an efficient implementation. The other relies on the Fourier transform to build a fixed-length representation, being thus suitable to be used in many biometric crypto-systems. The proposed method exhibits performance comparable with NIST's Bozorth3, that is a standard *de facto* for minutiae matching, but it shows to be more robust with cropped fingerprints.

4.1 Introduction

Fingerprints are the most-used biometric traits thanks to their usability, low-cost, and accuracy. The minutiae-based techniques [Peralta et al., 2015] are nowadays the consolidated matching methods, due to their high performance and low computational memory requirements. Nevertheless, they still show some weaknesses: mainly, the variability of the length of the representation and the drop of recognition rate in the cropped images scenario, due for example to the small size of the acquisition sensors of mobile devices.

The variability of the length of the representation makes the system incompatible with the majority of biometric crypto-system methods [Hine et al., 2017, Nandakumar and Jain, 2015, Gomez-Barrero et al., 2016a]. There is indeed a big effort from the community to find novel fixed-length representations of fingerprints [Xu et al., 2009, Jain et al., 1999]. The problem with these representations is that they incur a significant drop in recognition accuracy. Some attempts to build fixed-length representations directly from minutiae have been proposed, such as the spectral minutia representation [Xu et al., 2009] or minutia cylinder-code (MCC) [Cappelli et al., 2010]. The MCC method is not truly a fixed-length representation since some of its cells may be invalid, and the amount of invalid cells is unpredictable. The Spectral Minutia Representation suffers from poor recognition rates. This is mainly due to their minutiae representation that, with the aim of achieving translation invariance, gets rid of a large amount of useful information. This aspect will be extensively discussed in Section 4.2.1.

Regarding the drop of performance when dealing with partial fingerprint images, usually, additional features are taken from the fingerprint image [Lee et al., 2017, Zanganeh et al., 2014, Nandakumar and Jain, 2004]. These techniques are more computationally expensive because they usually apply cross-correlation or similar operations directly to the fingerprint images. Furthermore, the use of additional features to ISO/IEC 19794 standard minutiae goes against interoperability.

In this work, we take inspiration from the fundamentals at the basis of the spectral minutia representation approach [Xu et al., 2009] to arrange minutiae sets in such a way they can be treated with signal processing techniques. In more details, minutiae are represented by a sparse complex sig-

nal and the matching is based on a simple cross-correlation. Since no hard decision is taken on corresponding minutia couples, the system is more robust to the missing-minutiae scenario. The sparsity of the signal makes the cross-correlation computation very fast. Furthermore, all operations can be implemented also in the frequency domain by means of a fixed-length representation.
In Section 4.2.1, we will give some remarks on the representation proposed in [Xu et al., 2009] and discuss its limitation. In Section 4.2.2 we will show how to exploit the sparsity of the minutiae signal representation to design a very elegant, accurate and fast matching algorithm based on spatial-domain analytical cross-correlation. In Section 4.2.3, a spectral representation of the same algorithm will be shown. Eventually, experimental results will be shown in Section 4.3.

4.2 Complex Domain Minutia Representation

Let $M = m_i : \{x_i, y_i, \alpha_i | i = 1, ..., N\}$ be an unordered set of minutiae where x and y are the Cartesian coordinates and α is the orientation of the minutia. As suggested in [Xu and Veldhuis, 2010b, Xu and Veldhuis, 2010a, Xu et al., 2009], each minutia m_i can be represented as an isotropic Gaussian function centred in (x_i, y_i) whose amplitude is modulated by $e^{\iota\alpha}$. Therefore, a minutiae set can be represented as a mixture of Gaussian functions:

$$\begin{aligned} m(x,y) &= \sum_{i=1}^{N} e^{\iota\alpha_i} \frac{1}{2\pi\sigma^2} e^{\frac{-\left[(x-x_i)^2+(y-y_i)^2\right]}{2\sigma^2}} = \\ &= \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} * \sum_{i=1}^{N} e^{\iota\alpha_i} \delta(x-x_i, y-y_i), \end{aligned} \tag{4.1}$$

where $\delta(\cdot\,,\cdot)$ represents the Dirac distribution and $*$ the convolution operator. The σ parameter is meant to absorb the variability of the relative location of minutiae due to potential fingerprint distortion. This formulation has been shown to be very useful to generate a fixed-length representation in the spectral domain [Xu et al., 2009, Xu and Veldhuis, 2010b, Xu and Veldhuis, 2010a].

4.2.1 Some Remarks on the Spectral Minutiae Representation

In [Xu and Veldhuis, 2010b, Xu and Veldhuis, 2010a, Xu et al., 2009], the authors use as a template the absolute value of spectral representation of the minutiae set $|\mathcal{M}(\omega_x, \omega_y)|$, discarding the phase information, thus making the template invariant to spatial translation.

$$\begin{aligned}\mathcal{M}(\omega_x, \omega_y) &= \int\int m(x,y) e^{-\iota(\omega_x x + \omega_y y)} dxdy = \\ &= e^{-(\omega_x^2+\omega_y^2)\frac{\sigma^2}{2}} \sum_{i=1}^{N} e^{-\iota(\omega_x x_i + \omega_y y_i)} e^{-\iota\alpha_i}\end{aligned} \tag{4.2}$$

However, it is well known that the phase removal induces significant loss of information that is useful for the recognition process. As an example, in Figure 4.1 the original representation $m(x, y)$ and the one reconstructed when discarding the magnitude of the spectral representation (4.3) are shown.

$$\mathcal{F}^{-1}\left\{ e^{-(\omega_x^2+\omega_y^2)\frac{\sigma^2}{2}} \frac{\mathcal{M}(\omega_x, \omega_y)}{|\mathcal{M}(\omega_x, \omega_y)|} \right\} \tag{4.3}$$

By looking the figure, it is clear that the phase data alone contain almost all the information.
Furthermore, let's take into account two minutiae sets $m^{(a)}$ and $m^{(b)}$. Let's suppose

$$x_i^{(a)} = x_i^{(b)},\ y_i^{(a)} = y_i^{(b)},\ \alpha_i^{(a)} = \alpha_i^{(b)} + \pi\ \ \forall i \tag{4.4}$$

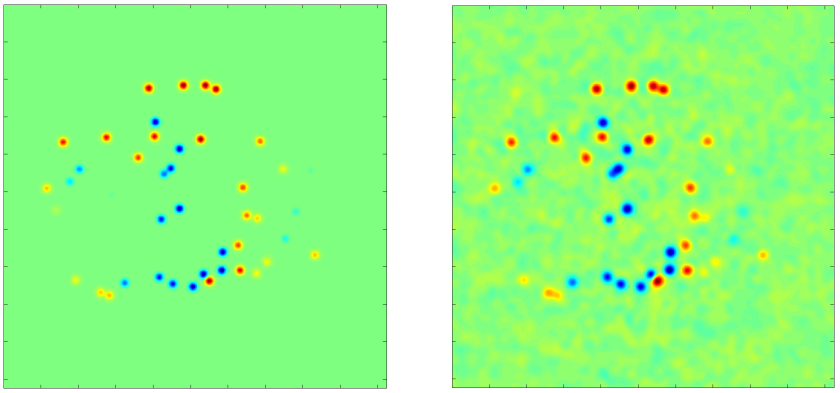
i.e. the locations of the minutiae are all the same while the orientations differ by π. Even if any minutiae matcher would mismatch this these two sets, according to [Xu and Veldhuis, 2010b], they would have the same template. It is well known in fact that:

$$|\mathcal{M}(\omega_x, \omega_y)|^2 = \mathcal{F}\{m(x,y) \otimes m(x,y)\} \tag{4.5}$$

being $\otimes$ the cross-correlation operator. Since the cross-correlation depends only on the relative phase difference between signals, it is clear that both $m^{(a)}$ and $m^{(b)}$ have equal autocorrelation.

4.2.2 Sparse Cross-correlation in the Continuous Spatial Domain

In this section we show how to use the complex minutiae representation (4.1) to design a matcher working directly in the spatial domain. Given a



(a) *Original Signal*

(b) *Reconstruction with phase only spectrum information*

Figure 4.1: *Real part of the Minutiae complex representation* $\mathcal{R}e\{m(x,y)\}$

pair of minutiae sets $m^{(a)}$ and $m^{(b)}$, their cross-correlation is defined as:

$$\begin{aligned} C^{(a,b)}(x,y) &= m^{(a)}(x,y) \otimes m^{(b)}(x,y) = \\ &= G(x,y) * \Delta^{a,b}(x,y) \end{aligned} \tag{4.6}$$

where

$$G(x,y) = \frac{1}{2\pi 2\sigma^2} e^{\frac{-(x^2+y^2)}{4\sigma^2}} \tag{4.7}$$

and

$$\Delta^{a,b}(x,y) = \sum_{i=1}^{N^a} \sum_{j=1}^{N^b} e^{\iota\left(\alpha_i^{(a)} - \alpha_j^{(b)}\right)} \delta\left[x - \left(x_i^{(a)} - x_j^{(b)}\right), y - \left(y_i^{(a)} - y_j^{(b)}\right)\right] \tag{4.8}$$

Actually, ridge endings and bifurcations need to be treated separately. Therefore, we divide the minutiae set into disjoint subsets M_{end} and M_{bif}, compute the cross-correlation between homologous sets and sum them:

$$C_{tot}^{(a,b)}(x,y) = C_{end}^{(a,b)}(x,y) + C_{bif}^{(a,b)}(x,y). \tag{4.9}$$

The similarity score is given by the maximum value of the real part of the suitably normalised cross-correlation:

$$S\left(m^{(a)}, m^{(b)}\right) = \frac{8\pi\sigma^2}{N_a + N_b} \max_{x,y} \left(\mathcal{R}e \left\{ C_{tot}^{(a,b)}(x,y) \right\} \right) \tag{4.10}$$

where $\mathcal{R}e\{\cdot\}$ represents the real value. The normalisation value is chosen so that the matching score between identical minutiae sets is approximately 1 (it is exactly 1 when $\sigma \to 0$). It is worth mentioning that no hard decision is made on the correspondence between a minutia pair, and the strength of each minutia similarity is kept for the final decision. As we will see in Section 4.3, this makes the method robust to missing-minutiae scenario.

The computation of (4.8) is straightforward since we just need to compute all the possible differences between minutiae:

$$\begin{aligned} C^{(a,b)} = \left\{ \left(x_i^{(a)} - x_j^{(b)}, y_i^{(a)} - y_j^{(b)}, \alpha_i^{(a)} - \alpha_j^{(b)} \right) \right\} \\ |i = 1, ...N^a, j = 1, ...N^b \end{aligned} \tag{4.11}$$

It is worth pointing out that this step is identical to what the majority of minutiae-based fingerprint matcher does. We will refer to (4.11) as minutiae set cross-correlation.

On the other hand, the full computation of the evenly sampled version of (4.6) would be quite computationally expensive since the evaluation of each point of the cross-correlation function underlines the computation of $N_{end}^a \cdot N_{end}^b + N_{bif}^a \cdot N_{bif}^b$ steps. Nevertheless, because of the sparsity of $C^{(a,b)}(x,y)$, and since we are interested only in estimating its maximum value, we can evaluate the values of $C^{(a,b)}(x,y)$ just in the set correlation points defined in (4.11), i.e.:

$$\begin{aligned} \widehat{C}^{(a,b)}(x,y) = C_{tot}^{(a,b)}(x,y) \cdot 1_C(x,y) \\ C = C_{end}^{(a,b)} \cup C_{bif}^{(a,b)} \end{aligned} \tag{4.12}$$

where $1_C(x,y)$ is the Indicator function:

$$1_A(x,y) = \begin{cases} 1 & \text{if } (x,y) \in A \\ 0 & \text{otherwise.} \end{cases} \tag{4.13}$$

It is sufficient to calculate the value of the cross-correlation in those points since the sought maximum is located next to highest aggregation of

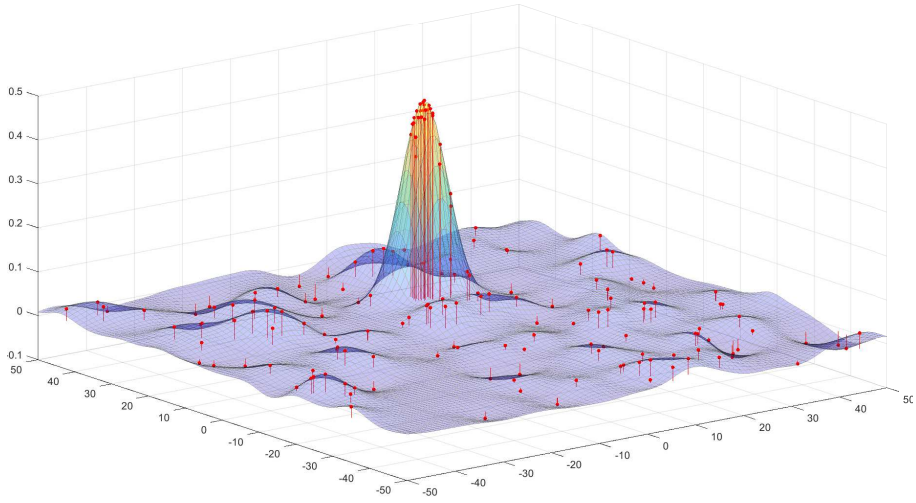


Figure 4.2: *Continuous spatial cross-correlation between complex minutiae $C^{(a,b)}(x,y)$ and sampled version $\widehat{C}^{(a,b)}(x,y)$.*

points from the C set. In other words, the spatial resolution of the sampled cross-correlation $\widehat{C}^{(a,b)}(x,y)$ grows with the value of $C^{(a,b)}(x,y)$. An example of this behaviour can be seen in Figure 4.2. The number of steps to compute $\widehat{C}^{(a,b)}(x,y)$ is thus $\left[N^a_{end} \cdot N^b_{end} + N^a_{bif} \cdot N^b_{bif}\right]^2$. The number of values to compute can be further decreased by discarding the points too far from the origin. In summary, the sparsity of the signal representing the minutiae set (4.1) makes the complexity of the algorithm be $O\left(N^4\right)$ and independent to the resolution of x and y axis. Note that the computational complexity is the same of NIST's Bozorth3 [Watson et al.,].
The described algorithm does not take into account rotations of the minutiae sets. It is then required to explicitly apply a set of rotations to one of the minutiae sets and find the optimal one.

$$\begin{pmatrix} x_j^{(b)} \\ y_j^{(b)} \end{pmatrix} \leftarrow \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} x_j^{(b)} \\ y_j^{(b)} \end{pmatrix} \qquad (4.14)$$
$$\alpha_j^{(b)} \leftarrow \alpha_j^{(b)} - \phi$$

The maximization algorithm we used is based on golden section search

and parabolic interpolation [Brent, 1973].

4.2.3 Frequency Fixed-Length Implementation

All the steps described in the previous section can be also implemented in frequency domain $\mathcal{M}(\omega_x, \omega_y) = \mathcal{F}\{m(x, y)\}$ where cross-correlation is given by:

$$\mathcal{C}^{a,b}(\omega_x, \omega_y) = \mathcal{M}^a(\omega_x, \omega_y)\mathcal{M}^b(\omega_x, \omega_y)^\star. \tag{4.15}$$

As we did before for the spatial implementation, we separate cross-correlation between homologous minutiae, i.e. ridge endings and bifurcation:

$$\mathcal{C}^{a,b}_{tot}(\omega_x, \omega_y) = \mathcal{C}^{a,b}_{end}(\omega_x, \omega_y) + \mathcal{C}^{a,b}_{bif}(\omega_x, \omega_y). \tag{4.16}$$

In order to find the matching score we should sample $\mathcal{C}^{a,b}_{tot}$, compute the Discrete Fourier Transform (DFT) and take the maximum value.

$$S\left(m^{(a)}, m^{(b)}\right) = \frac{2\,max\left(\mathcal{R}\left\{IFFT2\left[\mathcal{C}^{a,b}_{tot}[n, m]\right]\right\}\right)}{|<\mathcal{M}^a[n, m]>|^2 + |<\mathcal{M}^b[n, m]>|^2} \tag{4.17}$$

Since multiplications in the DFT domain correspond to a circular convolution in the spatial domain, in order to avoid aliasing effects, the sample rate in the frequency domain in ω_x (ω_y) direction should be chosen to be greater or equal to $2\frac{2\pi}{L}$, where L is the number of pixels in the x (y) direction. The maximum frequency to sample depends on the chosen σ value since it depends on which values (ω_x, ω_y) make $e^{-(\omega_x^2+\omega_y^2)\frac{\sigma^2}{2}}$ go close to zero. However, this implementation does not exploit the sparsity of the original signal in the spatial domain, since each minutia pulse is spread on the whole frequency domain, thus increasing the computational complexity. For this reason, various samples reduction techniques have been proposed [Xu and Veldhuis, 2010b]. Nevertheless, in this work, we have not dealt with this issue. Even though the spatial implementation is more computationally efficient, the frequency implementation exploits a fixed-length representation, that is a mandatory property for many biometric cryptosystems methods [Hine et al., 2017, Gomez-Barrero et al., 2016a].

4.3 Implementation and Experimental Analysis

The proposed algorithms have been evaluated on the MCYT [Ortega-Garcia et al., 2003] database. Only fingers acquired with optical devices have been taken into account. We have used both left- and right-hand index and middle fingers from 100 users (0000 to 0099 IDs). Each finger has 12 realizations, 6 of which have been used for enrolment, 6 for verification. During the tests, only homologous fingers have been compared each other. Minutiae have been extracted through NIST's MINDTCT [Watson et al.,].

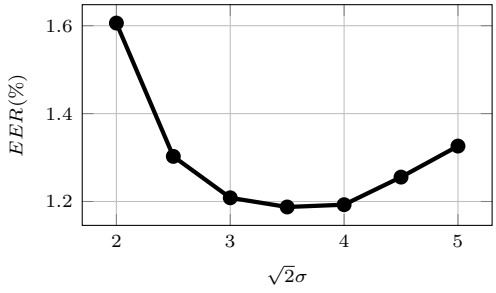


Figure 4.3: EER *vs* σ

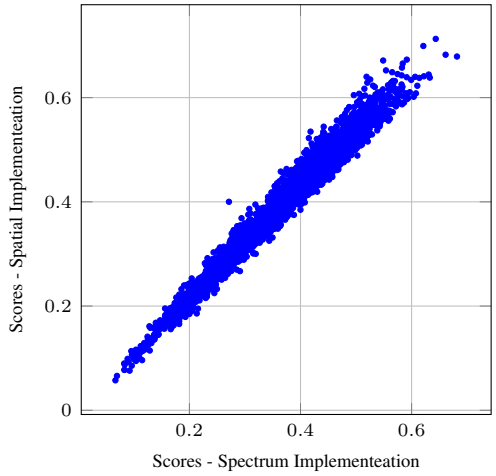


Figure 4.4: *Scatter plot of the scores computed through spatial and spectral implementations*

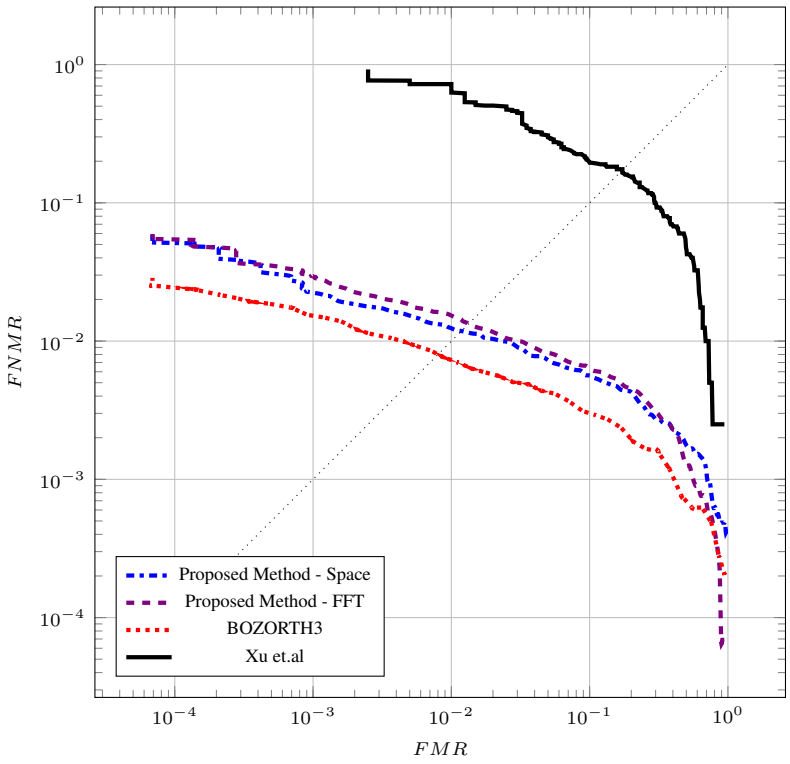


Figure 4.5: *ROC Curve*

A remarkable characteristic of our method is that it has very few parameters to be defined: the σ parameter, the research window of optimal rotation, and the maximum number of rotations to try. The research window has been set to $\left(-\frac{\pi}{12}, \frac{\pi}{12}\right)$ while the maximum number of rotations has been set to 10 for computational reasons. Regarding σ, in Figure 4.3 the equal error rate (EER) for different values of σ is shown. Since $\sigma = \frac{3.5}{\sqrt{2}}$ shows the best performances, the following tests use this parameter.
In Figure 4.5, the ROC curves of both implementations of our method, the spectral minutiae method [Xu and Veldhuis, 2010b] and NIST's BOZORTH3 [Watson et al.,] are compared. While [Xu and Veldhuis, 2010b] method performance are very low for reasons explained in Section 4.2.1, our method's performance are slightly below NIST's ones. Both our implementations show roughly the same performance. That is because they basically compute the same scores with different procedures. For this rea-

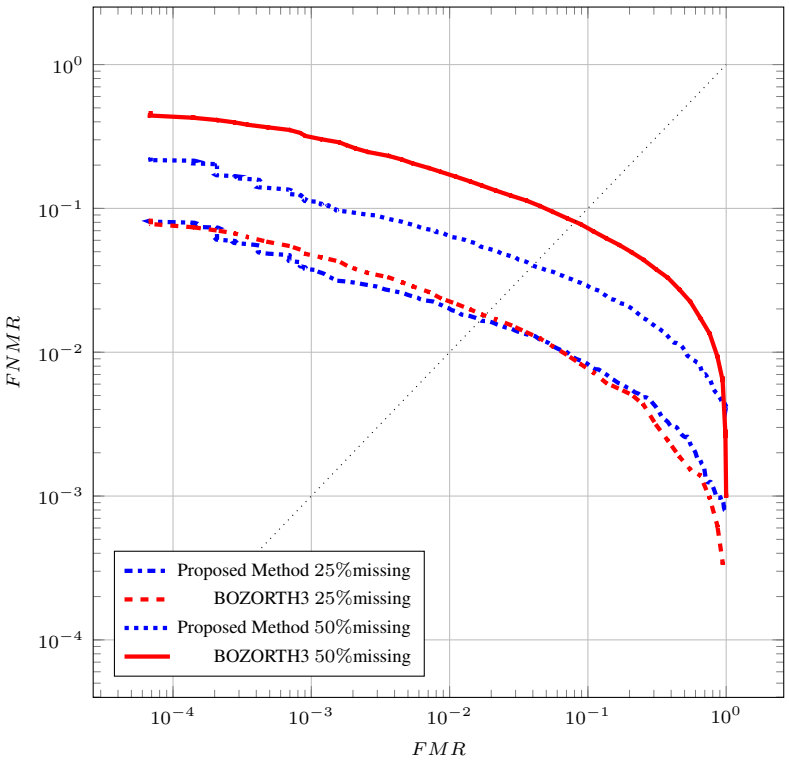


Figure 4.6: *ROC Curve in the case of missing-minutiae*

son, in the following tests, only the spatial implementation will be evaluated since it is the fastest. In Figure 4.4, the scatter plot of the scores obtained from the comparison of corresponding minutiae is shown. We can notice that, even though the scores are well correlated, the spatial domain implementation gives slightly higher scores. That is probably because the spatial domain implementation is more accurate in estimating the maximum cross-correlation value (4.10) due to the sampling effects in the FFT implementation.

Our approach has shown to be particularly robust when some minutiae are missing, such as in the case of small size acquisition device. We have simulated the aforementioned scenario by cropping the fingerprint images so that the minutiae are discarded. We took into account two different cases: $p = 25\%$ and $p = 50\%$ missing-minutiae. In order to remove $p\%$ of the minutiae, we randomly discarded minutiae falling below percentile p of x

or y position, or above $(100 - p)\%$. We considered the scenario in which only the genuine probes have cropped images, while the enrolled fingers and the attacker probes have not been cropped. As a matter of fact, in a realistic scenario, both enrolment and attack processes are more accurate than everyday genuine users' identification attempts. As it can be seen in Figure 4.6, in the 25% missing-minutiae scenario, our method and the NIST's one show roughly the same performance, while our approach works remarkably better than Bozorth3 in the 50% missing-minutiae scenario. The robustness of our method is probably due to the fact that, contrary to Bozorth3, no hard decision is taken on the correspondence between single minutiae pairs. Therefore, even if few minutiae are available, if they are strongly similar to a subset of the reference fingerprint, the matching decision is correctly taken.

4.4 Discussion

In this chapter, we have introduced a novel minutiae-based matching algorithm for fingerprint recognition built on an elegant and straightforward mathematical formulation. The method has shown to be more robust with cropped fingerprints compared with NIST's Bozorth3 method. We proposed two different implementations. The first one is very computationally efficient while the second one makes use of a fixed length representation. We think that the simple mathematical closed form of the algorithm can be a solid starting point to develop further methods. For example, the spatial implementation may be integrated with fuzzy vault techniques, while the frequency implementation with fixed-length helper data schemes. The current drawback of our frequency representation is that it is not invariant to spatial translations and rotations that let the arrangement of a helper data scheme to be not straightforward. Based on the idea presented in this Chapter, next Chapter shows a representation invariant to translation.

CHAPTER 5

Minutiae Triple Correlation: a Translation Invariant Fingerprint Representation

In this chapter, we introduce a novel translation-invariant minutiae representation through triple correlation. In contrast with other translation-invariant representations, triple correlation does not loose any information of the original signal, with exemption of the absolute position. Nevertheless, it is very little use in signal processing applications because of its memory complexity. By exploiting the intrinsic sparsity of the minutiae, we propose a sparse implementation of the triple correlation. Furthermore, we propose a matching algorithm suitable for the representation.

5.1 Introduction

As already pointed out in Section 1.4.1, translation-invariant representations in biometrics are an open issue. One of the major applications that is demanding this propriety can be found in biometric cryptosystems [Sood and Kaur, 2014]. Synchronization (or registration) of the input signals

is a mandatory preprocessing stage for most of the cryptosystems since they mainly work with point-wise functions such as set intersection, dot-product, hamming distance, etc. [Hine et al., 2017]. Other applications in which translation-invariant representation would be very useful are the all-vs-all matching as in the case of data deduplication [Rathgeb et al., 2018] in big biometric databases. In such cases, classical representations of minutiae make the system too slow because of the "shift and try" process [Barman et al., 2014]. In addiction, many translation-invariant minutiae representations proposed in literature loose information. For example, in [Xu et al., 2009], the authors propose to use the absolute value of a spectral representation of the minutiae as feature vector. As it has been shown in [Hine et al., 2018], the phase information removal degrades the performances drastically.

In this chapter, we propose a novel translation-invariant minutiae representation that do not loose any information but the absolute position of the minutiae. The relative positions and angles are preserved together with quality data.

The Chapter is organised as follow. In Section 5.2, minutiae representation through complex pulses is presented. A rough introduction of the triple correlation is given in Section 5.3.1 in order to introduce the proposed minutiae representation in Section 5.3.2 and the related matching algorithm in Section 5.3.3. An example of implementation to real data is given in Section 5.4.

5.2 Minutiae Representation Through Complex Pulses

As shown in [Xu et al., 2009], and as already presented in Chapter 4, a minutiae set $M = \{(x_k,\, y_k,\, \alpha_k, q_k) \,|\, k \in [1,\, N]\}$, namely x- and y-coordinates, orientation and quality, can be represented formally as a train of Dirac-delta distributions $\delta(\cdot)$:

$$m(x, y) = \sum_k a_k \, \delta(x - x_k,\, y - y_k) \tag{5.1}$$

with $a_k = f(q_k)\, e^{i\alpha_k}$, and $f(q_k)$ a non-decreasing function of the quality q_k. To simplify the mathematical formulation, in the following we will use the complex domain $\underline{z} = x + \imath y$ (and use the same convention for any other

underlined symbol):

$$m(\underline{z}) = \sum_k a_k \, \delta(\underline{z} - \underline{z}_k). \tag{5.2}$$

The interesting fact of this representation is that it maps the minutiae in a closed-form signal, that let us use conventional signal processing techniques. For example, in [Xu et al., 2009] the authors exploit this representation to define a fixed-length translation-invariant representation of the minutiae by means of the absolute value of the Fourier-transform of the signal defined above (5.1): $|\mathcal{M}(\omega_x, \omega_y)| = |\mathcal{F}\{m(x, y)\}|$ [1]. As it has been shown in [Hine et al., 2018], removing the spectral-phase information reduces the performance significantly since most of the information is contained in the phase itself.[2] Our goal in this chapter is to propose a minutiae set representation that it independent from absolute position but that does not loose any other information. To this end, we exploited the triple correlation, that is described in the next section.

5.3 Triple Correlation Minutiae Representation

In this section, we introduce the proposed triple-correlation representation of minutiae. After giving the mathematical definition of triple correlation, we introduce the representation and show the main properties that are useful to define the matching algorithm.

5.3.1 Triple Correlation Overview

The triple correlation of a signal $f(\underline{z})$ is defined as:

$$F(\underline{s}_1, \, \underline{s}_2) = \int_{-\infty}^{\infty} f^{\star}(\underline{z}) f(\underline{z} + \underline{s}_1) f(\underline{z} + \underline{s}_2) d\underline{z}. \tag{5.3}$$

It is straightforward to verify that $F(\underline{s}_1, \underline{s}_2)$ is invariant to a translation $x \leftarrow (\underline{z} - \underline{z}_0)$. The most interesting property is that every image $f(\underline{z})$ of finite size is uniquely determined up to translation by its triple correlation [Yellott and Iverson, 1992, Bartelt et al., 1984]. In other words, the triple correlation is a representation (in strict sense) of the signal $f(\underline{z} - \underline{z}_0)$,

[1] see more details in Section 4.2.3

[2] Note that this is equivalent to considering the auto-correlation of the signal since $|\mathcal{M}(\underline{\omega})|^2 = \mathcal{F}\{\int_{-\infty}^{\infty} f^*(\underline{z}) f(\underline{z} + \underline{s}) d\underline{z}\}$

except for the position $\underline{z}_0$. That means that $F(\underline{s}_1, \underline{s}_2)$ contains all the information to reconstruct the shape of the original signal. Nevertheless, triple correlation is very little-used in signal processing because of its computational complexity. To make an example, the triple correlation of a 256x256 image is made of 256^4 coefficients. If each coefficient is represented through a double precision format, that would be more than 34GB. Luckily, since the signal representing the minutiae set is sparse, the triple correlation function will be sparse as well. The sparse triple correlation is described in next section.

Triple correlation convolution theorem

Theorem 1. *Given*

$$g(\underline{z}) = f(\underline{z}) \star h(\underline{z}) = \int f(\underline{\zeta}) h(\underline{\zeta} - \underline{z}) d\underline{\zeta}, \tag{5.4}$$

its triple correlation $G(\underline{s}_1, \underline{s}_2)$ is given by:

$$\begin{aligned} G(\underline{s}_1, \underline{s}_2) = F(\underline{s}_1, \underline{s}_2) \star H(\underline{s}_1, \underline{s}_2) = \\ = \iint F(\underline{\zeta}_1, \underline{\zeta}_2)\, H(\underline{s}_1 - \underline{\zeta}_1, \underline{s}_2 - \underline{\zeta}_2)\, d\underline{\zeta}_1\, d\underline{\zeta}_2 \end{aligned} \tag{5.5}$$

Proof. Given

$$g(\underline{z}) = f(\underline{z}) \star h(\underline{z}) = \int f(\underline{\zeta}) h(\underline{\zeta} - \underline{z}) d\underline{\zeta}, \tag{5.6}$$

its triple correlation is given by:

$$\begin{aligned} G(\underline{s}_1, \underline{s}_2) = \int g^\star(\underline{z}) g(\underline{z} + \underline{s}_1) g(\underline{z} + \underline{s}_2) d\underline{z} = \\ = \int \left(\int f^\star(\underline{z}_1) h^\star(\underline{z}_1 - \underline{z}) d\underline{z}_1 \int f(\underline{z}_2) h(\underline{z}_2 - \underline{z} - \underline{s}_1) d\underline{z}_2 \right. \\ \left. \int f(\underline{z}_3) h(\underline{z}_3 - \underline{z} - \underline{s}_2) d\underline{z}_3 \right) d\underline{z} = \\ = \iiiint f^\star(\underline{z}_1) f(\underline{z}_2) f(\underline{z}_3) \\ h^\star(\underline{z}_1 - \underline{z})\, h(\underline{z}_2 - \underline{z} - \underline{s}_1)\, h(\underline{z}_3 - \underline{z} - \underline{s}_2)\, d\underline{z}\, d\underline{z}_1\, d\underline{z}_2\, d\underline{z}_3 \end{aligned} \tag{5.7}$$

Applying the following variables substitution (with unitary Jacobian)

$$\begin{cases} \underline{\zeta}_1 = \underline{z}_2 - \underline{z}_1 \\ \underline{\zeta}_2 = \underline{z}_3 - \underline{z}_1 \\ \underline{w} = \underline{z}_1 - \underline{z} \\ \underline{z} = \underline{z}_1 \end{cases} \tag{5.8}$$

we have:

$$\begin{aligned} &\iiiint f^\star(\underline{z}) f(\underline{z} + \underline{\zeta}_1) f(\underline{z}_1 + \underline{\zeta}_2) \\ &\quad h^\star(w)\, h(w + \underline{\zeta}_1 - \underline{s}_1)\, h(w + \underline{\zeta}_2 - \underline{s}_2)\, d\underline{w}\, d\underline{z}\, d\underline{\zeta}_1\, d\underline{\zeta}_2 = \\ &= \iint \left[\int f^\star(\underline{z}) f(z + \underline{\zeta}_1) f(z + \underline{\zeta}_2) d\underline{z} \right] \\ &\quad \left[\int h^\star(\underline{w})\, h(\underline{w} + \underline{\zeta}_1 - \underline{s}_1)\, h(\underline{w} + \underline{\zeta}_2 - \underline{s}_2)\, d\underline{w} \right] d\underline{\zeta}_1\, d\underline{\zeta}_2 = \\ &\quad = \iint F(\underline{\zeta}_1,\, \underline{\zeta}_2)\, H(\underline{\zeta}_1 - \underline{s}_1,\, \underline{\zeta}_2 - \underline{s}_2)\, d\underline{\zeta}_1\, d\underline{\zeta}_2 = \\ &\quad = \iint F(\underline{\zeta}_1,\, \underline{\zeta}_2)\, H(\underline{s}_1 - \underline{\zeta}_1,\, \underline{s}_2 - \underline{\zeta}_2)\, d\underline{\zeta}_1\, d\underline{\zeta}_2 = \\ &\quad = F(\underline{s}_1,\, \underline{s}_2) \star H(\underline{s}_1,\, \underline{s}_2) \end{aligned} \tag{5.9}$$

where the last step is due to triple correlation symmetry properties. *Q.E.D.*

5.3.2 Minutiae Triple Correlation

Let us consider sparse signal in the two-dimensional spatial domain as a train of δ-Dirac pulses in the complex domain $m(\underline{z}) = \sum_i a_i\, \delta(\underline{z} - \underline{z}_i)$ as in (5.2). Its triple correlation (5.3) can be written as:

$$M(\underline{s}_1, \underline{s}_2) = \sum_{i,\,j,\,k} a_i^\star a_j a_k\, \delta\left[\underline{s}_1 - \underline{\Delta}^{i,\,j},\, \underline{s}_2 - \underline{\Delta}^{i,\,k}\right] \tag{5.10}$$

where $\underline{s}_1 := (s_1^x + \iota s_1^y)$, $\underline{s}_2 := (s_2^x + \iota s_2^y)$, and $\underline{\Delta}^{i,\,j} := [(x_i - x_j) + \iota(y_i - y_j)]$.

Proof.

$$
\begin{aligned}
M(\underline{s}_1,\, \underline{s}_2) = \int m^\star(\underline{z})\, m(\underline{z}+\underline{s}_1)\, m(\underline{z}+\underline{s}_2) d\underline{z} = \\
= \int \sum_i a_i^\star\, \delta(\underline{z}-\underline{z}_i) \sum_j a_j\, \delta(\underline{z}+\underline{s}_1-\underline{z}_j) \\
\sum_k a_k\, \delta(\underline{z}+\underline{s}_2-\underline{z}_k)\, d\underline{z} = \\
= \int \sum_{i,\,j,\,k} a_i^\star a_j a_k\, \delta(\underline{z}-\underline{z}_i)\, \delta(\underline{z}+\underline{s}_1-\underline{z}_j)\, \delta(\underline{z}+\underline{s}_2-\underline{z}_k)\, d\underline{z} = \\
= \sum_{i,\,j,\,k} \left[a_i^\star a_j a_k \int \delta(\underline{z}-\underline{z}_i) \delta(\underline{z}+\underline{s}_1-\underline{z}_j)\ \delta(\underline{z}+\underline{s}_2-\underline{z}_k)\, d\underline{z} \right].
\end{aligned}
\tag{5.11}
$$

The integral in the last statement gives a contribution only when the three Dirac distributions have the same argument, that is:

$$
\begin{cases}
\underline{s}_1 = \underline{z}_j - \underline{z}_i \\
\underline{s}_2 = \underline{z}_k - \underline{z}_i
\end{cases}
\tag{5.12}
$$

that let to:

$$
M(\underline{s}_1,\, \underline{s}_2) = \sum_{i,\,j,\,k} a_i^\star a_j a_k\, \delta(\underline{s}_1 - \Delta^{j,\,i})\, \delta(\underline{s}_2 - \Delta^{k,\,i}). \tag{5.13}
$$

Q.E.D.

It is worth noticing that (5.10) has an interesting geometric interpretation. In fact, the function encodes all the possible minutiae triplets (Figure 5.2). As an example, in Figure 5.1, the scatter-plot of the triple correlation of a train of four Dirac distributions is shown. In the example, the four corresponding triplets are repeated in the six bounded areas. The six points on each axis represent the six possible couples of Dirac pulses. The redundancy is due to the symmetry properties of the triple-correlation that can be easily verified. Also the points laying on the axis, representing the pulses couples, can be easily reconstructed from the set of triplets. In summary, in the implementation, we may choose to compute only the values in one of the six domains. Note that also the triplets of the same minutia are included ($i = j = k$). Since these are not interesting for recognition,

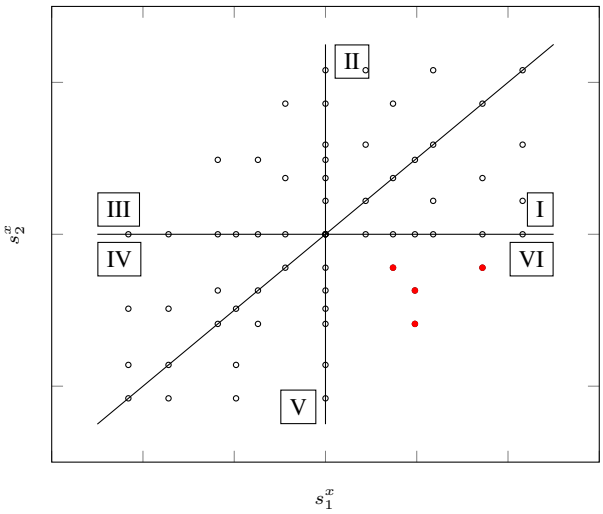


Figure 5.1: *Scatter Plot of the triple correlation of (mono-dimensional) train of 4 Dirac-pulses*

we decided to remove the corresponding pulse from the $(\underline{s}_1,\ \underline{s}_2)$ axis origin ($\Delta^{i,j} = \Delta^{i,k} = 0$). Formally:

$$\begin{aligned}\widetilde{M}(\underline{s}_1, \underline{s}_2) = \sum_{i,\,j,\,k} a_i^\star a_j a_k\, \delta\left[\underline{s}_1 - \underline{\Delta}^{i,j},\ \underline{s}_2 - \underline{\Delta}^{i,k}\right] + \\ -\delta(\underline{s}_1,\ \underline{s}_2) \int_{-\infty}^{\infty} m^\star(\underline{z}) m^2(\underline{z})\, d\underline{z} = \\ = \sum_{i \neq j \neq k} a_i^\star a_j a_k\, \delta\left[\underline{s}_1 - \underline{\Delta}^{i,j},\ \underline{s}_2 - \underline{\Delta}^{i,k}\right]\end{aligned} \tag{5.14}$$

Minutiae triplets have been already proposed in literature [Medina-Pérez et al., 2012], [Jeffers and Arakala, 2006], but their approach is entirely heuristic and the outcome are not strict-sense representations, and perhaps, useful information is wasted.

Unfortunately, the representation is not invariant to a rotation. Conversely, the rotation is coherently applied also to the triple correlation domain. In fact, since a rotation of an angle α of the minutiae set can be formalised as:

$$m^{(\alpha)}(\underline{z}) = e^{\iota\alpha} m(e^{\iota\alpha}\underline{z}), \tag{5.15}$$

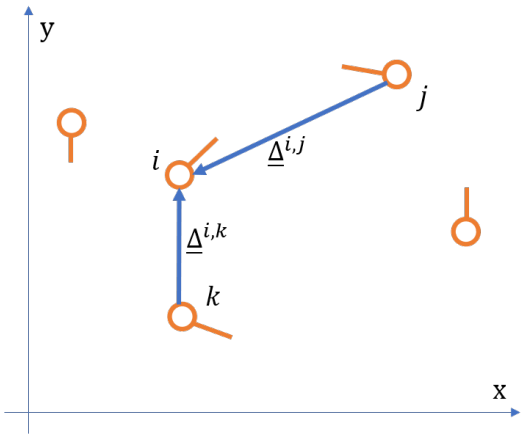


Figure 5.2: *Geometric interpretation of minutiae triple correlation*

we have:

$$M^{(\alpha)}(\underline{s}_1,\, \underline{s}_2) = \int e^{\iota\alpha} f(e^{\iota\alpha}\underline{z}) f(e^{\iota\alpha}(\underline{z}+\underline{s}_1)) f(e^{\iota\alpha}(\underline{z}+\underline{s}_2)) d\underline{z} = \\ e^{\iota\alpha} \int f(\underline{\zeta}) f(\underline{\zeta}+e^{\iota\alpha}\underline{s}_1) f(\underline{\zeta}+e^{\iota\alpha}\underline{s}_2) d\underline{\zeta} = e^{\iota\alpha}\, M(e^{\iota\alpha}\underline{s}_1,\, e^{\iota\alpha}\underline{s}_2) \tag{5.16}$$

5.3.3 Minutiae Triple Correlation Matching

In this Section, we propose a matching method suitable for triple correlation representations. The matching method we propose is based on a nice property of the L2-norm exposed in the following. Let's consider the case the train a of pulses function $m(\underline{z}) = \sum_i a_i\, \delta(\underline{z} - \underline{z}_i)$ as in (5.2). It's straightforward to compute the L2-norm:

$$|< M(\underline{s}_1,\, \underline{s}_2) >|^2 = \iint |M(\underline{s}_1,\, \underline{s}_2)|^2\, d\underline{s}_1 d\underline{s}_2 = \\ = \iint \left| \sum_{i,\,j,\,k} a_i^\star a_j a_k\, \delta\left[\underline{s}_1 - (\underline{\Delta}^{i,j}),\, \underline{s}_2 - (\underline{\Delta}^{i,k})\right] \right|^2 d\underline{s}_1 d\underline{s}_2 \leq \\ \leq \iint \sum_{i,\,j,\,k} |a_i^\star a_j a_k|^2\, \delta\left[\underline{s}_1 - (\underline{\Delta}^{i,j}),\, \underline{s}_2 - (\underline{\Delta}^{i,k})\right] d\underline{s}_1 d\underline{s}_2 = \\ = \sum_{i,\,j,\,k} |a_i a_j a_k|^2 = \left\{ \sum_i |a_i|^2 \right\}^3 = \left\{ \int |m(\underline{z})|^2 d\underline{z} \right\}^3 \tag{5.17}$$

where the inequality sign is due to the possibility that some pulses in the $(\underline{s}_1, \underline{s}_2)$-domain overlap in the same point and they sum with respect to amplitude and phase rather than power. Although, excluding the pulses in the axis origin, it is not very likely that triplets have the same relative positions, except in the case that the train has some periodic structure. For real-word minutiae we can claim that the following inequality is very close to equality:

$$\begin{aligned} \iint \left|\widetilde{M}(\underline{s}_1, \underline{s}_2)\right|^2 d\underline{s}_1 d\underline{s}_2 \lesssim \sum_{i\neq j\neq k} |a_i a_j a_k|^2 = \\ = \left\{\sum_i |a_i|^2\right\}^3 - \sum_i \left(|a_i|^2\right)^3 . \end{aligned} \tag{5.18}$$

As a proof of concept, Figure 5.3 shows the scatter-plot of L2-norm computed directly on the minutiae vs the estimation computed based on the triple correlation.

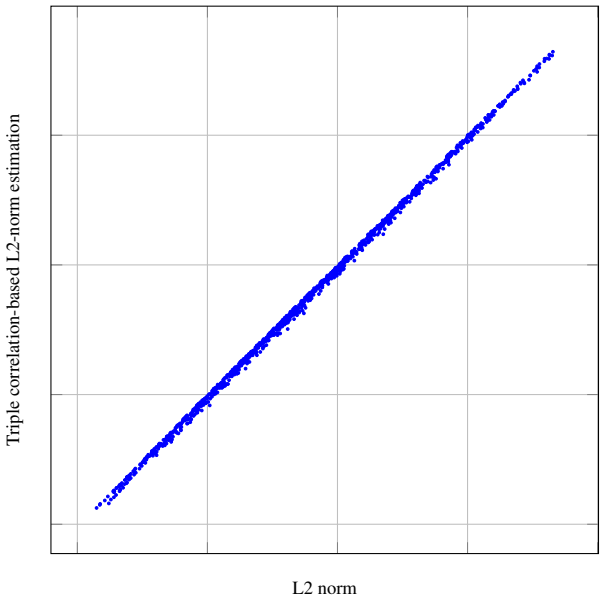


Figure 5.3: *Scatter-plot of L2-norm computer directly on the minutiae vs the estimation computed based on the triple correlation*

In the hypothesis of all unitary qualities q_k, the L2-norm of the train of pulses in (5.1) is equal to the number of minutiae, making it be a very interesting metric space. Therefore, a suitable matching function can be based on the dot-product:

$$\Re e\left\{< A,\, B >\right\}^{\frac{1}{3}} == \Re e\left\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A^{\star}(\underline{s}_1,\, \underline{s}_2)\, B(\underline{s}_1,\, \underline{s}_2)\, d\underline{s}_1 d\underline{s}_2\right\}^{\frac{1}{3}}. \tag{5.19}$$

When $A = B$, the last equation equals the L2-norm. Basically, the matcher counts the number of common triangles between two minutiae set, weighting the entries with respect to quality and the cosine distance. An interesting feature of the proposed score is that, for sparse signals, it can be implemented through a set intersection. This has some stimulating implications that we will discuss later. Actually, as we have already done in the previous Chapter, we split the minutiae with respect to their type (bifurcation/end-point) and sum the scores obtained from each subset. That is, the similarity function is computed as:

$$S\left(A,\, B\right) = \Re e\left\{< A_{\text{bif}},\, B_{\text{bif}} >\right\}^{\frac{1}{3}} + \Re e\left\{< A_{\text{end}},\, B_{\text{end}} >\right\}^{\frac{1}{3}}. \tag{5.20}$$

Obviously, a point wise similarity function, as the one just defined, is not suitable in a real scenario in which non-linear distortion of the minutiae set may occur. For this reason, pulses must be enlarged by means of a kernel in order absorb the variability of the minutia position. As it has been done in [Hine et al., 2018], we choose to use the Gaussian kernel, whose triple correlation has a known closed form. Given $g(\underline{z}) = m(\underline{z}) \star h(\underline{z}) = \sum_i a_i h(\underline{z} - \underline{z}_i)$, thanks to the triple correlation convolution theorem (proved in Appendix 5.3.1), we can write:

$$\begin{aligned} &\widetilde{G}(\underline{s}_1, \underline{s}_2) = \widetilde{M}(\underline{s}_1, \underline{s}_2) \star H(\underline{s}_1, \underline{s}_2) = \\ &= \sum_{i,\,j,\,k} a_i^{\star} a_j a_k\, H\left[\underline{s}_1 - \underline{\Delta}^{i,\,j},\, \underline{s}_2 - \underline{\Delta}^{i,\,k}\right] \end{aligned} \tag{5.21}$$

By choosing a Gaussian kernel $h(\underline{z}) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)$, it is easy to

verify that its triple correlation is:

$$H\left(\underline{s}_1,\, \underline{s}_2\right) = \frac{1}{\left(2\pi\sqrt{3}\sigma^2\right)^2} e^{-\frac{\left(s_1^{x\,2}+s_2^{x\,2}-s_1^x s_2^x\right)+\left(s_1^{y\,2}+s_2^{y\,2}-s_1^y s_2^y\right)}{3\sigma^2}} \tag{5.22}$$

As long as the kernel width is sufficiently narrow, the same claim of L2-norm conservation (5.18) can be stated since the contribution given from interference of the pulses (perhaps destructive) is statistically negligible.

$$\begin{aligned} |<\widetilde{G}(\underline{s}_1,\, \underline{s}_2)>|^2 = \iint \left|\widetilde{G}(\underline{s}_1,\, \underline{s}_2)\right|^2 d\underline{s}_1 d\underline{s}_2 \lesssim \\ \lesssim |<H(\underline{s}_1,\, \underline{s}_2)>|^2 \left\{ \left(\sum_i |a_i|^2\right)^3 - \sum_i \left(|a_i|^2\right)^3 \right\}. \end{aligned} \tag{5.23}$$

5.4 Implementation and Experimental Analysis

The proposed algorithm has been evaluated on the MCYT [Ortega-Garcia et al., 2003] database. Only fingers acquired with optical devices have been taken into account. We have considered right-hand index finger from 100 users (0000 to 0099 IDs). Each finger has 12 realizations, 6 of which have been used for enrolment, 6 for verification. Minutiae have been extracted through NIST's MINDTCT [Watson et al.,].

A remarkable characteristic of our method is that it has very few parameters to be defined: the σ parameter and the function to apply to the quality information $f(q_f)$. The function $f(q_f)$ has been chosen as $f(q_f) = q_k^2$. The only limitation in arbitrarily choosing σ is given by memory complexity. In fact, as σ increases the sparsity of the signal decreases. For the same reason, we had to bound the number of minutiae to consider for each fingerprint, since the complexity of the algorithm goes with 3rd power of the set size. Thus, we have considered only the first best quality-wise 25 minutiae per each type of minutiae (bifurcation/endings).

In Figure 5.4, the number of non-zero coefficients to compute per each kernel as a function of σ is shown, where we are considering only truncated Gaussian kernels. As shown, the number of coefficients to compute

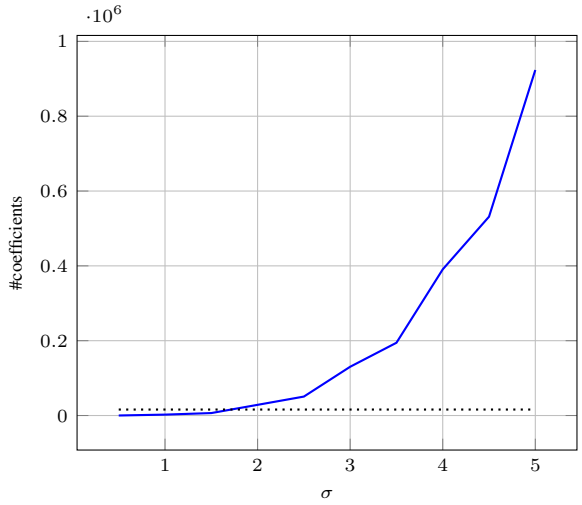


Figure 5.4: *Kernel size vs σ*

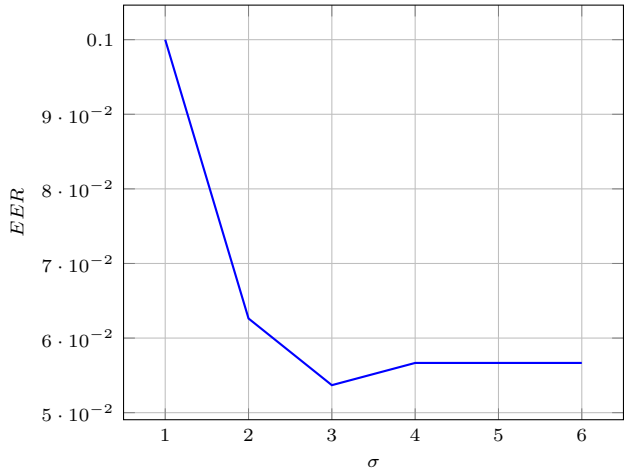


Figure 5.5: *EER vs σ*

grows proportionally to 4-th power of σ and this makes the computation rapidly unsustainable. We decided to up-bound the number of coefficients to $16,000$. In Figure 5.4 the equal error rate (EER) for different values of σ is shown. As shown in Figure 5.5, $\sigma = 3$ gives the best performances and therefore it is used in the following tests. Probably the performances are affected by the fact that we have bounded the number of coefficients representing the pulses. In Figure 5.6, the recognition performance in terms

of false match rate (FMR) and false non-match rate (FNMR) for different valus of threshold are shown, together with a table summarising the main operative points.

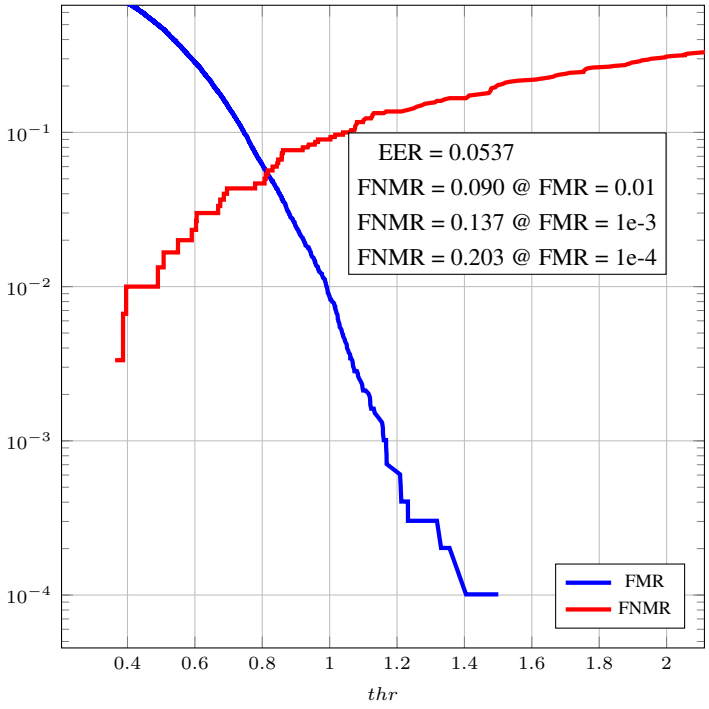


Figure 5.6: *FMR vs FNMR @* $\sigma = 3$

Figure 5.7 shows the performance comparison between the proposed triple correlation method, the cross-correlation method proposed in Chapter 4, and spectral minutiae method [Xu and Veldhuis, 2010b] described in Section 4.2.1. Triple correlation performances are significantly higher than the Xu's method. In fact, as already remarked, our translation-invariant representation does not loose any useful information about the original minutiae. Conversely, since Xu's method gets rid of the spectrum phase information, it does not take into account useful information. Nevertheless, triple correlation performance are lower than the ones achieved using the method proposed in the previous Chapter. It is worth pointing out that this is not due to the representation itself, since, from a signal processing point of view, the triple correlation brings the same information as the original signal. The achieved performances are probably due to the very basic matching algo-

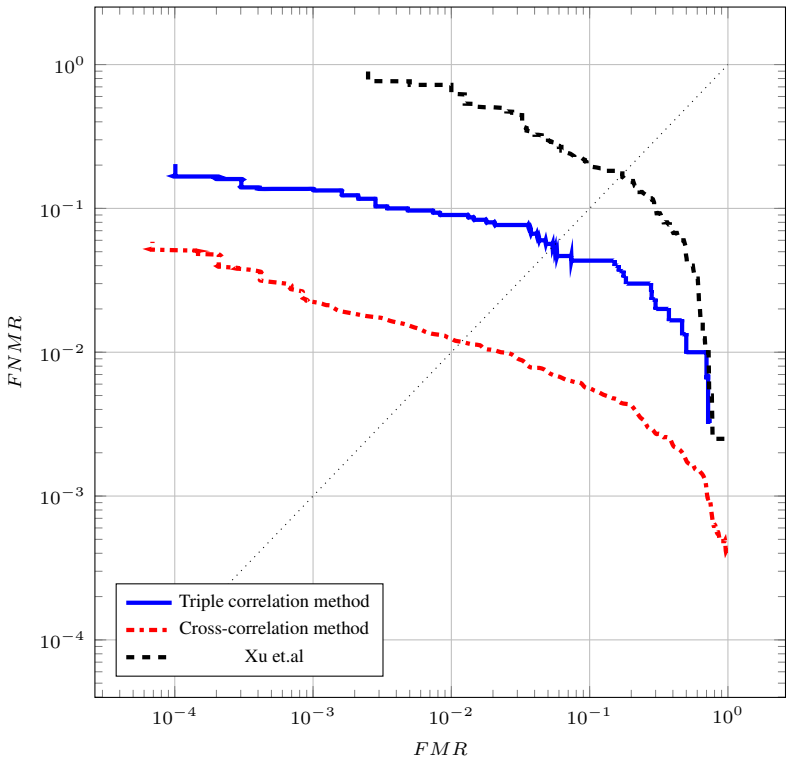


Figure 5.7: *ROC Curve*

rithm. The fact that the triple correlation is a strict-sense representation of the signal ensures that there exists an algorithm capable to achieve the same performance we can accomplish considering raw minutiae.

5.5 Discussion

In this Chapter, we have introduced a novel closed-form translation-invariant representation for fingerprint minutiae. The representation exploits a simple and elegant mathematical formulation. Contrary to other translation-invariant approaches, ours is a representation in strict sense. No information of the original minutiae set are lost, except for the absolute position. This fact suggests that, despite the not excellent performances we have achieved, they are not intrinsic in the representation, but depend on the matching algorithm we choose. Although translation-invariant repre-

sentations of biometric traits are imperative for many applications such as biometric cryptosystems, we have not tried yet to use our representation in such application. A straightforward way would be to apply homomorphic encryption techniques such as Private Set Intersection (PSI) [De Cristofaro and Tsudik, 2010] since the proposed matching method can be implemented through set intersections thanks to the sparsity of the signals representations. Another possibility could be to find fixed-length representation of the proposed triple-correlation signal. In this way we could apply any kind of fixed-length cryptosystem, such as the one presented in Chapter 2. For example, the Fourier-transform of triple correlation leads to the so-called bi-spectrum. The problem with this representation is its unsustainable memory complexity. Nevertheless, thanks to the closed-form representation of the signals, we may be able to compute a down-sampled version or the projection onto a sub-space. For example, several papers [Petropulu and Pozidis, 1998] show that it is possible to compute only some particular slices of the bi-spectrum without affecting too much objects recognition. In general, there are lot of results in literature regarding triple correlation and bi-spectrum, especially in the optics domain. Thereby, our closed form representation opens several research paths that are worth to be followed.

Conclusions

In this thesis, we proposed a novel biometric cryptosystem that achieves the zero-leakage condition. The system has been analysed in a holistic manner, having considered both theoretical and practical aspects. We showed that the zero-leakage condition is not sufficient alone to consider the system privacy compliant and we proposed a novel privacy evaluation parameter. We discussed design aspects that can influence privacy, security, and recognition performance. Unlike the majority of biometric cryptosystems, that are characterized by an intrinsic lack of flexibility from a design point of view, the framework we proposed makes the system quite ductile in the choice of the operating point. A comprehensive implementation has been proposed and tested on real fingerprint data. In this context, we recommended many practical design details in order to maximize performances, such as the use of turbo codes with soft decoding, and the use of adaptive bit allocation. A method to avoid linkability has been proposed and a preliminary analysis of its effectiveness has been discussed. In contrast with many methods proposed in the literature, our method does not imply the use of any secret key. Eventually, a translation-invariant representation of fingerprint minutiae has been proposed. Contrary to similar representations proposed in literature, no information of the original minutiae set are lost, with the obvious exception of the absolute position. This fact makes us quite confident on the possibility to achieve state of the art performances, even if the proposed matching algorithm is not that exciting.

Admitting that further investigations are needed, the author thinks that the methods proposed in this thesis are promising starting points to finally achieve a biometric system that satisfies the requirements that the scientific community and the market are asking for.

APPENDIX A: Information Theory Elements

In this appendix, some fundamental notions from the information theory are introduced, such as entropy and channel capacity notions that are frequently used along the thesis.

A1 Entropy

Let be X a discrete random variable with probability function $P(X = x_i) = P_i$. How much information does the occur of the event $X = x_i$ bring? Intuitively, an information measure should verify at least the following conditions:

- the less the event is expected (probable) the greater is the amount of information associated with an event. Under this perspective the amount of information measures the uncertainty of an event;
- the amount of information linked to a couple of mutually independent events is the sum of the amounts linked to the single events.

Starting from these two conditions, Shannon, in his most famous work "Mathematical Theory of Communication", defined the amount of information associated with an event x_i as:

$$I(x_i) = log\frac{1}{P_i} = -\log P_i \tag{5.24}$$

Consequently, the uncertainty of random variable is defined as the expected value of the information associated with the event:

$$H(X) = E_X\{I(x_i)\} = -\sum_i P_i \log P_i \tag{5.25}$$

Such a quantity is known as entropy. Here we list some of its most interesting properties:

- $H(X) = 0$ if and only if $P_j = 0 \forall j \neq i$ and $P_i = 1$. That is if and only if the event $X = x_i$ is certain. In fact, its occurrence does not bring any information;
- given N the number of possible events, the entropy is maximized in the case of equally probable events and equal to $\log N$;
- the joint entropy of two variables X and Y is less or equal to the sum of their entropies: $H(X,Y) \leq H(X)+H(Y)$, with equality sign only in the case of independent variables;
- the uncertainty of a random variable Y cannot rise with the knowledge of another variable X: $H(Y|X) \leq H(Y)$. $H(Y|X)$ is known as equivocation of Y given X.

A2 Mutual Information and Channel Capacity

n this section, we focus on giving a measurement of the amount of information that is possible to transmit through a channel. Even if the concept of channel comes from the communication theory, we can imagine a channel any time there is a probabilistic relation between two random variables. Such relations are usually made up of a deterministic and random component describing the communication noise. Formally, and considering for the moment just the discrete case, a communication channel can be described with a set of input and output symbols $\{x_i\}$, $\{y_j\}$ and the conditional probabilities $\{P_{Y|X}(y_j, x_i)\}$. We want to know how much information we can gain about X when observing Y. Such measure is given by the Mutual Information $I(X,Y)$, defined as:

$$I(X,Y) = \sum_{i,j} P_{X,Y}(x_i, y_j) \log \left[\frac{P_{X|Y}(x_i|y_j)}{P_X(x_i)} \right]. \tag{5.26}$$

It is straightforward to demonstrate that we can write:

$$I(X,Y) = H(X) - H(X|Y). \tag{5.27}$$

This relation is explanatory. In the extreme case that the relation between X and Y is completely random, i.e. they are mutually independent, then $H(X|Y) = H(X)$ and $I(X,Y) = 0$. On the opposite case, in which the relation between X and Y is fully deterministic, then $H(X|Y) = 0$ and the mutual information is maximum and equal to $I(X,Y) = H(X)$. It is also easy to demonstrate that the mutual information is symmetric:

$$I(X,Y) = I(Y,X) = H(Y) - H(Y|X). \tag{5.28}$$

The concept of mutual information let us introduce the concept of channel capacity. Channel capacity is defined as the maximum value that mutual information between two variable can assume with respect to all possible distributions of the input variable:

$$C = \max_{P_X(x)} I(X,Y), \tag{5.29}$$

i.e. it represents the maximum transferable information with respect to all the possible information sources. This value has a very strong meaning. The Shannon's coding theorem states that, given an information source with entropy H and a channel with capacity C:

- if $H \leq C$ then there is a coding system that allows the transmission of the data produced from the source with an arbitrary small error rate, i.e. arbitrary equivocation;
- if $H > C$ there is no coding system that can let the equivocation be less then $H - C$.

It is worth to notice that, the theorem states that the coder exists, but it does not give any tip on how to design the coder.

A3 Differential Entropy

n this section, we introduce the concept of differential entropy, that is the extension of the entropy concept to the continuous case. Even if the mathematical definition is very similar to the one given in section , it is necessary

to highlight some remarkable differences in order to make the right interpretations.

Definition: the differential entropy $h(X)$ of a continuous random variable X with probability density function $p_X(x)$ is defined as:

$$h(X) = -\int_{-\infty}^{\infty} p_X(x) \log p_X(x) dx. \tag{5.30}$$

Example: Let's consider the case of a continuous random variable with uniform probability density function in $[0,\ \Delta]$ (this case will appear very often in the thesis). In such a case, the differential entropy is:

$$h(X) = -\int_{0}^{\Delta} \frac{1}{\Delta} \log \frac{1}{\Delta} dx = \log \Delta. \tag{5.31}$$

Note that, if $\Delta < 1$ then $h(X) < 0$. It is evident that differential entropy cannot be interpreted in the same way of entropy and even if a negative entropy is not intuitive, it has a simple geometric interpretation. Just like in the discrete case, where $2^{H(X)}$ represents the size of the effective alphabet of the source, in the continuous case, $2^{h(X)}$ represents the size of the volume that contains the majority of probability density. So $h(X)$ is a logarithmic measure of the of volume the random variable occupies.

This interpretation has an interesting consequence: the differential entropy of a discrete variable diverges to $-\infty$. That is because the domain of a discrete variable has a geometrically null size. Thus, being $h(X) = log(0) = -\infty$.

List of Figures

List of Equations

Bibliography

[Barman et al., 2014] Barman, S., Chattopadhyay, S., Samanta, D., Bag, S., and Show, G. (2014). An efficient fingerprint matching approach based on minutiae to minutiae distance using indexing with effectively lower time complexity. In *2014 International Conference on Information Technology*, pages 179–183.

[Bartelt et al., 1984] Bartelt, H., Lohmann, A. W., and Wirnitzer, B. (1984). Phase and amplitude recovery from bispectra. *Appl. Opt.*, 23(18):3121–3129.

[Berrou and Glavieux, 1996] Berrou, C. and Glavieux, A. (1996). Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Trans. on Communications*, 44(10):1261–1271.

[Blanton and Aliasgari, 2011] Blanton, M. and Aliasgari, M. (2011). On the (non-)reusability of fuzzy sketches and extractors and security in the computational setting. In *Proceedings of the International Conference on Security and Cryptography*, pages 68–77.

[Blanton and Aliasgari, 2013] Blanton, M. and Aliasgari, M. (2013). Analysis of reusability of secure sketches and fuzzy extractors. *IEEE Transactions on Information Forensics and Security*, 8(9):1433–1445.

[Boyen, 2004] Boyen, X. (2004). Reusable cryptographic fuzzy extractors. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 82–91, New York, NY, USA. ACM.

[Brent, 1973] Brent, R. (1973). *Algorithms for Minimization Without Derivatives*. Dover Books on Mathematics. Dover Publications.

[Bringer et al., 2006] Bringer, J., Chabanne, H., and Do, Q. D. (2006). A fuzzy sketch with trapdoor. *IEEE Trans. on Information Theory*, 52(5):2266–2269.

[Buhan et al., 2010a] Buhan, I., Breebaart, J., Guajardo, J., de Groot, K., Kelkboom, E., and Akkermans, T. (2010a). A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem. In Garcia-Alfaro, J., Navarro-Arribas, G., Cuppens-Boulahia, N., and Roudier, Y., editors, *Data Privacy Management and Autonomous Spontaneous Security*, pages 78–92, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Buhan et al., 2008a] Buhan, I., Doumen, J., and Hartel, P. (2008a). Controlling leakage of biometric information using dithering. In *16th European Signal Processing Conference*, pages 1–5.

[Buhan et al., 2008b] Buhan, I., Doumen, J., Hartel, P., Tang, Q., and Veldhuis, R. (2008b). Embedding renewable cryptographic keys into continuous noisy data. In *Information and Communications Security*, pages 294–310. Springer.

[Buhan et al., 2010b] Buhan, I., Guajardo, J., and Kelkboom, E. (2010b). Efficient strategies to play the indistinguishability game for fuzzy sketches. In *2010 IEEE International Workshop on Information Forensics and Security*, pages 1–6.

[Bui et al., 2010] Bui, F. M., Martin, K., Lu, H., Plataniotis, K. N., and Hatzinakos, D. (2010). Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications. *IEEE Trans. on Information Forensics and Security*, 5(1):118–132.

[Campisi, 2013] Campisi, P. (2013). *Security and Privacy in Biometrics*. Springer Publishing Company, Incorporated.

[Cappelli et al., 2010] Cappelli, R., Ferrara, M., and Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12):2128–2141.

[Chen and Wornell, 2001] Chen, B. and Wornell, G. W. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Trans. on Information Theory*, 47(4):1423–1443.

[Cimato et al., 2009] Cimato, S., Gamassi, M., Piuri, V., Sassi, R., and Scotti, F. (2009). Privacy in biometrics. In N.V. Boulgouris, K. P. and Micheli-Tzanakou, E., editors, *Biometrics: Theory, Methods, and Applications*. John Wiley & Sons, Inc., Hoboken, NJ, USA.

[Cover and Thomas, 2012] Cover, T. M. and Thomas, J. A. (2012). *Elements of information theory*. John Wiley & Sons.

[De Cristofaro and Tsudik, 2010] De Cristofaro, E. and Tsudik, G. (2010). Practical private set intersection protocols with linear complexity. In Sion, R., editor, *Financial Cryptography and Data Security*, pages 143–159, Berlin, Heidelberg. Springer Berlin Heidelberg.

[de Groot et al., 2016] de Groot, J., Škorić, B., de Vreede, N., and Linnartz, J.-P. (2016). Quantization in zero leakage helper data schemes. *EURASIP Journal on Advances in Signal Processing*, 54:1–13.

[de Groot and Linnartz, 2011] de Groot, J. A. and Linnartz, J.-P. (2011). Zero leakage quantization scheme for biometric verification. In *IEEE International Conference onAcoustics, Speech and Signal Processing (ICASSP)*, pages 1920–1923.

[de Groot et al., 2013] de Groot, J. A., Škorić, B., de Vreede, N., and Linnartz, J.-P. (2013). Diagnostic category leakage in helper data schemes for biometric authentication. In *IEEE SECRYPT*, pages 1–6.

[Dodis et al., 2004] Dodis, Y., Ostrovsky, R., Reyzin, L., and Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Lecture Notes in Computer Science, Vol. 3027*, pages 523–540.

[European Union, 2016] European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L119:1–88.

[Fierrez et al., 2010] Fierrez, J., Galbally, J., Ortega-Garcia, J., Freire, M. R., Alonso-Fernandez, F., Ramos, D., Toledano, D. T., Gonzalez-Rodriguez, J., Siguenza, J. A., Garrido-Salas, J., Anguiano, E., Gonzalez-de Rivera, G., Ribalda, R., Faundez-Zanuy, M., Ortega, J. A., Cardeñoso-Payo, V., Viloria, A., Vivaracho, C. E., Moro, Q. I., Igarza, J. J., Sanchez, J., Hernaez, I., Orrite-Uruñuela, C., Martinez-Contreras, F., and Gracia-Roche, J. J. (2010). Biosecurid: a multimodal biometric database. *Pattern Analysis and Applications*, 13(2):235–246.

[Gomez-Barrero et al., 2016a] Gomez-Barrero, M., Fiérrez, J., Galbally, J., Maiorana, E., and Campisi, P. (2016a). Implementation of fixed-length template protection based on homomorphic encryption with application to signature biometrics. *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 259–266.

[Gomez-Barrero et al., 2018] Gomez-Barrero, M., Galbally, J., Rathgeb, C., and Busch, C. (2018). General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, 13(6):1406–1420.

[Gomez-Barrero et al., 2016b] Gomez-Barrero, M., Rathgeb, C., Galbally, J., Busch, C., and Fierrez, J. (2016b). Unlinkable and irreversible biometric template protection based on bloom filters. *Inf. Sci.*, 370(C):18–32.

[Hine et al., 2017] Hine, G. E., Maiorana, E., and Campisi, P. (2017). A zero-leakage fuzzy embedder from the theoretical formulation to real data. *IEEE Transactions on Information Forensics and Security*, 12(7):1724–1734.

[Hine et al., 2018] Hine, G. E., Maiorana, E., and Campisi, P. (2018). Fingerprint minutiae matching through sparse cross-correlation. In *2018, 26th European Signal Processing Conference (EUSIPCO)*.

[Ignatenko and Willems, 2015] Ignatenko, T. and Willems, F. (2015). Fundamental limits for privacy-preserving biometric identification systems that support authentication. *IEEE Trans. on Information Theory*, 61(10):5583–5594.

[Ignatenko and Willems, 2008] Ignatenko, T. and Willems, F. M. J. (2008). Privacy leakage in biometric secrecy systems. In *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, pages 850–857.

[Ignatenko and Willems, 2009] Ignatenko, T. and Willems, F. M. J. (2009). Biometric systems: Privacy and secrecy aspects. *IEEE Trans. on Information Forensics and Security*, 4(4):956–973.

[Ignatenko and Willems, 2010] Ignatenko, T. and Willems, F. M. J. (2010). Information leakage in fuzzy commitment schemes. *IEEE Transactions on Information Forensics and Security*, 5(2):337–348.

[Ignatenko and Willems, 2013] Ignatenko, T. and Willems, F. M. J. (2013). Privacy leakage in binary biometric systems: From Gaussian to binary data. In Campisi, P., editor, *Security and Privacy in Biometrics*, pages 105–122. Springer London.

[ISO/IEC 2382-37, 2017] ISO/IEC 2382-37 (2017). Information technology vocabulary part 37: Biometrics. Standard, International Organization for Standardization (ISO).

[ISO/IEC 30136, 2018] ISO/IEC 30136 (2018). Information technology performance testing of biometric template protection schemes. Standard, International Organization for Standardization (ISO).

[Jain et al., 2008] Jain, A. K., Nandakumar, K., and Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, pages 1–17.

[Jain et al., 1999] Jain, A. K., Prabhakar, S., Hong, L., and Pankanti, S. (1999). Fingercode: a filterbank for fingerprint representation and matching. In *Proceedings. 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (Cat. No PR00149)*, volume 2, page 193 Vol. 2.

[Jain et al., 2000] Jain, A. K., Prabhakar, S., Hong, L., and Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE Trans. on Image Processing*, 9(5):846–859.

[Jeffers and Arakala, 2006] Jeffers, J. and Arakala, A. (2006). Minutiae-based structures for a fuzzy vault. In *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, pages 1–6.

[Jin et al., 2004] Jin, A. T. B., Ling, D. N. C., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245 – 2255.

[JTC1 SC27 IT Security Techniques ISO/IEC 24745, 2011] JTC1 SC27 IT Security Techniques ISO/IEC 24745 (2011). Biometric information protection. Standard, International Organization for Standardization (ISO).

[Juels and Sudan, 2006] Juels, A. and Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257.

[Juels and Wattenberg, 1999] Juels, A. and Wattenberg, M. (1999). A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, pages 28–36, New York, NY, USA. ACM.

[Kelkboom et al., 2011] Kelkboom, E. J. C., Breebaart, J., Kevenaar, T. A. M., Buhan, I., and Veldhuis, R. N. J. (2011). Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121.

[Kevenaar et al., 2010] Kevenaar, T. A. M., Korte, U., Merkle, J., Niesing, M., Ihmor, H., Busch, C., and Zhou, X. (2010). A reference framework for the privacy assessment of keyless biometric template protection systems. In *BIOSIG 2010 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 09.-10. September 2010 in Darmstadt, Germany*, pages 45–56.

[Kholmatov and Yanikoglu, 2008] Kholmatov, A. and Yanikoglu, B. (2008). Realization of correlation attack against the fuzzy vault scheme.

[Korte and Plaga, 2007] Korte, U. and Plaga, R. (2007). Cryptographic protection of biometric templates: Chance, challenges and applications. In *BIOSIG*, pages 33–46.

[Lai et al., 2015] Lai, L., Ho, S.-W., and Poor, H. V. (2015). Privacy-security trade-offs in biometric security systems - part i: Single use case. *IEEE Trans. on Information Forensics and Security*, 6(1):122–139.

[Lee et al., 2017] Lee, W., Cho, S., Choi, H., and Kim, J. (2017). Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners. *Expert Systems with Applications*, 87:183 – 198.

[Li et al., 2010] Li, P., Yang, X., Cao, K., Tao, X., Wang, R., and Tian, J. (2010). An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *J. Netw. Comput. Appl.*, 33(3):207–220.

[Linnartz and Tuyls, 2003] Linnartz, J. and Tuyls, P. (2003). New shielding functions to enhance privacy and prevent misuse of biometric templates. In *AVBPA*, pages 393–402.

[Linnartz et al., 2007] Linnartz, J.-P., Tuyls, P., and Škorić, B. (2007). A communication-theoretical view on secret extraction. In *Security with Noisy Data*, pages 57–77. Springer.

[Maiorana et al., 2012] Maiorana, E., Blasi, D., and Campisi, P. (2012). Biometric template protection using turbo codes and modulation constellations. In *IEEE WIFS*.

[Maiorana et al., 2014] Maiorana, E., Campisi, P., and Neri, A. (2014). Iris template protection using a digital modulation paradigm. In *IEEE International Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, pages 3759–3763.

[Maiorana et al., 2013a] Maiorana, E., Hine, G. E., and Campisi, P. (2013a). Hill-climbing attack: Parametric optimization and possible countermeasures. an application to on-line signature recognition. In *International Conference on Biometrics (ICB),*, pages 1–6.

[Maiorana et al., 2015a] Maiorana, E., Hine, G. E., and Campisi, P. (2015a). Hill-climbing attacks on multibiometrics recognition systems. *IEEE Trans. on Information Forensics and Security*, 10(5):900–915.

[Maiorana et al., 2013b] Maiorana, E., Hine, G. E., La Rocca, D., and Campisi, P. (2013b). On the vulnerability of an EEG-based biometric system to hill-climbing attacks algorithms' comparison and possible countermeasures. In *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–6.

[Maiorana et al., 2015b] Maiorana, E., Rocca, D. L., and Campisi, P. (2015b). Cognitive biometric cryptosystems a case study on eeg. In *International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 125–128.

[Medina-Pérez et al., 2012] Medina-Pérez, M. A., García-Borroto, M., Gutierrez-Rodríguez, A. E., and Altamirano-Robles, L. (2012). Improving fingerprint verification using minutiae triplets. *Sensors*, 12(3):3418–3437.

[Mordini, 2008] Mordini, E. (2008). Biometrics, human body and medicine: A controversial history. In P. Duquenoy, C. G. and Kimppa, K., editors, *Ethical, Legal and Social Issues in Medical Informatics*, pages 249–272. Hershey, PA: Idea Group Inc.

[Nandakumar and Jain, 2004] Nandakumar, K. and Jain, A. K. (2004). Local correlation-based fingerprint matching. In *In Indian Conference on Computer Vision, Graphics and Image Processing*, pages 503–508.

[Nandakumar and Jain, 2015] Nandakumar, K. and Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5):88–100.

[Nandakumar et al., 2007] Nandakumar, K., Jain, A. K., and Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757.

[Ortega-Garcia et al., 2003] Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J. J., Vivaracho, C., Escudero, D., and Moro, Q. I. (2003). Mcyt baseline corpus: a bimodal biometric database. *IEE Proceedings - Vision, Image and Signal Processing*, 150(6):395–401.

[Paillier, 1999] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In Stern, J., editor, *Advances in Cryptology — EUROCRYPT '99*, pages 223–238, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Patel et al., 2015] Patel, V. M., Ratha, N. K., and Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine: Special Issue on Biometric Security and Privacy*, 32(5):54–65.

[Peralta et al., 2015] Peralta, D., Galar, M., Triguero, I., Paternain, D., García, S., Barrenechea, E., Benítez, J. M., Bustince, H., and Herrera, F. (2015). A survey on fingerprint minutiae-based local matching for verification and identification. *Inf. Sci.*, 315(C):67–87.

[Petropulu and Pozidis, 1998] Petropulu, A. P. and Pozidis, H. (1998). Phase reconstruction from bispectrum slices. *IEEE Transactions on Signal Processing*, 46(2):527–530.

[Rane, 2014] Rane, S. (2014). Standardization of biometric template protection. *IEEE MultiMedia*, 21(4):94–99.

[Rane et al., 2013] Rane, S., Wang, Y., Draper, S. C., and Ishwar, P. (2013). Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine*, 30(5):51–64.

[Rathgeb et al., 2018] Rathgeb, C., Buchmann, N., Hofbauer, H., Baier, H., Uhl, A., and Busch, C. (2018). Methods for accuracy-preserving acceleration of large-scale comparisons in cpu-based iris recognition systems. *IET Biometrics*, 7(4):356–364.

[Rathgeb and Uhl, 2011] Rathgeb, C. and Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 3:1–25.

[Shannon, 1948] Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423.

[Shannon, 1949] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715.

[Simoens et al., 2009] Simoens, K., Tuyls, P., and Preneel, B. (2009). Privacy weaknesses in biometric sketches. In *2009 30th IEEE Symposium on Security and Privacy*, pages 188–203.

[Sood and Kaur, 2014] Sood, P. and Kaur, M. (2014). Methods of automatic alignment of fingerprint in fuzzy vault: A review. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pages 1–4.

[Sripad and Snyder, 1977] Sripad, A. B. and Snyder, D. (1977). A necessary and sufficient condition for quantization errors to be uniform and white. *IEEE Trans. on Acoustics, Speech, and Signal Processing*, 25(5):442–448.

[Stoianov, 2009] Stoianov, A. (2009). Security issues of biometric encryption. In *IEEE Toronto International Conference on Science and Technology for Hunanity (TIC-STH)*, pages 34–39.

[Sutcu et al., 2007] Sutcu, Y., Q.Li, and Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. *IEEE Trans. on Information Forensics and Security*, 2(3):503–512.

[Tams, 2014] Tams, B. (2014). Decodability attack against the fuzzy commitment scheme with public feature transforms. *CoRR*, abs/1406.1154.

[Tams, 2016] Tams, B. (2016). Unlinkable minutiae-based fuzzy vault for multiple fingerprints. *IET Biometrics*, 5:170–180(10).

[Tuyls et al., 2005] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijen, G.-J., Bazen, A. M., and Veldhuis, R. N. J. (2005). Practical biometric authentication with template protection. In *AVBPA*, pages 436–446.

[Tuyls et al., 2004] Tuyls, P., Verbitskiy, E., Ignatenko, T., Schobben, D., and Akkermans, A. (2004). Privacy-protected biometric templates: Acoustic ear identification. In *Proceedings of SPIE, Vol. 5404*, pages 176–182.

[Uludag et al., 2004a] Uludag, U., Pankanti, S., and Jain, A. K. (2004a). Biometric cryptosystems: issues and challenges. *Proceedings of IEEE*, 92(6):948–960.

[Uludag et al., 2004b] Uludag, U., Pankanti, S., Prabhakar, S., and Jain, A. K. (2004b). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6):948–960.

[Watson et al.,] Watson, C., Garris, M., Tabassi, E., Wilson, C., Janet, S., and Ko, K. User?s guide to export controlled distribution of nist biometric image software (nbis-ec).

[WD 30136, 2014] WD 30136 (2014). Performance testing of biometric template protection schemes. Standard.

[Xu and Veldhuis, 2010a] Xu, H. and Veldhuis, R. (2010a). *Spectral Minutiae Representations for Fingerprint Recognition*, pages 341–345. IEEE Computer Society.

[Xu and Veldhuis, 2010b] Xu, H. and Veldhuis, R. N. J. (2010b). Complex spectral minutiae representation for fingerprint recognition. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, pages 1–8.

[Xu et al., 2009] Xu, H., Veldhuis, R. N. J., Bazen, A. M., Kevenaar, T. A. M., Akkermans, T. A. H. M., and Gokberk, B. (2009). Fingerprint verification using spectral minutiae representations. *IEEE Transactions on Information Forensics and Security*, 4(3):397–409.

[Yellott and Iverson, 1992] Yellott, J. I. and Iverson, G. J. (1992). Uniqueness properties of higher-order autocorrelation functions. *J. Opt. Soc. Am. A*, 9(3):388–404.

[Zanganeh et al., 2014] Zanganeh, O., Srinivasan, B., and Bhattacharjee, N. (2014). Partial fingerprint matching through region-based similarity. In *2014 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*, pages 1–8.

[Zhou and Busch, 2012] Zhou, X. and Busch, C. (2012). Measuring privacy and security of iris fuzzy commitment. In *IEEE International Carnahan Conference on Security Technology (ICCST)*, pages 168–173.

[Zhou et al., 2011] Zhou, X., Kuijper, A., Veldhuis, R., and Busch, C. (2011). Quantifying privacy and security of biometric fuzzy commitment. In *International Joint Conference on Biometrics (IJCB)*, pages 1–8.