PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF KASDI MERBAH OUARGLA

Faculty of New Information Technologies and Communication

Department of Electronics and Telecommunications

Thesis submitted in partial fulfillment of the requirements for the degree of

Master

In: Telecommunications systems

By: BENDANIA Manal Khedidja & ZEKRI Amel

Theme

Biometric Crypto System for Person Information Security

JURY

Mr..KORICHI Maarouf	Ouargla University	President
	Ouargla University	Examiner
	Ouargla University	Examiner
	Ouargla University	Supervisor

2019- 2020

Acknowledgment

First, I would like to thank ALLAH for giving us the strength to complete this project.

Then, we would like to thank all the people who contributed in some way to the work described in this dissertation. At first, I thank my academic advisors Mr. KORICHI Maarouf for their support and positive attitude towards the project. The guidance, inspiration and different perspectives added in our discussions have been most valuable.

A special thanks to the member of jujus performing this dissertation has been a valuable learning experience for both of us, to learn more about the industrial world.

Dedication

I dedicate this dissertation to the most important persons in my life.

My mother who has a smile of sunshine and a heart of pure gold, in her eyes there is a bright shining stars, in her cheeks fair roses a wonderful mother .

To my father a man like no other, a person who loves and kind he held me play with me shouted at me kissed me but most importantly, he loved me unconditionally

I also want to dedicate this work to my sisters and four brothers; I thank them for being by my side every day.

To my dear girlfriend and my lifelong companion, ZEKRI Amel, may God protect her.

To my amazing friends, GHETTAS Nadjat, MALIANA Boutheina who thought me that friendship is not about whom I have known the longest, but it is about who came and never left my side.

Dedication

I dedicate this humble work to those who are my strength, inspiration and determination

To my dear mother, may God have mercy on her, who left the world and never left my heart, which always gave me strength and hope in this life.

To my dear father, for his encouragement and support, and above all for him Sacrifice so that nothing gets in the way of my studies. May God protect him and prolong his life.

To my brothers and sisters May God protects them and their children.

To all members of the ZEKRI family and all my friends

To everyone who lent me a helping hand to all the people I love.

To my dear girlfriend and my lifelong companion, Manel Ben - Dania, may God protect her.

ABSTRACT

Information security is the science that works to provide protection for information and services circulating on the Internet from the dangers that threaten it. With the development of technology, the security of this information has become an obsession and a very important topic, and reliance on traditional means has become very worrying due to the ease of penetration of this information, so the world went to search for Other systems are safer and more effective, and among these well-known systems is the biometric- crypto system, and the latter resulted from the merging of two biometric and cryptography systems, which were combined to overcome the deficiency in both systems.

In this memoire we have provided a definition of a biometric crypto-system and her modalities and How can we evaluate It is performed on several criteria, moreover we talked about two biometric techniques and those were Unimodal and multimodal , and we reveal how is it that Multimodal biometric system is better than unimodal.

In the context of vision, Gabor filters correspond to information reaching the visual cortex and fragmented into small packets. So in our work this we experimented a uni / multimodal biological system based on PLM by using Gabor geometry. With using a database of 300 people, we were able to prove the efficacy of PLM modality in a Biometric- Crypto system.

Key Words: Security Biometric Unimodal Multimodal PLM

Résumé

La sécurité de l'information est la science qui œuvre pour protéger les informations et les services circulant sur Internet contre les dangers qui la menacent. Avec le développement de la technologie, la sécurité de ces informations est devenue une obsession et un sujet très important, et le recours aux moyens traditionnels est devenu très inquiétant en raison de la facilité de pénétration de ces informations, de sorte que le monde est allé à la recherche d'autres systèmes sont plus sûr et plus efficace, et parmi ces systèmes bien connus, il y a le système biométrique-crypto, et ce dernier résulte de la fusion de deux systèmes biométriques et cryptographiques, qui ont été combinés pour surmonter les lacunes des deux systèmes.

Dans ce mémoire, nous avons fourni une définition d'un crypto-système biométrique et ses modalités et Comment pouvons-nous l'évaluer Il est effectué sur plusieurs critères, de plus nous avons parlé de deux techniques biométriques et celles-ci étaient unimodales et multimodales, et nous révélons comment se fait-il que Le système biométrique multimodal est meilleur qu'un système unimodal.

Dans le cadre de la vision, les filtres de Gabor correspondent à des informations atteignant le cortex visuel et fragmentées en petits paquets. Ainsi, dans notre travail, nous avons expérimenté un système biologique uni / multimodal basé sur le PLM en utilisant la géométrie de Gabor. En utilisant une base de données de 300 personnes, nous avons pu prouver l'efficacité de la modalité PLM dans un système Biométrique-Crypto.

Mots clés: PLM multimodal uni modal biométrique de sécurité

Table of contents

Chapter III: Experimental results and discussion

Figure list

Table list

Abbreviation list

AES: Advance Encryption Standard

CMC: Cumulative Match Curve

DES: Data Encryption Standard

DNA: Deoxy de Nucleic Acid

EER: Equal Error Rate

FAR: False Acceptance Rate

FRR: False Rejection Rate

GAR: Genuine Acceptance Rate

GL: Grey Level representation

MSP: Multispectral Palm print

NIR: Near Infra-Red

PIN: Personal Identifier Number

PLM: Palm print

RC4: Rivest Cipher 4

ROC: Receiver Operating Characteristic

ROR: Recognition One Rate

RPR: Recognition Perfect Rate

Introduction

With the development of technology and information, the world has become a small village, where there has become a shortening of distances and an acceleration of services, Especially in recent times, we find that most services are done electronically through smart devices, including : e-banking ,ecommerce And many services related to work and education but on the other hand, we find the world is facing a problem because of this technological development it is the problem of protecting this information is generally sensitive and must be secured therefore, it is necessary to have a comprehensive safety system able to recognize and authenticate the identity of users such as the biometric system and crypto system biometric system is essentially a pattern recognition system that operates by ac-quirking biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template specified in the database and crypto system is a system allows a secure key to be linked with biometric data to obtain a so-called secure graph so, we find that biometrics and cryptographic are protection systems, but each of them has a deficiency, and to overcome this deficiency, they must be combined to obtain an effective safety system, what is called Biometric-Crypto system, Biometric cryptosystem are designed to securely bind a digital key to a biometric or generate digital key from a biometric, and this last one can be integrated into three ways namely : 1) Key Release, 2) Key Binding and 3) Key Generation.

Nowadays biometric identification is used in many applications such as protecting access to the computer, mobile phone, bank cards ...Many biometric technologies have been developed, all based on identifier physiological and behavioral biometrics such as: iris, voice, fingerprints, PLM, face, signature.... These are more reliable than conventional systems (key, password...) in the recognition of a person because they are difficult to falsify. This is the reason why biometric systems are currently more and more in demand among these biometric models, we choose the strongest to recognize the character, which in turn attracted researchers due to its stable characteristics, it is also an acceptable technology for individuals, simple and easy to use this technique is called palm print. Palm print recognition is a biometric authentication method based on the unique patterns of various characteristics in the palm of people's hand.

Our work is divided into three chapters

- In the first chapter, we began to present a general concept of information security strategies later we describe cryptography and its types, In addition to biometrics in its traditional and modern types and their modalities, and at the end we provided a brief overview of Biometrics Crypto-system and its keys.

- And the second chapter we describe biometric system architecture, we learned about the technology used to extract the features In addition to proposed biometric crypto system we ended this chapter with a security analysis of Biometrics Crypto-systems.

- In the last chapter, we presented a theoretical explanation of a biometric feature called palm print, using single-modal and multimodal systems, thus analyzing and presenting the results obtained and concluding the thesis.

CHAPTER I

INFORMATION SECURITY STRATEGIES

Chapter I: Information Security strategies.

I.1 Introduction

Information security is a method of protecting information from unauthorized access. Authentication plays very important role in the field of information security. It brings about the availability, confidentiality, and integrity. Literally, numerous methods were proposed to ensure it. The well-known and the most used method one can cite cryptography and biometric.

The aim of this chapter is to give an overview on the techniques that used in the field of information security. Firstly, we will introduce some notion on information security. Then, the classical information security techniques. After that, we will discuss the problem related to these classical methods. Finally, as a solution to that problem, we will present the biometric based template protection or one can call as Biometric-Crypto system.

I.2 Information security

Information security is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another. You might sometimes see it referred to as *data* security. As knowledge has become one of the 21st century's most important assets, efforts to keep information secure have correspondingly become increasingly important. [1]

Information Security is not all about securing information from unauthorized access. It is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Information can be physical or electrical one. It can be anything like your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus, information security spans so many research areas like Biometrics and Cryptography. [2]

Biometrics and cryptography are two widely used techniques for providing information security. Biometrics is defined as automated recognition of individuals based on their behavioral and biological characteristics. Biometric recognition provides a strong link between the user's identity and the authenticator. Cryptography, on the other hand, deals with protecting information with the help of secret keys. In cryptography, it is understood that the keys are kept secret, i.e., it requires trust, and this trust is projected where it is required. [3]

I.3 Cryptography

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage. In Encryption, the data, denoted as plaintext, is transformed into illegible gibberish, denoted as ciphertext, with the help of an encryption key. The reverse of data encryption process is called data Decryption. [4]

Cryptography is closely related to the disciplines of Cryptology and Cryptanalysis. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into cipher text, then back again. Individuals who practice this field are known as cryptographers. The basic idea of cryptography is shown in **Figure I.1**.

Hereafter we give a brief definition of some most known terms in cryptography:

- **Plain Text**: the original message that the person wishes to communicate with the other is defined as Plain Text. For example, Alice is a person wishes to send “Hello Friend how are you” message to the person Bob. Here “Hello Friend how are you” is a plain text message.

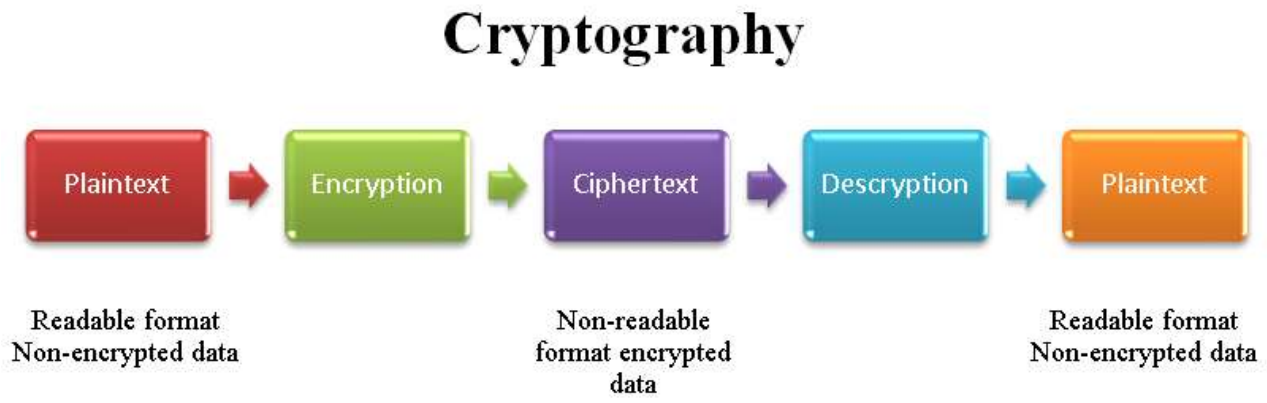


Figure I. 1 : Basic idea of cryptography.

- **Cipher Text:** The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. For example, “Ajd672#@91ukl8*^5%” is a Ciphertext produced.

- **Encryption:** The process of converting Plaintext into Ciphertext is called as Encryption. Cryptography use encryption technique to send confidential messages through an insecure channel.

- **Decryption:** It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Ciphertext). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally, the encryption and decryption algorithm are same.

- **Cryptographic Key:** A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Ciphertext produced will be "Suhvlghqw". [5]

Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography. Following are the different goals of cryptography:

1. **Confidentiality:** it means nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contact only by the authorized party and not by unauthorized person.
2. **Authentication**: This process is proving a one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from an authorized person or unauthorized person or wrong identity.
3. **Integrity**: only the authorized party is modifying the transmitted information or message. Nobody can change the given message [4].

In the field of cryptography there exist several techniques for encryption/decryption. These techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Confidentiality defines a set of rules that limits access or adds restriction on certain information.

I .3.1 Types of Cryptographic Algorithm

According to the literature review, one can classify the cryptographic algorithms into two main categories namely:

- Secret Key Cryptography or also called as **Symmetric Key Cryptography**.
- Public Key Cryptography this or simply **Asymmetric Key Cryptography**

I.3.1.1 Symmetric Cryptography:

Symmetric-key cryptographic algorithm includes a class of algorithms for cryptography that uses same cryptographic key for the purpose of encryption of plain text and the decryption of cipher text. It is the oldest known encryption method. The secret key can be as simple a number or a string of letters etc. The keys, in practice, represent a shared secret between the participating parties to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Symmetric-key encryption can use either of the stream cipher or block cipher, where a stream cipher encrypts the digits/bytes of a message one at a time and the block cipher take a number of bits as input and encrypt them as a single unit. The popular symmetric cryptographic algorithms include, AES, Blowfish, RC5, DES, 3DES and IDEA. When using symmetric algorithms, same key is used for encryption and decryption by both the parties. [6]

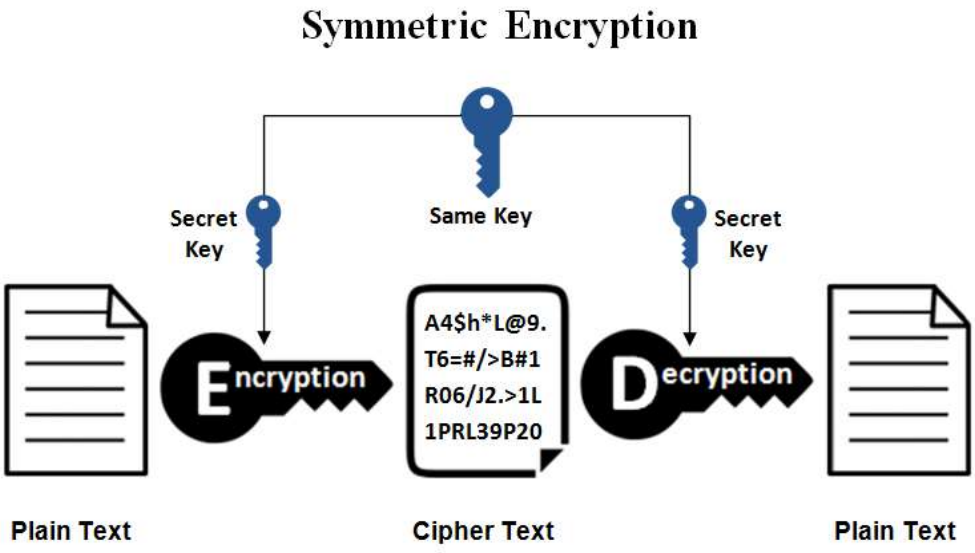


Figure I. 2 : Symmetric encryptions.

I.3.1.2 Asymmetric cryptographic techniques:

Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key, encrypts, only the other can decrypt. Frequently (but not necessarily), the keys are, interchangeable, in the sense that if key A encrypts a message, then B can decrypt it, and if, Key B encrypts a message, then key A Can decrypt it. While common, this property is not essential to asymmetric encryption. As shown in the **Figure I.3.**

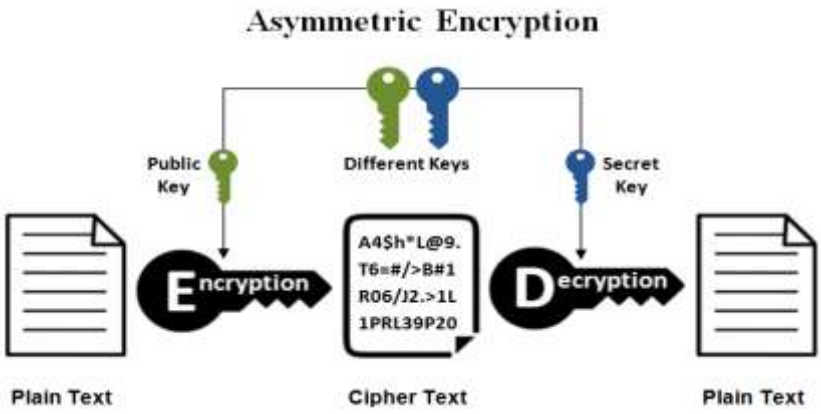


Figure I. 3: Asymmetric Encryption.

Asymmetric Encryption is also known as public key cryptography, since users typically create a matching key pair, and make one public while keeping the other secret. Users can "sign" messages by encrypting them with their private keys. This is effective since any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user's secret key was used to encrypt it. If the user's secret key is, in fact, secret, then it follows that the user, and not some impostor, really sent the message.

Users can send secret messages by encrypting a message with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that user should have access to the required secret key.

The key to successful use of Asymmetric Encryption is a key management system, which implements a public key infrastructure. Without this, it is difficult to establish the reliability of public keys, or even to conveniently find suitable ones.

I.3.2 Problem related to cryptography

According to the Kirchhoff's principle, security of a cryptographic system lies entirely on the secrecy of the cryptographic key. Additionally, for security reasons, the cryptographic keys are required to be long. For example, the possible lengths of keys required in the AES are 128, 192, or 256 bits. For public-key cryptographic systems such as RSA, the key lengths are even higher (e.g., 512, 1024, or 2048 bits). Clearly, a user cannot remember such long keys and therefore, the keys need to be stored somewhere, e.g., on a smart card or in a computer.

In order to restrict access to these keys only to legitimate users, authentication mechanisms are used. Traditionally, authentication mechanisms employed in cryptography are knowledge based (e.g., passwords) or possession based (e.g., token, smart card, etc.). These authenticators are assigned to the user identity and do not necessarily indicate the presence of the person to which they belong. Therefore, they can be (more or less easily) stolen by an attacker, and in this situation, the system cannot distinguish between the attacker and a legitimate user. [3]

I.4 Biometric

Biometrics is a term, which is an artificial composition of two the Greek words "bios" meaning life and "metros" for metric [7]. Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Several aspects of this definition require elaboration [8]. There exist three principles classes for obtaining information about personal traits for measurement of biometrics. The biometric traits are also known as biometric modalities [7]:
The first classes deal with the analysis of the persons physiological traits such as fingerprint, palm print, face, ear, iris and etc... Whereas the second classes treat the person behavior likes voice, keystroke dynamics, or individual gait. The last classes are concerned with the treatment of biological characteristics which is based on the analysis of biological data related to the individual (saliva, DNA, etc.)**(**See **Figure I.4).**
In practice, any morphological or behavioral characteristic can be considered a biometric characteristic, so far as it satisfies the following properties [9]:

- **Universality:** all persons to be identified must possess it.
- **Uniqueness:** the information must be as dissimilar as possible between the different people.
- **Permanence:** the information collected must be present throughout the life of an individual.
- **Collectability:** the information must be collectable and measurable to be used for

comparisons.

- **Acceptability:** the system must respect certain criteria (acquisition facility, rapidity, etc), to be used.

Figure I. 4 : Taxonomy of biometric modalities.

The risks of using biometrics fall into a few categories, including data and network hacking, rapidly evolving fraud capabilities, biometric enrollment security, familiar fraud (that is, caused by a family member or friend), spoofed sensors, and sensor inaccuracy.

One of the greatest risks is data security. Biometric sensors produce digital maps of a body part, which are then used for future matching and unlocking. That digital map can be stored locally on some devices or transmitted across a network to a central storage database. Locally held data is significantly better protected because it is never out of your control while in transit. Data in motion must be encrypted on its way to storage and then secured. In both transit and storage, the data is vulnerable, and hackers are fairly adept at breaking into either, particularly if the data isn't encrypted.

I.5 Introduction to Biometric cryptosystem

As seems in the previous section, we found that both of cryptography and biometric suffer from different problems. For that, the researcher proposes to combine between them in order to produce a new system called Biometric-Crypto system to overcome their drawbacks. A combination of biometrics and cryptography has the potential to provide a higher assurance of the legal information

holder. A crucial issue in cryptographic systems is the problem of key management. Hence, how to make use of biometrics in cryptographic systems is often related to the issue of how to combine biometrics with cryptographic keys. Literally, Biometric-Crypto system can be classified in three main categories namely: Key release, Key binding or regeneration and Key generation. In a key release mode, biometrics plays a predetermined role in a cryptosystem. The key would be released to users only if biometric matching is successful. A key generation mode requires the key of a cryptosystem being derived directly format biometric template, hence the unique biometrics provides a unique key for the security system based on some transformer feature extraction. In the key binding mode, the system binds a cryptographic key with the user's biometrics at the time of enrollment. The key would be retrieved only upon a successful authentication. The key generation/binding mode seems to be more secure than the key release mode because in key release mode, the user authentication and key release are two separate parts. However, whatever mode a biometric cryptosystem takes, one major difference between biometrics and cryptographic key management should be addressed.

The conventional cryptography systems do not need any complex pattern recognition strategy as in biometric systems. They almost always depend on an accurate key matching process. For that, it requires that keys are exactly correct and does not tolerate a single bit error. However, as biometric characteristics are known to be variable and noisy and each new biometric sample is always different, only an approximate match under a threshold between the input biometric data to a corresponding stored template would lead the authentication successful. Therefore, how to build a bridge between the fuzziness of biometric matching and the exactness of key based cryptography systems seems to be a great challenge for Biometric-Cryptosystems. [10]

Hereafter, we will give a brief discussion of the three mode of Biometric-Crypto system

I.5.1 Key Release based on biometrics

The basic idea of biometric-based keys is that the biometric component performs user authentication, while a generic cryptographic system can still handle the other components of containment. Thus, in such systems, a cryptographic key is stored as part of a user's database record, together with the user name, biometric template, access privileges, and that is only released upon a successful biometric authentication. This method of integrating biometrics into a cryptosystem is referred as the method of biometric- based key release. The characteristics of the biometric key release system design are: it requires access to biometric templates for biometric

matching and user authentication and key release are completely decoupled. A schematic diagram of this configuration is shown in **Figure I.5** [11].

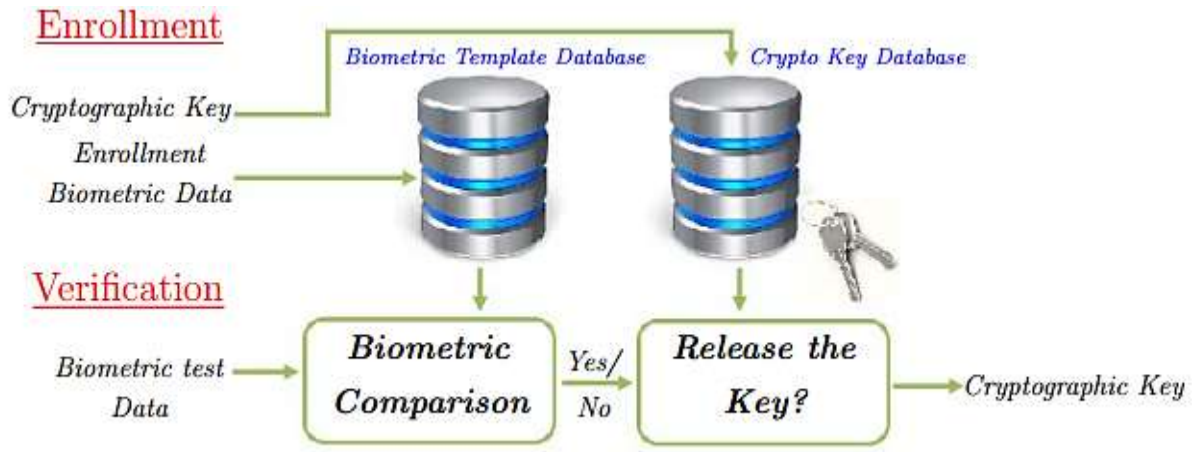


Figure I. 5 : key Release based on biometric [9]

I.5.2 Key Binding Biometric cryptosystems

When secure sketch is obtained by combining cryptographic key which is independent of biometric features with biometric template, it is referred as key binding biometric cryptographic systems such as Fuzzy Vault and Fuzzy commitment algorithms. This involves hiding the cryptographic key within the enrollment template itself via a trusted (secret) bit-replacement algorithm. Upon successful authentication by the user, this trusted algorithm would simply extract the key bits from the appropriate locations and release the key into the system. Unfortunately, this implies that the cryptographic key will be retrieved from the same location in a template each time a different user is authenticated by the system. Souter et al [11].

Proposed biometric encryption algorithm using image processing. This algorithm binds a cryptographic key with the user's fingerprint images at the time of enrolment. The key is then retrieved only upon a successful authentication. Thus, if an attacker could determine the bit locations that specify the key, then the attacker could reconstruct the embedded key from any of the other users' templates. If an attacker had access to the enrollment program then he could determine the locations of the key by enrolling several people in the system using identical keys for each enrollment. The attacker then needs only to locate those bit locations with common information across the templates [11].A schematic diagram of this approach is shown in **Figure I.6.**

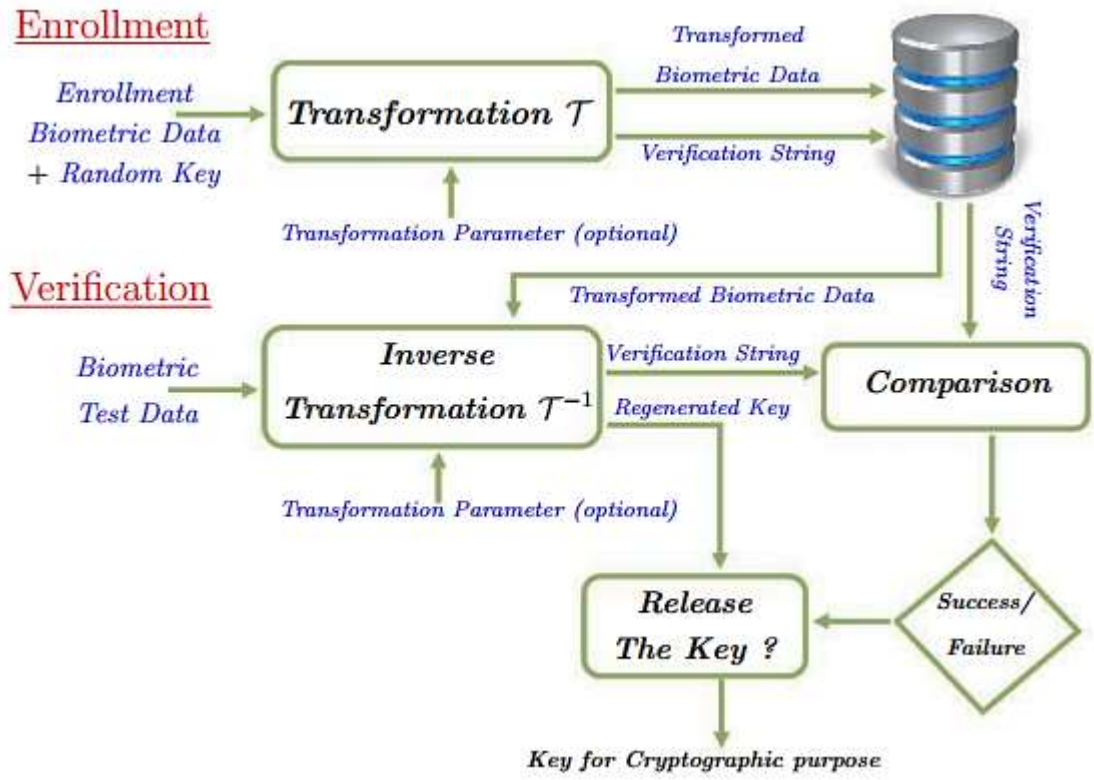


Figure I. 6: cryptographic key binding using biometrics [9].

Hereafter we will give a brief overview on the well-known biometric-cryptosystem based key binding schemes which are the fuzzy vault and the fuzzy commitment:

I.5.2.1The fuzzy vault schemes:

Proposed by Jules and Sudan the hard-ness of this scheme is based on the difficulty of polynomial reconstruction problem. During enrollment, a user selects a polynomial $f(x)$ and encodes his cryptographic key k into the polynomial's coefficients. The encoding of k can be achieved by dividing k into non-overlapping chunks and mapping to the coefficients. For a given set of features$x \in < N$, the polynomial $f(x)$ can then be evaluated at each element $x_i$andstore all pairs of $\{(x_i, f(x_i)), i = 1 \ldots N\}$ as the genuine set G. The users then generate a random set of chaff pairs$C$, and merge with the G set to generate the final vault. The pairsin C do not lie on the polynomial. Within the final vault, the points are not known whether they belong to set Gor C. At verification, only when the biometrics representation of the authenticator has substantial overlap with the enrolled user, the pairs lying on the polynomial can be identified and the key can be reconstructed [12]. (See **Figure I.7**)

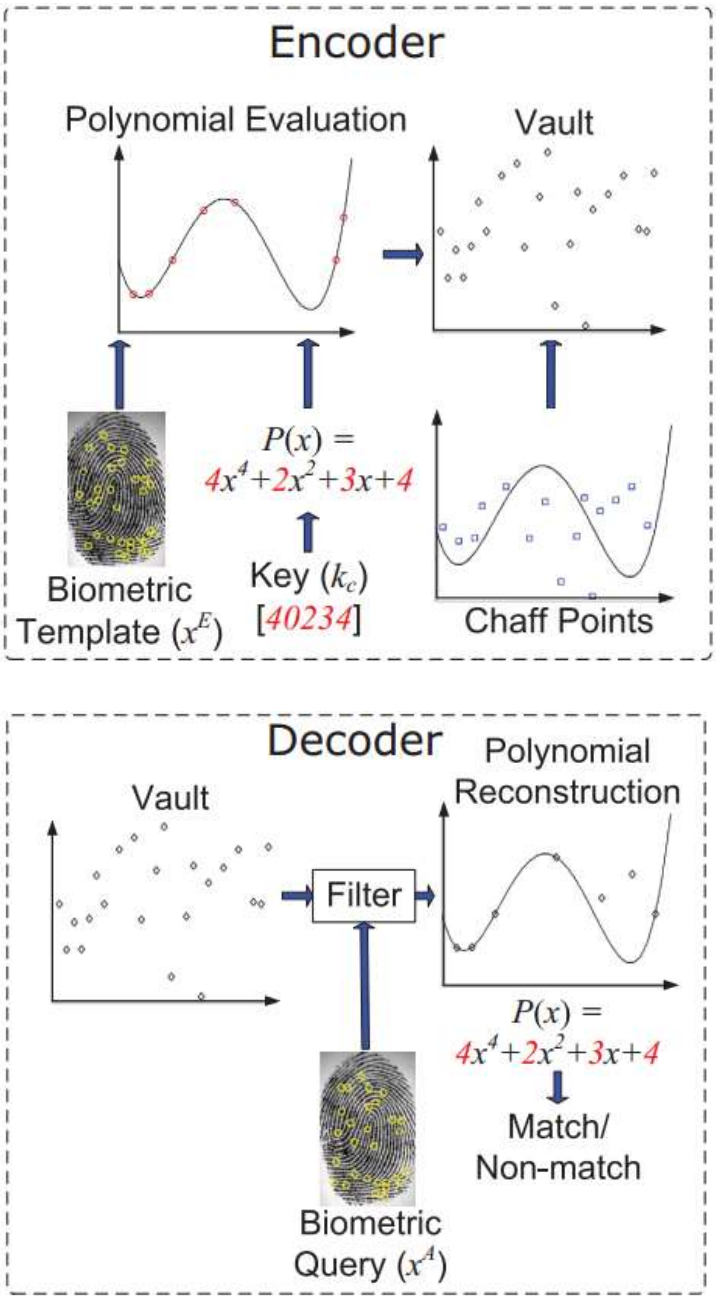
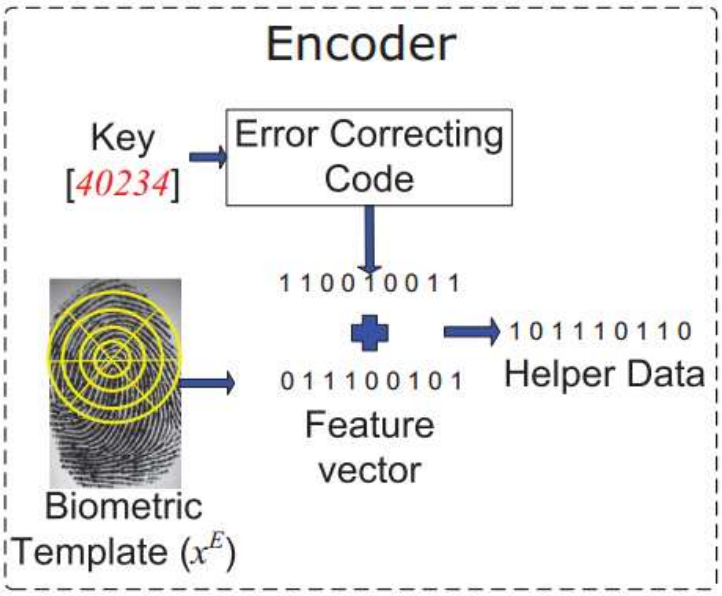


Figure I. 7 : Typical fingerprint Fuzzy vault Encoding and decoding [9]

I.5.2.2 The fuzzy commitment scheme (FCS):

Was proposed by Jules and Wattenberg in 1999. One branch is to combine the biometrics and cryptography. Fuzzy commitment scheme is one of the pioneer and effective security primitives. Using the generated binary feature as input and based on fuzzy commitment scheme, author constructed the biometric cryptosystems. A biometric template must be in the form of an ordered bit string of a fixed length. A key is mapped to an (n, k, d) Error Correcting Code (ECC) codeword of the same length,n as the biometric template. The code word and the template are XOR-ed, and the resulting $n - bit$ string is stored into helper data along with the hashed value of

the key. On verification, input biometric template is XOR-ed with the stored string, and the result is decoded by the ECC. If the code word obtained coincides with the enrolled one (this is checked by comparing the hashed values), the$k - bit$ key is released. If not, a failure is declared.In fingerprint's recognition system, minutiae feature is most distinguishable, but it cannot be used directly with FCS naturally. It can be transformed into binary string from minutiae points. Fuzzy commitment scheme is a smart biometric cryptosystem framework which can deal with hamming errors happening between different biometric samples. It demands for the binary length-fixed biometric feature b input into the system. Code word c is randomly selected. Encrypted template is : $e = b \oplus c$($\oplus$is XOR). Using hash function$h(c)$ is taken to store along with e. In decoding phase, query biometric b' is XORed with e to gete'. It is computed as, $e' = b' \oplus e = b' \oplus b \oplus c$. By decoding$e'$, codeword c' is obtained. Now, if query image is same as stored biometrics and within a certain threshold in terms of hamming measure, we can say ,$c = c'$. This can be validated by checking $h(c) = h(c')$[13]. (See **Figure I.8).**



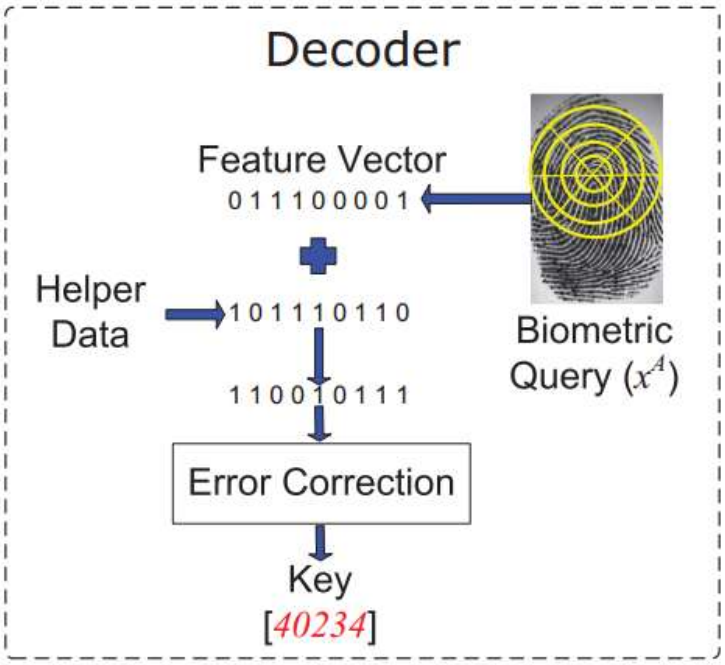


Figure I.8 : Typical fingerprint Fuzzy commitment Encoding and decoding [9].

I.5.3 Key Generation Biometric-cryptosystems:

If secure sketch is derived only from the biometric template and cryptographic key is directly generated from helper data and query biometric features, and then it is called key generation biometric cryptosystems. Such as Secure sketch and Fuzzy extractor. The data is derived directly from a biometric image. However, there are two main problems with this method. First, as a result of changes in the biometric image due to environmental and physiological factors, the biometric template is generally not consistent enough to use as a cryptographic key. Secondly, if the cryptographic key is ever compromised, then the use of that particular biometric is irrevocably lost. In a system where, periodic updating of the cryptographic key is required [11]. a schematic diagram of this approach is shown in **Figure I.9.**

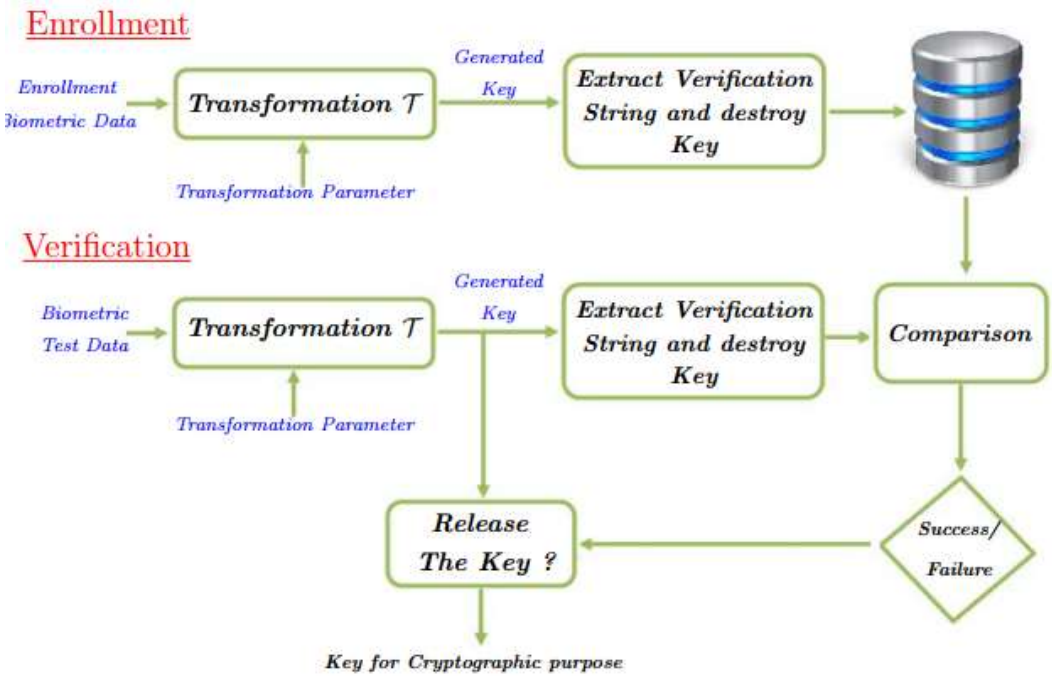


Figure I. 9: cryptographic key generation from biometrics [9]

I.6 Conclusion

In this chapter, we have chiefly described the general context of information security by describing the cryptography, biometric, and different biometric-crypto systems categories. Also point out the biometric crypto system and its keys. The information security is all about the protection of digital assets, such as digital content, personal health records or a secret personal document.

In the next chapter we are intended to focus our study on the second scheme of biometric crypto system which is the key binding-based algorithm. We will try to design an e-application system namely e-banking.

CHAPTER II

An e-banking scheme based Biometric-Crypto system

Chapter I: Information Security Strategies

Chapter II: An e-banking scheme based biometric-cryptosystem

Chapter III : Experimental results and discussion

II.1 Introduction

The financial institution, such the bank, is one of the societies whose started using internet as a distribution channels for their services. Thus, such online Bank service is called e-Banking. .In order to construct an e-baking system, many challenges can occur and oppose the electronic banking services. Those challenges are concerned with the information security and privacy. However, it is not enough for an e-banking system to just provide information to their customers but to provide it to the right customers and at the right time. One of the main means to guarantees such a secure communication between the bank and their customers is cryptography. Generally, the keeper of the cryptographic key must be a legitimate user and for a security reason the key is constructed to be too long. Hence, it would clearly not be feasible to require the user tore member and enter the key each time when required. As a solution to over comes those drawbacks, many researchers propose to combine cryptography with a powerful mean that grantees identity called Biometric. The resulted system is called Biometric-Crypto system.

In this chapter we will focuses on the construction of a secured e-banking system in term of conception and security analysis. Firstly, we are going to talk about the architecture of the biometric system. Then a brief discussion of the proposed e-banking system will be presented. Finally, this chapter will be concluded by a conclusion.

II.2 Biometric system architecture

A typical biometric system is constituted of four principal modules (see **Figure II.1**) [14]:

A. Biometric sensor: It is responsible for capturing the biometric characteristics from the biometric subject and converting it to a digital form to be transferred to the subsequent module. The performance of the overall process depends heavily on the quality of the acquired raw data. In fact, this data is a result of transforming a real continuous phenomenon (such as a face) to a digital discreet form (face image) resulting in a loss of data. The quality of the acquired data depends on the technology of the reader, the added noise and the degree of the interoperability of the user with the system.

B. Enrollment: The acquired raw data is first preprocessed to enhance its quality. After that, some relevant discriminatory features are extracted, by the extractor sub-module, to generate a compact representation called “template” that efficiently resumes the biometric characteristics. The generated template is then sent to the storage system. Generally, the

enrollment step allows the biometrics recognition system to learn the identities of the authentic persons in working environment.

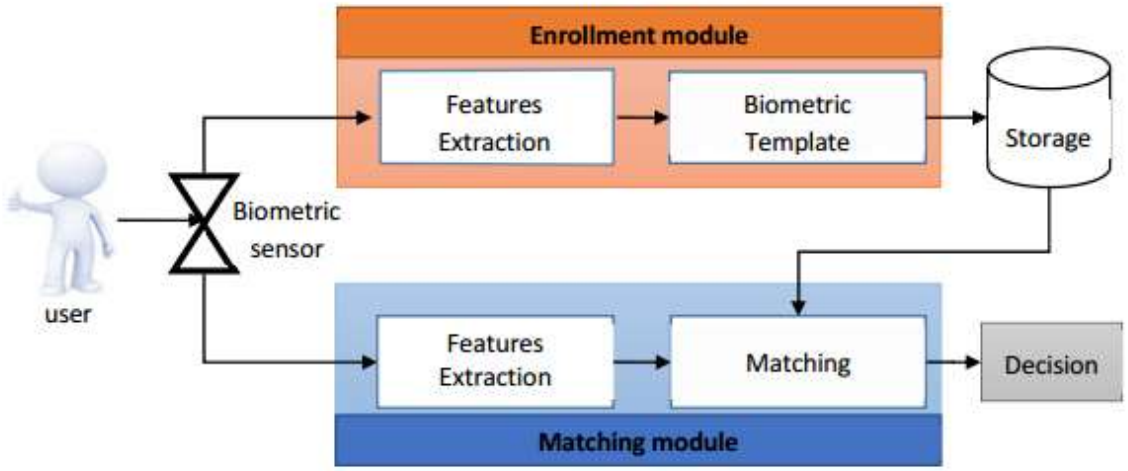


Figure II. 1: Atypical biometric system architecture [14]

C. **Storage systems:** the storage system can be a simple file in a simple smartcard as it can be a big database managed by database (DBMS) in association with the generated template, some biographic information (name, passwords, address, etc.) can be stored. In any case, the important factor to deal with is the security of the stored template. A compromised template can help to reconstruct the original biometric characteristics, which constitutes a real threat.

D. **Matching module:** during the operating phase, the system is requested to identify a person. It proceeds to extract his discriminatory features using the extractor sub-module in the same manner that it has been done in the enrollment step. These extracted features are called query features. After that, the stored template is revoked to be compared with the query. The comparison aims to confirm that both the query and the template features originate from the same biometric subject (person). Generally, the comparison result is a degree of similarity suitable decision about the identity of the user. On the other hand, the biometric system can operate either in verification or identification mode. In verification mode, the comparison is made only against one template in the system by conducting 1 to 1 comparison. This is possible when we want to confirm the identity claimed by a user. In the identification mode, the comparison is achieved against all records in the database by conducting 1 to many comparisons. This is the case when we want to know if the individual already exists in the database. So, the system tries to answer the question **"who is the user?".**

II.3 Feature Extraction Techniques

In this section, we are going to talk about the used feature vector descriptor that is used to extract an appropriate feature. The choice of those features descriptors is depending on their performances in the biometric feature extraction task. For this reason, a Gabor filter response with a binarization thresholding is chosen to extract the principal line of the biometric traits.[9]

II.3.1 Gabor filter response overview

Gabor filter, Gabor filter bank, Gabor transform and Gabor wavelet are widely applied to image processing, computer vision and pattern recognition. Thus, for applications requiring orientation analysis, Gabor functions produce very useful wavelet decomposition. Gabor filters can be used to extract components corresponding to different scales and orientations from images. Hence, the circular Gabor filter can represent by the following general form [9]:

$$h(x,y) = \frac{1}{2\pi\sigma^2} e^{-\{(x^2+y^2/2\sigma^2)\}} e^{2\pi i\mu(x\cos\theta + y\sin\theta)} \quad \text{(II.1)}$$

Where:

- $i \quad = \sqrt{-1}$.
- μ Is the frequency of the sinusoidal signal.
- θ Control the orientation of the function.
- σ Is the standard deviation of the Gaussian envelope.

The Gabor filter application requires an empirical choice of filter parameters (θ, μ, σ). These empirical parameters are very difficult to determine and this is one of the drawbacks of approaches based on this filter.

- **Feature vector generation:** Most biometric systems do not directly compare the acquired raw data. Instead, different mathematical methods are used to reduce the raw data, but with preservation of the essential information that makes it possible to characterize two images. The Gabor filter representation of an image I is the convolution of this image with the Gabor filter, defined by:

  $$I_G(x,y) = h(x,y) * I(x,y) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} h(m,n) I(x-m, y-n) \quad \text{(II.2)}$$

Where * denotes discrete convolution. As the Gabor filter has a complex formula, it is important to use the information given by the real part and those given by the imaginary part of the Gabor coefficients.

The Gabor features vector should be binarized by a proper threshold value in order to generate a new feature vector. It is important to find the proper threshold value in order to separate the lines from input image. Finally, the feature vectors are obtained by:

$$F_X(i,j) = \begin{cases} 1 & if V_X(i,j) \geq T_X \\ 0 & otherwise \end{cases} \quad \text{(II.3)}$$

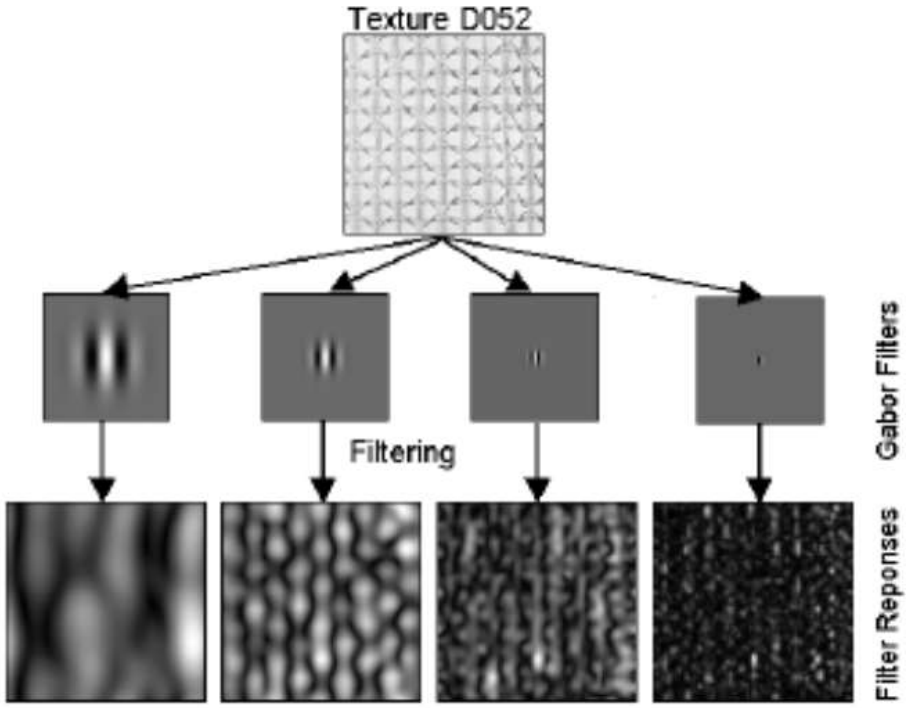


Figure II. 2: Texture features extraction using Gabor filter.

II.4 Proposed biometric crypto system

The main objective of this part is to design and develop a secured e-banking system. The proposed system uses symmetric cryptographic and multi-factor authentication methods. Authentication methods that depend on more than one factor are more reliable and stronger fraud deterrents. Accordingly, in our system, customers authentications are based on a card combined with a PIN and a biometric trait (PLM modalities). The proposed e-banking transaction scheme based on multifactor authentication is shown in **Figure II.3** [15].

Figure II. 3: E-banking transaction services model based on multi-factor authentication**.**

In the literature, a wide range of techniques have been presented based on the combination of biometrics and cryptography, in order to cope with both problems: variability of biometric templates and protection of personal data in our scheme (see figure II.4), a fuzzy commitment technique is used. Thus, in the customer terminal and after the preliminary verification, using the customer card and the card PIN code, a feature extraction technique is applied on the biometric modality (PLM) in order to extract a discriminate feature vector (m). Then, a fuzzy commitment scheme (where a secret message (encryption key, c), is protected using the extracted vector (m)) is applied. In this case, an error correcting code is used in order to associate the encryption key c with a person and to compute an offset μ such as:

$$\alpha = \tilde{c} \oplus m \qquad \text{where} \qquad \tilde{c} = [c; c; \cdots c] \tag{II.4}$$

Where the length of $\tilde{c}$is equal to the length of the extracted vector m. The encrypted message (the fuzzy commitment) is then represented by the pair (α, h(c)), where h(c) is a one-way hash function. It is worth to notice that neither the biometric feature, nor the associated code words are publicly transmitted. Finally, the terminal device sent the encryption transaction (Ṡ) data and the pair (α, h(c)) to the bank. In the bank, the authentication process is correctly $\tilde{c} = \alpha \oplus m$ sufficiently close to c so that the code decodes it to c and the comparison between their hash values succeeds. In this case, the bank can decrypt and treat the transaction data (S) and send confirmation information to the costumer.

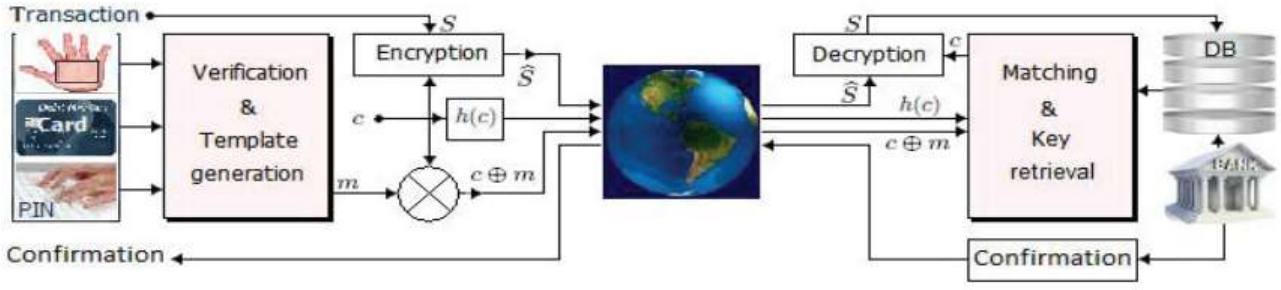


Figure II. 4: Basic block diagram of e -banking transactions system.

II.4.1 Proposed methodology

In each e-banking transaction, there are two parts for the application. One is a customer terminal and the other is for bank server (administration). The customer request is sent over the network in an encrypted data format (transaction data). Thus, the administrator (bank server) has to decrypt the transaction data sent by the customer terminal which is in the encrypted format and also verifies the integrity of the received data.

II.4.1.1 Enrollment phase

For each costumer, during the enrollment process, the feature vectors (or template) is generated from their PLM biometric modalities and stored for later use (identification process) in a costumer's identification server as well as in the costumer ID smart-card. In addition, a PIN code is randomly generated and stored in this smart-card. However, the PIN code is used for security purposes and to authenticate the user in the electronic transaction device (e.g. PC or smart-phone).

II.4.1.2 Customer terminal

As the first part of the e-banking transaction process, verification and template generation are the foundation on which the card PIN code is verified, if it is true, the feature extraction technique is applied on the user PLM modality for generate the template (feature vector), see **Figure II.5.** On the other hand, if the card PIN code does not match with the card, the user access is denied.

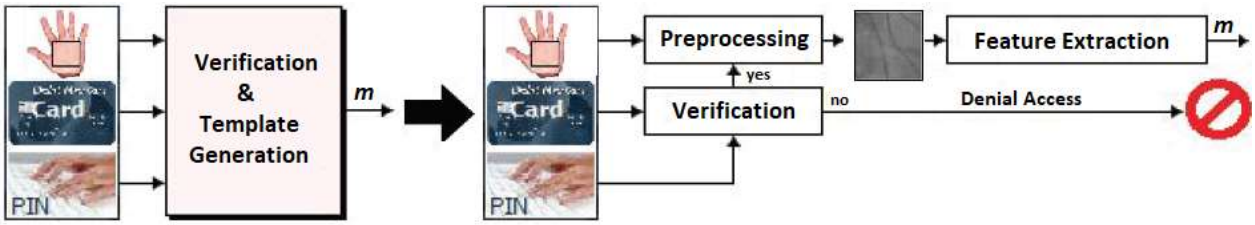


Figure II. 5: Flowchart of access verification and template generation process in customer terminal.

One of the most critical problems in the pattern recognition is the selection of suitable characteristics for a compact and optimal representation of the image. Thus, several methods for extracting texture features, which are based on the spatial relationship between pixels, have been proposed over the years. Among them, the Gabor filter response method, recently developed, provides a powerful descriptor of texture whose results are superior, in terms of the accuracy and the computational complexity in many applications.

II.4.2 Bank server

The second part of the e-banking transaction process consists of the customer authentication and the key retrieval process. **Figure II.6** shows the flowchart of customer authentication and key retrieval process in the bank server. The main modules in this part consist of the key retrieval and the feature matching process.

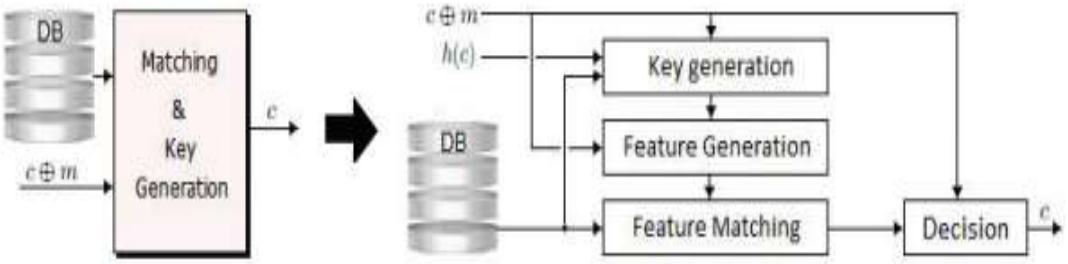


Figure II. 6: Flowchart of customer authentication and key retrieval process in the bank server.

- **Key retrieval:** The key retrieval process in the bank server is illustrated in **Figure II.6**. The system requests the user template from their database. Then, the binary representation of the user template (ḿ) is XORed with the binary string α. ($\tilde{c} = \alpha \oplus$ ḿ)Now, the key can be recovered. To achieve that, bits of binary vector are mapped into matrix M x (with size of k × v , where k represent the key length and v is the number of key within c̃1) and the key retrieval is performed by taking the majority vote among M x. After that, to check whether the retrieve key (ć) is identical to the key generated (c) in the customer terminal, the system checks to see whether h(c) = h (ć). It is important to notice that, the success of the key retrieval process is as function of the intra/interclass variations of the genuine user's template. So, it is very necessary to use an efficiency feature extraction technique which decreases the intra-class variability and increases the inter-class variability.
- **Feature matching:** In biometrics, it is very likely to find persons having almost the same biometric features (very low inter-class variability), so it is possible to retrieve the encryption key in the impostor users' templates. For that, an authentication module after the key retrieval is necessary to accept or reject this key. However, in this module, before the feature matching process, the user template must be generated.
- **Message decryption step:** Our scheme decrypts confidential data (transaction data) that has been encrypted using biometric data combined with random numbers (encryption key). As a result, confidential data can be decrypted just with the costumer biometric data (stored in central system database); however, the need for a proper and reliable key management

mechanism is required in order to confirm that the listed keys actually belong to the given costumer. Indeed, the central system uses key recovery algorithm to disassemble the encryption key (c) from the feature vector and then to decrypt transaction data (S) and authenticate the costumer.

$S = F^{-1}(\hat{S}, c)$(II.5)

Where S is the original costumer data, $\hat{S}$, is the encrypted voter data, c is the key and F^{-1} denote the decryption function.

II.4.3 Multimodal System

Using a single modality in a biometric system may often lead to some errors in verification/identification. So, the data fusion technique can be used to improve the performance of the unimodal biometric system. In our work, the PLM&PLV modalities is fused at the matching score level, which isthe most effective scheme compared to the sensor, features, and decision level. For a serious judgment on our e-banking system, the included biometric identification system must be evaluated under several lengths of the encryption key. Because our multimodal biometric system uses two biometric modalities, two ideas for embedding the key are tested. First, the encryption key is combining, at the same time, with the two feature vectors given by PLP and PLV (Separated key).So, encryption key can been retrieved by [16]:

$$c = \begin{cases} \tilde{c}_{GL} & \text{if} \quad h(c) = h(\tilde{c}_{GL}) \\ \tilde{c}_{NIR} & \text{if} \quad h(c) = h(\tilde{c}_{NIR}) \\ \tilde{c}_{GL} \quad or \quad \tilde{c}_{NIR} & \text{if} \quad h(c) = h(\tilde{c}_{GL}) = h(\tilde{c}_{NIR}) \end{cases} \quad \text{(III.6)}$$

Where the $\hat{C}_{GL}$is the retrieved key from the GL based palm print representation and the $\hat{C}_{NIR}$ is theretrieved key from the NIR representation. Whereas, in the second scheme, each template (for eachrepresentation) contains a different key. Thus, in this case, the entire encryption key is given by the concatenated of the two extracted keys, as follow:

$$C = [\hat{C}_{GL} \quad , \quad \hat{C}_{NIR}] \quad \text{(III.7)}$$

It is important to note that, the first scheme is dedicated for the small to medium length key, whereas, the second scheme for the greater length key.

II.5 Security Analysis of Biometrics Cryptosystems

In the last section, the Biometric-Crypto system is revealed to solve the problems related to both biometric and cryptography. So, the biometric-crypto systems are supposed to increase the security, and therefore, it is required to carry out theoretical as well as experimental security analysis of such systems. On this regard, when we talk about the security analysis of those systems, we must take into consideration that the design of the Biometric-Cryptosystem mustn't decrease the biometric system based identification performance, this is on one hand. On the other hand, the constructed system must also robust on each kind of attacker based key retrieval. Hence, two security scenarios are considered: stolen biometric: when the biometric data for all the users are compromised; and stolen key: when the secret keys of all the users are compromised. As that one of our main research, during the realization of this thesis, is the design of the Biometric-Crypto system. An analysis of such metrics rates is required. Those metrics include FRR (GAR), FAR and EER or the ROR and RPR for the closed-set identification based applications as well as a security analysis depending on the secrecy of cryptographic keys. This will be performed by calculating a genuine key retrieval rate and the impostor based key retrieval rate [9].

II.6 Conclusion

The objective basic of this chapter is, to introduce and design the biometric system structure, the feature extraction technique, and the proposed biometric crypto system. In addition of the main and important topic, how it works service e-banking with the biometric crypto system.

The biometric cryptosystem, which combines biometrics and cryptography, may provide another effective method to protect people‘s sensitive information, especially in the service e-banking to ensure the convenience of users of this service.

In the next chapter will explain the practice how it works the service e-banking with biometric cryptosystem.

CHAPTER III

Experimental results and discussion

Chapter I: Information Security strategies.
Chapter II :An e-banking scheme based Biometric-Crypto system

Chapter III : Experimental results and discussion

III.1 Introduction

Nowadays, the internet becomes very vital for any kind of information exchange. One of the applications which can use internet for information exchange is Online banking (e-banking). Indeed, e-banking has several advantages like the accessibility for the disabled and elderly; the ease of long-distance banking; the low costs and the greater customer's turnout. Thus, the challenges that oppose e-banking application are the concerns of security of transmitted data which are exchanged as well as the privacy issues (customers information), which ensure the secrecy of customers information.

In this chapter of experiment, we propose a secure Biometric-crypto scheme dedicated to online e-banking system. The fuzzy commitment concept associated with the palmprint (PLM) modality is the core of our system. In this part of study, to enhance the discriminating capability of the PLM feature vectors, we suggest the use of GABOR descriptor with binarization. This choice is justified by the high performances obtained with the use of this descriptor in term of accuracy and high genuine key retrieval rate. Subsequently, the customer's data is encrypted using a random key then this key is binding in the extracted feature vector using the fuzzy commitment scheme. Then, in the central system, a new scheme for the key retrieval is implemented in order to extract this key which used for decrypt the message and then treated.

III.2 The used biometric modalities: PLM and palm vein (NIR)

III.2.1 Palm print (PLM)

Palm print is one of the relatively new physiological biometrics, attracted the researchers due to its stable and unique characteristics. The rich feature information of palm print offers one of the powerful means in personal recognition. [17]

Palm print recognition has been introduced a decade ago. Palm is the inner surface of the hand between the wrist and the fingers. The Palm area contains a large number of features shown in the **Figure III.1** that can be used as biometric features such as Principal lines, geometry, wrinkle, delta point, minutiae, datum point features and texture.

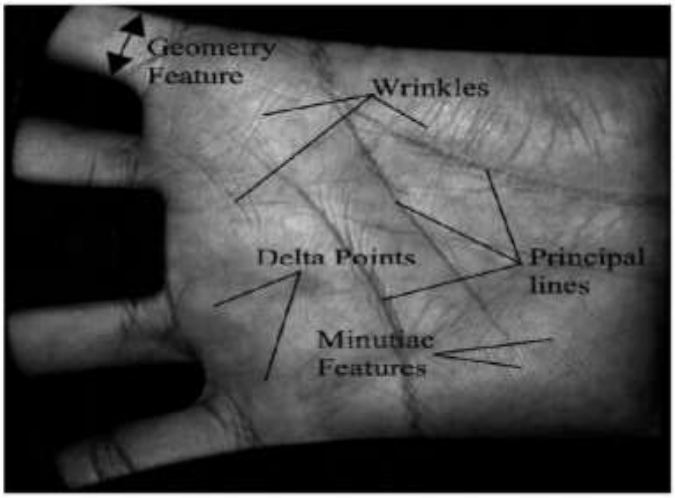


Figure III. 1 : Different palm print features [17].

III.2.2 Palm Vein (NIR)

Palm vein authentication uses the blood vessel patterns of the palm vein in the subcutaneous tissue of the human body to discriminate between individuals. Palm vein patterns are captured by the camera with near-infrared light. When a hypodermic vein is irradiated with near-infrared light, the reduced hemoglobin contained in the vein absorbs near infrared light and the hypodermic vein creates a shadow on an image. The shadow pattern is then extracted from the captured image of the palm vein pattern using image-processing technology. The resulting vein patterns are compared using vessel structure features such as directions and bifurcations, or by using the patterns themselves. In practical terms, palm vein patterns of a hand are used for authentication because such parts of the hand are easy to expose to a sensor.

The palm vein authentication technology has been deployed for its ease-of-use and assurance that it has given users through its robust security. It has been widely adopted worldwide for personal identification at financial institutions, as a computer login and room entrance control method at corporations.

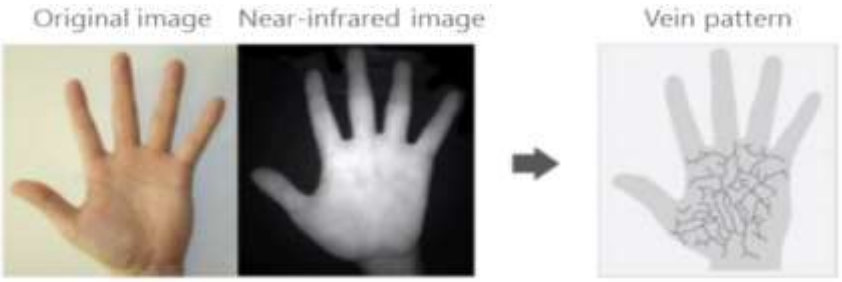


Figure III. 2 : Capture the Palm vein patterns.

III.2.3 Choice justification

Identification using palm print characteristics is a frequently used as biometric traits. The palm prints contain more information than the other modalities, so they are more discriminating. They contain additional distinctive features that can be extracted from low resolution images.

In the following table we have classified the different modalities according to the cost of use and their sensitivity to the physical and emotional state of individuals.

- **1st class:** DNA, Iris and Retina.
- **2nd class:** Face, Voice, Signature, Approach, Keystroke.
- **3rd class:** hand related Modalities.

Table III. 1: Biometric modalities classification

	1st class	2nd class	3rd class
Acceptability	↓↓	↑↑	↑↑
Permanence	↑↑	↓↓	↑↑
Identification rate	↑↑	↓	↑

According to the previous table, we have concluded that the modalities linked to the hand are the most suited to our requirement: permanent, very well accepted by individuals with an acceptable error rate.

III.3 Biometric Cryptosystem performance evaluation

III.3.1 Used Database description:

PolyU Multi-Spectral Palmprint Images Database

The database images that we used in our experiment are PolyU multi-spectral palmprint images. The Biometric Research Centre (UGC/CRC) at The Hong Kong Polytechnic University has developed a real time multispectral palm print capture device which can capture palm print images under blue, green, red and near-infrared (NIR) illuminations, and has used it to construct a large-scale multispectral palm print database. [18]

PolyU contains Multispectral palmprint images were collected 300 individuals using a palmprint images; Experiments are performed on the Hong Kong PolyU multi-spectral palm print database. This dataset can be considered as an example similar to the number of voters in small to medium

size office. In all experimental results, two image representations are used, the first representation (Gray Level-GL), is constructed from the red, green and blue bands, and the second representation is the Near-Infrared (NIR) band. Thus, we randomly select three samples for each representation in order to construct the system database (enrollment phase). The remaining nine samples were used to test the system performance.

III.3.2 Adaptation of parameters

III.3.2.1 Work Environment

In this section, we present the hardware and software environments of our work.

- **Hardware environment**

In order to carry out this project, a set of equipment has been made available to us, the characteristics of which are as follows:

A TOSHIBA-PC computer with the following characteristics:

→ Processor: Intel (i3) Pentium (R)

→ RAM: 4.00 GB of RAM.

→ Hard Disk: 750 GB.

→ OS: Microsoft Windows 7(32bits).

- **development tools**

In order to successfully complete this project, we have used MATLAB 2014a during the development of our system, which we will present below.

MATLAB 8.3 (R2014a) and its interactive environment is a high-level language that allows the execution of tasks requiring great computing power and whose implementation will be much easier and faster than with traditional programming languages. It has several toolboxes in particular that of image processing "Image Processing Tool Box" which offers a set of algorithms and reference graphics tools for the processing, analysis, visualization and development of image processing algorithms.

III.3.3 Assessment protocol

Accordingly, the aim of this part of experiments is to design a key binding based Biometric-Crypto system using those two previous representations in order to choose which representation is

better to be used in the Biometric-crypto system design. Our experimental results can be divided into three parts; it must firstly select the best parameter (the binary threshold used in the feature extraction method). We decompose our set of experiments into three parts. As a first part, we evaluate the biometric system without the encryption key and with several binarized threshold in order to choose the best threshold giving the best performance. in the second part, we integrate the biometric system in our proposed e-banking scheme and we re-evaluated this system as well as the key retrieval process with several lengths of the cryptographic key (32 bits to 512 bits by a step of 32 bits). Finally, in the last part of those tests we use unimodal biometric systems.

Among the important tasks at any pattern recognition scheme, the feature extraction task has an important impact on the system accuracies. In our tests and based on PLM and PLV modalities, we execute several experiments by varying Tth for selecting the best threshold of binarization. Because our feature vector depends essentially of the mean value of the module response of the filtered image (ρ) and a parameter (n). Therefore, we can vary the parameter$n$and compute every time the system accuracy. Based on these accuracies of the system, we can empirically select the n, which can be effectively enhancing the feature vector. Therefore, in our study, we used seven values of n varying from 1 to 2 by a step of 0.1, See Table III.2.We compute the identification rate for each value of$n$and choose the value that gives the best rate (maximum rate).

Table III. 2: Binarization Threshold selection

Threshold	ROR
1.0	**99.85%**
1.2	**99.81%**
1.3	**99.88%**
1.4	**99.88%**
1.5	**99.71%**
1.6	**99.67%**
2.0	**95.65%**

The aim of the first experiment is to find the threshold that optimize the performance of the proposed biometric system by giving the highest value of ROR, for that different values of the binarization threshold was tested and evaluated. From table III.2, one can observe that the

threshold at **1.4**gives the best performance. Consequently, we will fix the binarization threshold at this value for the next experiments.

III.3.4 Biometric-Crypto system evaluation without key insertion

- **unimodal system test results :**

  The aim of the first experiment is to evaluate the system performance without key insertion when we use our proposal descriptor (Gabor filter). Thus, in our e-banking scheme, before using the proposed biometric system in a biometric-crypto protocol, it must firstly evaluate to test the efficiency and robustness of this proposed methodology.

After we found the best parameters, we will use the feature extraction method in the other Unimodal systems (GL, and NIR) in n the two identification modes, ***open-set***, and ***closed-set***.

- For ***open-set*** we measured Equal Error Rate (EER) and Threshold (T0).
- For ***closed-set*** we measured Rank-One Recognition (ROR) and Rank of Perfect Recognition (RPR).

Table III. 3: PLM based Unimodal Test Result.

Band	Open set identification		Closed set identification	
	EER	**T0**	**ROR**	**RPR**
Grey level	0.0370	0.2109	**99.8889**	123
Finger vein (NIR)	**0.0218**	0.1812	99.5555	8

The second part of experiment is the evaluate the performance of the biometric cryptosystem without key insertion in order to see if the insertion of the cryptographic key affect the performance of the system or no. However, a series of experiment were conducted where two representation of the palmprint modality were used. The GL (grey level) representation constructed from three bands (Red, Green, Blue) and Near infrared (NIR) representation. The obtained result for both identification modes was plotted in Table III.2. The analysis of the open-set identification performance shows that the NIR representation gives the best results in term of EER by giving an EER equal to **0.0218**at the threshold **T0=0.1812**. The use of GL representation gives an **EER= 0.0370**with a **T0= 0.2109**.

Finally, a ROC curves for the two representations which plot the FRR against FAR is illustrated in **Figure III.3**.

For the closed-set identification mode, it seems that the GL representation achieve the best performance by giving a ROR equal to **99.8889%**with an RPR equal to **123**. The NIR representation gives a **ROR=99.55%**with an **RPR=8**. The performance of the closed-set identification was plotted as a CMC curves as shown in **Figure III.4.**

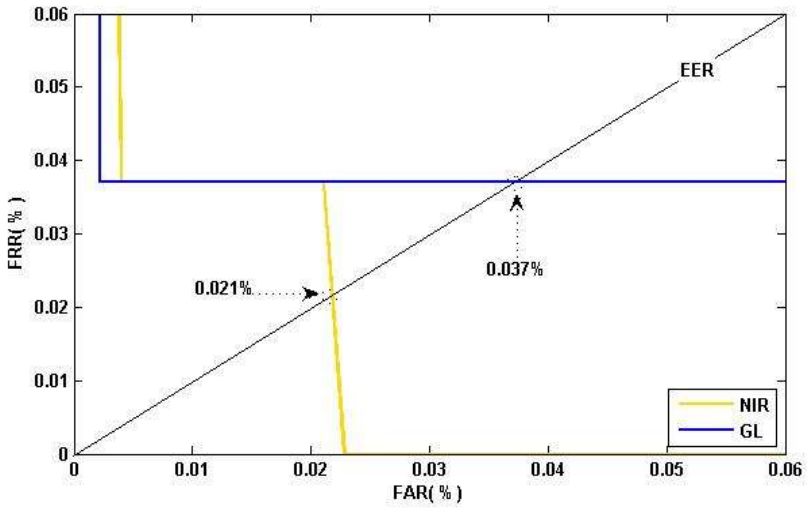


Figure III. 3:ROC curves (FRR against FAR) for the two representations**.**

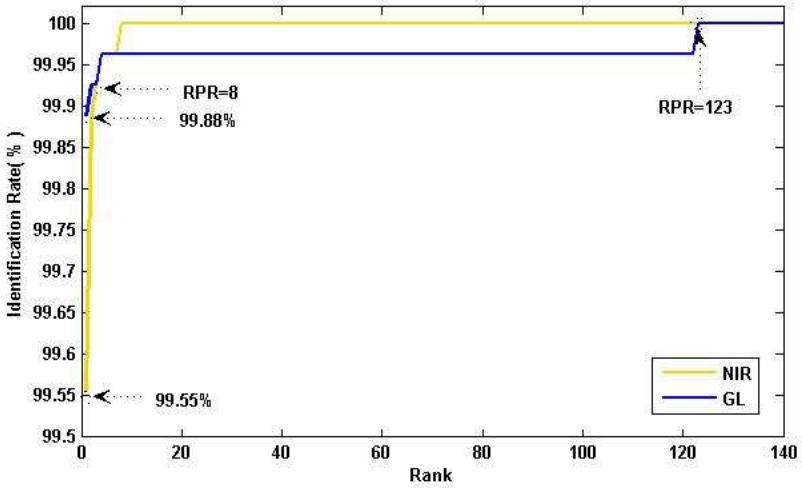


Figure III. 4:CMC curves, identification rate against Rank for the two representations.

III.3.5 Biometric-Crypto system evaluation with key insertion

In our scheme, the generation process seamlessly binds a random key, generated independently of the customer at the customer terminal, into the customer biometric template in such a way that both the cryptographic key and biometric template are inaccessible to the attacker while the

cryptographic key can be released in the bank server upon valid presentation of the customer biometric template (previously stored in the bank database). This method offers both conveniences, as the user no longer has to remember a cryptographic key (pass code), and secure identity confirmation, since only the valid user can release the key.

- **Unimodal based biometric cryptosystem test results**

the embedding of the cryptographic key into the biometric feature vector (at the terminal system), it is basically that this feature vector can be affected by some noise after extracting the embedded cryptographic key (at e-banking system) which affects, off course, the performance of the identification system. To study this purpose, in this part, we evaluate the unimodal based biometric cryptosystem under several key lengths.

Table III. 4: GL based Biometric-Crypto system performance evaluation

Key size	Open set identification		Closed set identification		Genuine key retrieval rate	Impostor key retrieval rate
	EER	T0	ROR	RPR		
32	0.0370	0.2565	99.6667	14	100	99.9782
64	0.0370	0.2565	99.6667	14	100	88.2529
96	0.0370	0.2565	99.6667	14	100	99.6789
128	0.0370	0.2565	99.6667	14	98.7778	11.0903
160	0.0370	0.2565	99.6667	14	100	95.3881
192	0.0370	0.2565	99.6667	14	99.9630	57.0311
224	0.0370	0.2565	99.6667	14	99.9630	74.9018
256	0.0370	0.2565	99.6667	14	97.7037	3.0311
384	0.0370	0.2565	99.6667	14	95.2963	0.4127
512	0.0370	0.2565	99.6667	14	90.7778	0.0448

Table III. 5:NIR based Biometric-Crypto system performance evaluation

Key size	Open set identification		Closed set identification		Genuine key retrieval rate	Impostor key retrieval rate
	EER	T0	ROR	RPR		
32	0.0370	0.3182	99.8519	39	100	99.3517
64	0.0370	0.3182	99.8519	39	99.8519	66.1687
96	0.0370	0.3182	99.8519	39	100	97.1968
128	0.0370	0.3182	61.0891	39	96.8519	1.5100
160	0.0370	0.3182	99.8519	39	100	86.6394
192	0.0370	0.3182	99.8519	39	99.6667	33.0603
224	0.0370	0.3182	99.8519	39	100	61.0891
256	0.0370	0.3182	99.8519	39	95.1852	0.2792
384	0.0370	0.3182	99.8519	39	92.5926	0.0223
512	0.0370	0.3182	99.8519	39	87.8889	0.0017

Table III.4 and **Table III.5** present the performance of the unimodal GL and NIR based biometric cryptosystem in which the system retrieves the encryption key, then reformulates the template to compare it with the one stored. In order to see the behavior of the system, several key lengths are used. By analyzing the rates obtained, for the open identification mode, we can say that the performance of the biometric system is affected by the insertion of the encryption key. Thus, degradation becomes important in long keys. In general, regardless of the length of the keys, the performances obtained were closes to those obtained when the system was working without a key. GL based biometric system can operates with a ROR equal to **99.6667% (To = 0.2565)** and **99.8889% (To =0.2109)** for a template containing an encryptions keys and a template without key, respectively. Similarly, these rates become **99.8519 %** instead **99.5555%,** for the NIR based biometric system. To judge the effectiveness of the system, we must also consider the performance of the closed-set identification and the key retrieval process. In **Table III.4** and **Table III.5** also we illustrate as the key retrieval rates of NIR and GL based systems for various key lengths **32bits**to **512 bits** by step of 32bits. By reading in-depth theresults obtained in this tables, we observe that the maximum key retrieval rate is equal to **100%** for key size **32; 64; 96; 160**bits, for GL; and key size **32; 96; 160; 224**; **Table III.4**, show that the key retrieval rate is confined between**[87.8889 % … 99.6667%]** the lowest rate of key retrieval is obtained when a key of size 512 bits is used.

On the other hand, when the NIR representation is used. The first observation which can be made is that the lowest obtained key retrieval rate when the NIR representation is used becomes smaller **(87.8889%)** than the GL one at key size of 512bits **(90.7778%)**

For the other key size and from **Table III.4** and **Table III.5**, it can be seen that the system performance under the NIR representation is almost similar to the system performance when we use the GL representation with a slight superiority of the GL representation compared to the NIR based system performance. To summarize the genuine key retrieval rate under the two representations in terms of key sizes **Figure III.5**. Is plotted.

The second part discusses the impostor key retrieval rate under the two representations. it obvious that when the cryptographic key has a small size, the impostor guesses easily the key and its capability of retrieve the key is decreased when the key size length increase. Moreover, the impostor key retrieval rate under different key sizes is also cited in **Table III.4** and **Table III.5**, by a comparison between the results obtained in those two tables under the two representations, one can note the maximum impostor key retrieval rate is observed when we use a key size of length 32bits where the impostor can achievea**99.9782 %**of key retrieval rate under the GL representation. As for the NIR representation the maximum rate, the impostor can achieve a **99.3517%** of the key in the same key size. For the rest of key size impostor retrieval rate, one can observe that this rate when we use the GL images is among the interval of**[57.0311% 99.9782%]** and among the interval **[33.0603% … 99.3517%]** under the NIR images for the key size less than 224bit except the key size of rank 128 where the impostor key retrieval rate didn't exceed the **11.0903%**when the system is based on GL images and **1.5100%** for the NIR images. For the key greater the 224bits the rate become less then**3.1%** and balanced between **[0.0448% … 3.0311%]** under the GL representation and between **[0.0017% …0.2792%]** under the NIR representation. To see the performance of the proposed biometric-crypto system against the impostor attack, **Figure III.6**is made.

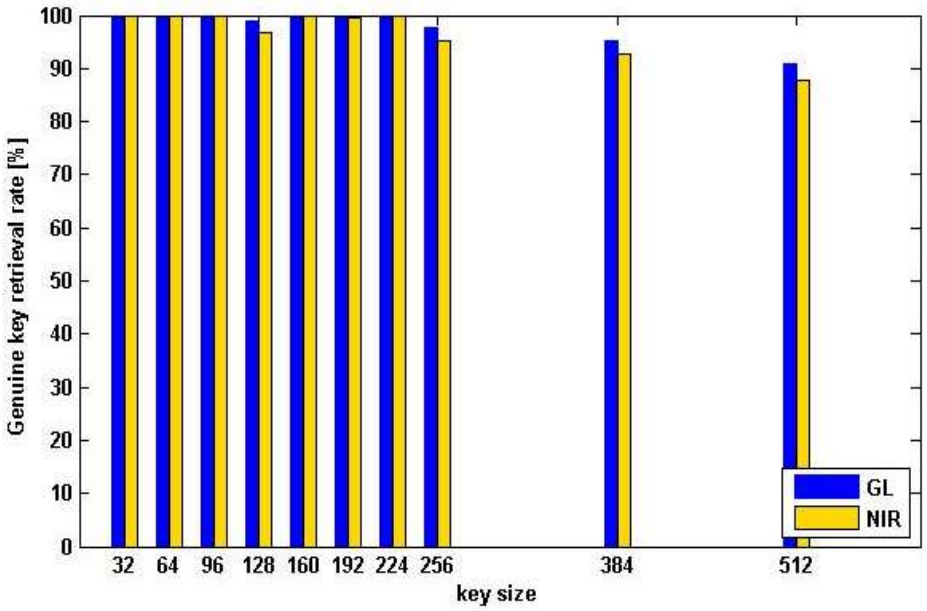


Figure III. 5: Biometric-Crypto system genuine key retrieval rate under the two representations GL and NIR with different key sizes.

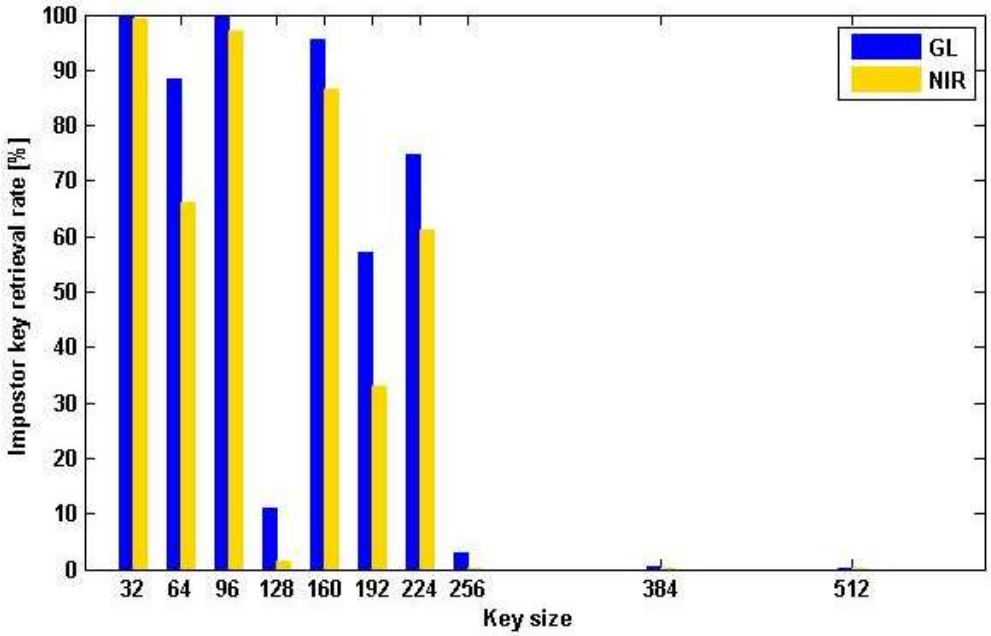


Figure III. 6: Biometric-Crypto system impostor key retrieval rate under the two representations GL and NIR with different key sizes.

- Multimodal Biometric-Crypto system evaluation

Several studies demonstrate the effectiveness of the fusion at matching score level. Thus, in this part, we use this scheme for a possible improvement of our proposed Biometric cryptosystem. In our test we use only then SUM-based rule for our fusion purpose. Each template for each representation contains a different key (Separated key). The obtained experimental results are

illustrated in Table III.7.For the proposed fusion scheme, the key is devised in the two representations. The obtained results are shown in Table III.7, from this table, the first note that appear from the result analysis is that the impostor key retrieval rate is reduced almost to zero where the rate varies between **[0%, 99.9767%]**which give this scheme a great influence on the system security. For the genuine key retrieval rate evaluation, the global key is the concatenation of the two extracted key. Table III.7 indicate a great improvement of genuine key retrieval especially in the case of key length of **256bits** which means a global key with size of 512 bits where the rate was **97.6296%** improvement of 7.59**%** compared with the best case obtained in the unimodal system **90.7778%**.Also, for the other key sizes, the rate is improved by the means of fusion process. The more the key is increased the more the rate is improved.

Due to the possible similarity of the biometric modality in many persons, the biometric feature vectors of these persons become very close, so that an imposter can retrieve the encryption key. In this case, the message can be decrypted. A minor probability that two different persons have similar of two PLM image representations GL and NIR, for that, using the biometric multimodality makes it possible to secure the encryption key.

Table III. 6: Biometric-crypto system based multimodal test results evaluation (Separated Key).

Key size	Closed set identification		Genuine key retrieval rate	Impostor key retrieval rate
	ROR	RPR		
32	99.6667	14	100	99.9767
64	99.6667	14	100	87.6678
96	99.6667	14	100	99.6316
128	99.6667	14	98.7407	10.0310
160	99.7407	16	100	82.8004
192	99.7407	16	99.6296	19.4745
224	99.7407	16	99.9630	46.5487
256	99.6667	14	97.6296	2.3882
384	99.6667	14	90.5556	4.9548e-04
512	99.7407	16	83.9259	0

III .4 Conclusion

The objective of this study is to develop a design model that implements the concepts of fuzzy commitment scheme based on palmprint biometrics to reduce risks of fraud and to improve customer's trust in online banking transactions. In this study, to enhance the discriminating capability of the palmprint feature vector, an efficient method of feature vector extraction which based on the 2D Gabor filter was used. After that, the transaction information is encrypted using a random key then this key is binding in palmprint (GL or NIR) modality of the bank using fuzzy commitment scheme and then transmitted to the bank. In the bank server, a new scheme for the key retrieval is implemented in order to determine the cryptographic key which used for decrypt the message and then treated. The analysis of the obtained experimental results, using a database of 300 users, showed that customers trust in security for e-banking can be increased by the proposed the proposed palmprint based biometric-crypto system scheme.

Conclusion

Technology and security are two criteria that go together according to a positive, progressive relationship. The higher and better the rapid performance of technology and electronic life, the greater the need to raise the level of security. Security is a growing imperative around the world because insecurity can lead to it Great damage. Physical security, personal security and information security are the main forms of security. In security, authentication means verifying that an individual has access to a system based on their identity. For several decades now, a user's identity has been verified through a traditional method (for example, password and smart card), which can be easily forgotten or stolen. However, a rapid upgrade in technology replaced the traditional method and a new system called the dynamic coding system was created. It is more secure and convenient as there is no need to memorize secret codes like password and it is hard to steal because it is based on unique human biometrics features.

it all started with the unimodal biometric system that uses a single biometric modality but given its many But with the development of time it had to be developed and exchanged with the multimodal biometric system that uses more than one biometric modality and as expected it has overcome many of the obstacles that the unimodal biometric system had like the universality and imposter attacks ...etc.

Our main goal was to design a biometric-crypto system. Literally, three ways can be found to integrate biometric with cryptography. So, we direct our research into the Key binding schemes based biometric-crypto system where the Fuzzy commitment scheme issued. The proposed biometric-crypto system is tested through a conception of an e-application namely e-banking system. In this architecture of biometric-crypto system, a binary template is required.by creating a multimedia model and unimodal system based on the capture of multi-specters images of the (GL)for the palmprint and (NIR) for the palm vein, an efficient method of feature vector extraction which based on the 2D Gabor filter was used. The obtained results showed that the insertion of the cryptographic Key didn't affect the biometric based identification system. The performance of the proposed biometric-crypto system was tested through the calculation of the genuine key retrieval rate and impostor key retrieval rate. The results obtained indicate that the system can achieve a 100% of genuine key retrieval rate in certain key size. Where the greater impostor key retrieval rate didn't exceed the 99% by using the lowest key size 32 bit and didn't exceed the 3% if the key size is greater than 224bit.

Bibliography

[1] Josh Fruhlinger. What-is-information-security-definition-principles-and-jobs.2020.https://www.csoonline.com article 3513899.

[2] https://www.geeksforgeeks.org/what-is-information-security/

[3] Sanjay Ganesh Kanade. \Enhancing information security and privacy by combining biometricswithcryptography,"Doctoralthesis.InstitutNationaldesTélécommunications, University of Evry Val of Essonne, Fance, 2010.

[4] Annapoorna Shetty, Shravya Shetty K, Krithika K"A Review on Asymmetric Cryptography – RSA and El Gamal Algorithm, "International Journal of Innovative Research in Computer and Communication Engineering, ISSN, pp.2320-9801, 2014.

[5] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 4 No. 05 May 2012.

[6] Swapna B Sasi, Dila Dixon, Jesmy Wilson, '' A General Comparison of Symmetric and Asymmetric "Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security'' IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719Vol. 04, Issue 03 (March. 2014), ||V3|| PP 01-04].

[7] Shilpa Shrivastava. Biometric: Types and its Applications. International Journal of Science and Research (IJSR)ISSN (Online): 2319-7064.

[8] Aleksandra Basic "Biometric Authentication. Types of biometric identifiers "Bachelor's Thesis Degree Programmed in Business Information Technology 2012

[9] M.KORICHI. "Biometrics and Information Security for a Secure Person Identification". Thesis Doctoral, KASDI MERBEH UNIVERSITY, OURGLA, 2019.

[10] Jing Dong .TieniuTan."Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations". National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O.Box 2728, 10190, Beijing, China.

[11] Jisha Nair.RanjithaKumari."A Review on Biometric Cryptosystems. RVS College of Arts & Science", Sulur, Tamil Nadu, India. International Journal of Latest Trends in Engineering and Technology (IJLTET)].

[12] V. Sujitha. D. Chitra .A REVIEW ON BIOMETRIC CRYPTOSYSTEM USING FUZZY VAULT. Pak. J. Biotechnology. Vol. 15 (Special Issue 1) Pp. 40-44 (2018) www.pjbt.org, PISSN: 1812-1837, EISSN: 2312-7791.

[13] Hubhangi Spakal, R RD esthumukh. “Biometric Template Protection with Fuzzy Vault and Fuzzy Commitment”, Government college of Engineering. Babasaheb Ambedkar Marathwada University, Aurangabad.

[14] Foudil Belhadj. Biometric system for identification and authentication. Computer Vision and Pattern Recognition [cs.CV]. Doctoral thèse. Ecole nationale Supérieure en Informatique Alger, 2017.

[15] Int. J. of Embedded Systems, Vol. x, No. x, 201X”Can Finger Knuckle Patterns Help Strengthen the E-banking Security?”Copyright 2016 Inderscience Enterprises Ltd.

[16] Abdallah Meraoumia1, Hakim Bendjenna1, Mohamed Amroune1 and Yahia Dris2
“Towards a Secure Online E-voting Protocol Based on Palmprint Features”
1Laboratory of Mathematics, Informatics and Systems (LAMIS), University of Larbi Tebessi, TEBESSA, 12002, ALGERIA. 2Management Sciences Department, University of TEBESSA, Algeria

[17] Mohammed Adnan BAHAZ & Mahdi Abdurrahman HAMZA, “Palmprint and Palm vein Recognition Based on Deep Lerning”, master memory, KASDI MERBEH UNIVERSITY 2018/2019.

[18] The Hong Kong Polytechnic University, PolyU Palmprint Database, http://www.comp.polyu.edu.hk