POPULAR DEMOCTRATIC
REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION
AND SCIENTIFIC RESEARCH

UNIVERSITY CHIKH LARBI TEBESSI - TEBESSA
FACULTY OF EXACT AND NATURAL LIFE SCIENCES
DEPARTEMENT OF COMPUTER SCIENCE

Master Dissertation

In obtaining of MASTER Degree – ACADEMIC

Domain: Computer Science

Branch: Computer Science

Speciality: Systems and Multimedia

TITLE

Biometric Based Image Cryptography in the Era of Digital Piracy

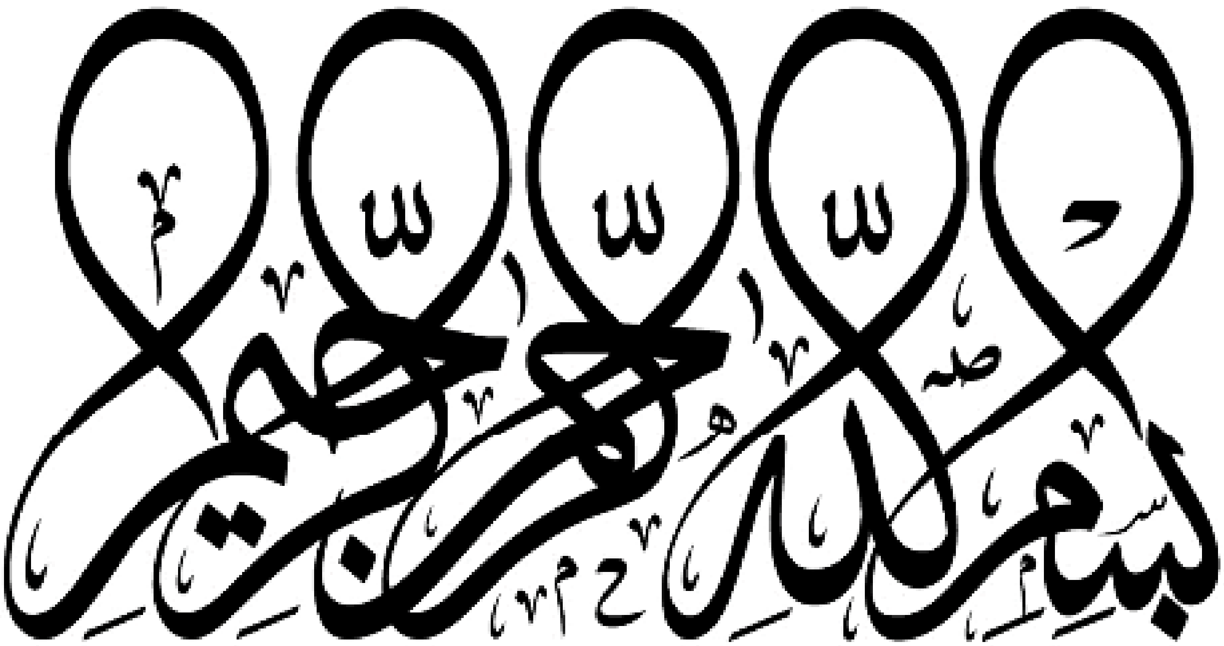
By:

Mr. Harkati Oussama

Board of Examiners

Dr. Ahmed Zeggari	**President**
Pr. Hakim Bendjenna	**Supervisor**
Pr. Abdallah Meraoumia	**Co-Supervisor**
Dr. Hassiba Laifa	**Examiner**

Academic Year 2023 / 2024


بسم الله الرحمن الرحيم

This project is dedicated to my family, whose unwavering support and encouragement have been my greatest motivation.

To my parents, for their endless love, sacrifices, and belief in my abilities. Your guidance and support have been the foundation of my success.

To my friends, for their constant encouragement and for being my pillars of strength throughout this journey.

To my brother, who lives far from us. Your resilience and dedication continue to inspire me every day. Even though distance separates us, your support has always been close at heart.

Thank you all for being my sources of inspiration and strength.

Harkati Oussama

Appreciation

I would like to express my deepest gratitude to everyone who supported and guided me throughout my final year project.

First and foremost, I am extremely grateful to my supervisors, Prof. Hakim Bendjenna and Prof. Abdallah Meraoumia and Dr. Yacine Belhoucine for their invaluable advice, continuous support, and patience during my research. Their immense knowledge and plentiful experience have encouraged me throughout all the stages of my project.

I also wish to thank the faculty members for their insightful comments and encouragement, which pushed me to broaden my research from various perspectives.

A special thanks to my friends and fellow students for their unwavering support and cooperation. Your camaraderie has been a source of motivation and inspiration.

Lastly, I am forever indebted to my family for their unconditional love, unwavering support, and endless encouragement throughout my academic journey. Their belief in me has been a constant source of strength.

Thank you all.

O. Harkati

Abstract:

In the era of digital piracy, securing digital content has become a paramount concern. This project explores the implementation of biometric-based image cryptography as a novel approach to enhance the security of digital images. By integrating biometric traits such as fingerprints or facial recognition into the cryptographic process, this method ensures a higher level of security compared to traditional cryptographic techniques. The study demonstrates how biometric-based encryption can effectively prevent unauthorized access and protect sensitive image data from digital theft. Through comprehensive analysis and experimentation, this project highlights the potential of biometric cryptography as a robust solution to combat digital piracy.

Résumé :

A l'ère du piratage numérique, la sécurisation du contenu numérique est devenue une préoccupation majeure. Ce projet explore la mise en œuvre de la cryptographie d'image basée sur la biométrie comme une nouvelle approche pour améliorer la sécurité des images numériques. En intégrant des traits biométriques tels que les empreintes digitales ou la reconnaissance faciale dans le processus cryptographique, cette méthode garantit un niveau de sécurité plus élevé par rapport aux techniques cryptographiques traditionnelles. L'étude démontre comment le cryptage basé sur la biométrie peut empêcher efficacement l'accès non autorisé et protéger les données d'images sensibles contre le vol numérique. Grâce à une analyse et des expérimentations approfondies, ce projet met en évidence le potentiel de la cryptographie biométrique en tant que solution robuste pour lutter contre le piratage numérique.

ملخص

في عصر القرصنة الرقمية، أصبح تأمين المحتوى الرقمي قضية بالغة الأهمية. يستكشف هذا المشروع تنفيذ تشفير الصور القائم على القياسات الحيوية كنهج جديد لتعزيز أمان الصور الرقمية. من خلال دمج السمات الحيوية مثل بصمات الأصابع أو التعرف على الوجه في عملية التشفير، تضمن هذه الطريقة مستوى أمان أعلى مقارنةً بالتقنيات التقليدية للتشفير. توضح الدراسة كيف يمكن للتشفير القائم على القياسات الحيوية أن يمنع الوصول غير المصرح به بشكل فعال ويحمي بيانات الصور الحساسة من السرقة الرقمية. من خلال التحليل الشامل والتجارب، يبرز هذا المشروع إمكانيات التشفير الحيوي كحل قوي لمكافحة القرصنة الرقمية.

Table of Content

Chapter III : Experimental Results

Annexes

..

List of Figures

Figures **Page**

List of Tables

General Introduction

Introduction

In recent years, the proliferation of computer systems, which now permeate almost every aspect of our modern lives, has introduced new challenges to securing user data and ensuring the confidentiality and privacy of individuals. This increased need for data security is essential for maintaining user trust. Unfortunately, numerous studies indicate a significant rise in data theft, especially on the Internet, in recent years. Often, existing security systems fail to provide adequate protection for user data [1]. Traditional methods of identity verification, such as those based on possession (*e.g.,* smart cards) and knowledge (*e.g.,* passwords), are widely used but have inherent vulnerabilities that can be exploited by unauthorized individuals to steal user data and misuse it [2]. Recently, biometrics has emerged as a viable alternative to traditional security methods, leading to the development of various automatic human recognition systems that utilize physical, behavioral, or biological traits. Biometrics offers a significant advantage in safeguarding user data because biometric traits cannot be easily lost, forgotten, or stolen. This makes biometrics one of the most promising and ambitious methods for providing enhanced protection to user data [3].

Remote identity verification/identification is the process of confirming an individual's identity from a distance, without the need for physical presence [4]. This is typically done using digital technologies and various methods of authentication to ensure that the person is who they claim to be. It is widely used in scenarios such as online banking, remote work, telehealth, e-commerce, and other online services. The goal of remote identity verification/identification is to securely and accurately confirm identities, thereby preventing fraud and unauthorized access to sensitive information or services. In other hand, data encryption is a process of converting raw data into an incomprehensible data to prevent unauthorized access [5]. Encryption ensures that only authorized parties can understand the encryption data by using specific algorithms and keys.

Hybridization of biometrics and encryption for remote identity verification/identification combines the strengths of both technologies to enhance security and reliability in both authenticating individuals and data protection. Therefore, the hybridization of biometrics and encryption in remote identity verification provides a robust solution to the challenges of securing personal data and ensuring accurate authentication [6]. This approach leverages the unique, hard-to-fake nature of biometric data and the strong protection offered by encryption to create a secure and reliable verification system.

Remote identity verification/identification and the protection of transmitted data are crucial. Thus, integrating biometrics with encryption is essential to safeguard both the data and the person's identity from theft. In this dissertation, a system was proposed to identify a person remotely and protect the transmission of images. The biometric system utilized a classifier based on deep learning principles, specifically Deep Rule Based (DRB)[7]. This classifier takes as inputs feature vectors extracted from palmprints using two well-known handcrafted methods: Histogram of Oriented Gradients (HOG) [8] and Local Phase Quantization (LPQ) [9]. For encrypting the images, chaos systems were employed to enhance security by dividing the image into several blocks and encrypting each block individually.

To achieve our objective, this dissertation is organized into three chapters:

The **first chapter** presents a general overview of biometrics, covering in detail the different biometric modalities as well as the structure and operation of biometric systems.

The **second chapter** provides an overview of how biometric systems and encryption methods can be combined to enhance the security of the encryption process and safeguard biometric systems from hackers. This chapter details the proposed method, including comprehensive explanations of the system's design and implementation. Additionally, it covers the necessary prerequisites for the generated system, ensuring a clear understanding of the foundational components required for successful integration.

The **third chapter** presents experimental results related to both the performance of the biometric system and security analysis with all necessary analyzes and discussions, using a database of 300 persons.

Finally, a **general conclusion** with future perspectives is provided at the end of the dissertation.

Chapter 1

Biometrics for security

Abstract

Biometrics holds immense potential for enhancing information security. This chapter begins by describing the fundamental principles of biometric systems. Furthermore, it examines how biometric systems operate, from the initial enrollment process to the recognition and verification phases. Additionally, the evolving landscape of biometric fusion, in which multimodal approaches leverage the synergistic potential of multiple biometric modalities to improve accuracy and resilience against fraudulent attempts, is explored...

Introduction

Information security and biometrics complement each other in providing robust security solutions. By integrating biometric authentication with information security practices such as access control, data encryption, multi-factor authentication, and fraud detection, organizations can enhance the security of their systems and protect sensitive data more effectively. In this chapter, we will first introduce the fundamental concepts of biometrics. Next, we will discuss an overview of multimodal biometrics, as well as the associated scenarios and fusion levels.

I.1 Information security and biometric

In the era of digital transformation, safeguarding information systems is paramount for both organizations and individuals. This highlights the pressing requirement for precise user identification and identity verification. Consequently, researchers have dedicated significant efforts to developing effective methodologies to bolster safety across various processes. The primary aim of these methodologies is to control access to the system [10]. However, traditional methods have demonstrated vulnerabilities, including identity theft. To mitigate these security risks, traditional approaches are being replaced with alternatives that capitalize on a user's intrinsic characteristics or biometric traits. Thus, the integration of biometric systems with information security methods, such as encryption, is symbiotic and can be described as follows:

I.1.1 Biometric as a service to cryptography

Biometrics can play a crucial role in improving the security of encryption systems by providing unique and reliable methods of generating and sharing keys in symmetric encryption.

1) Key generation: Biometric traits can be used to generate encryption keys. For example, a fingerprint scans (see Fig. I.1) or iris pattern can be converted into a unique cryptographic key, which can then be used to encrypt and decrypt data [11].

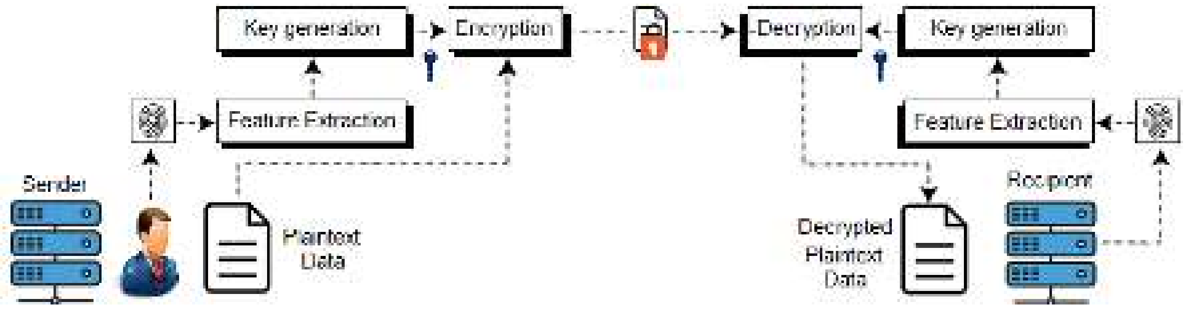


Fig. I.1 Biometric key generation for symmetric cryptography

Biometric key generation process leverages the unique and immutable characteristics of an individual's biometrics to enhance security. Therefore, any encryption system based on a key generated from biometrics has the following advantages [12]:

- ***Enhanced Security:*** Biometric keys are highly secure because biometric traits are unique to each individual and difficult to replicate or steal.
- ***Convenience***: Users do not need to remember complex passwords or carry physical tokens. Their biometric traits are always with them and can be easily used to generate encryption keys.
- ***Non-repudiation:*** Biometric keys provide non-repudiation, meaning that an individual cannot deny having accessed or encrypted the data, as the key is uniquely tied to their biometric data.

- ***Reduction in Key Management Issues:*** Traditional key management can be complex, involving the storage, distribution, and protection of keys. Biometric key generation simplifies this process by tying the key generation to the user’s biometric traits.

- ***Resistance to Brute Force Attacks:*** Since biometric data is highly complex and unique, it significantly increases the difficulty for attackers to generate the same key through brute force methods.

It is important to note that biometric data can vary due to factors like age, injuries, or changes in the environment. Algorithms must be robust enough to account for these variations while still generating consistent keys.

2) Key embedding: Key embedding is a process where a cryptographic key is embedded into biometric data (for example fingerprint) or combined with it in such a way that the key can only be retrieved or used if the correct biometric input is provided (see Fig. I.2). Thus, this approach enhances security by ensuring that the cryptographic key is tightly bound to the user's biometric traits[13].

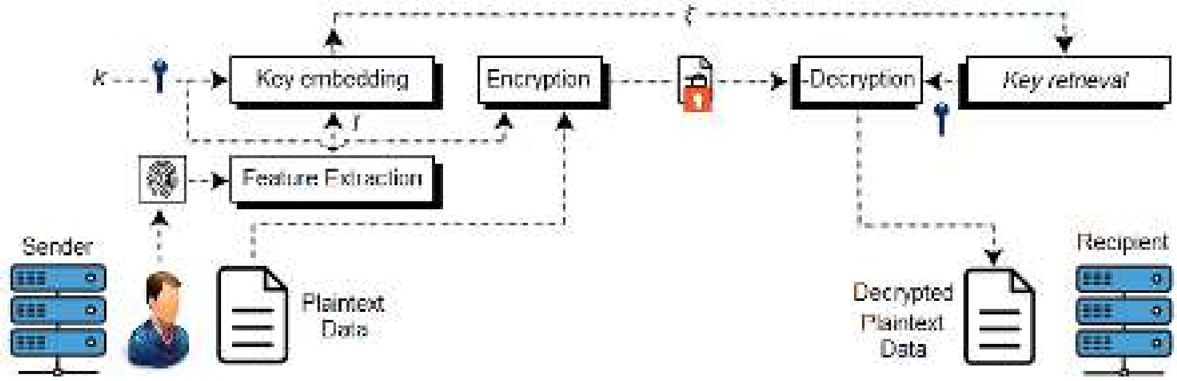


Fig. I.2 key embedding process for symmetric cryptography

By embedding cryptographic keys within biometric data, key embedding enhances the security and usability of cryptographic systems, providing a robust solution for protecting sensitive information and ensuring that only authorized users can access it. Therefore, any encryption system based on a key embedding in biometrics data has the following advantages:

- ***Enhanced Security:*** Embedding the key within biometric data makes it highly secure, as the key cannot be extracted or used without the correct biometric input.

- ***User Convenience:*** Users do not need to remember complex passwords or carry physical tokens. Their biometric traits serve as a natural and convenient way to access the cryptographic key.

- ***Integrated Authentication and Encryption:*** Key embedding provides a seamless way to integrate authentication with encryption, enhancing the overall security architecture.

- ***Reduced Risk of Key Exposure:*** Since the cryptographic key is not stored explicitly but is embedded within biometric data, the risk of key exposure through data breaches is reduced.

In key embedding approach, two well-known techniques were used. Thus, in the key embedding approach, two well-known techniques were used: fuzzy vault and fuzzy commitment: In the fuzzy vault scheme approach, a cryptographic key is secured using the user's biometric data by creating a vault of points. Some points are genuine (derived from the biometric data) and some are chaff points (random points). The correct biometric data can help identify the genuine points and reconstruct the key, while the chaff points prevent an attacker from easily determining the key. In the fuzzy commitment scheme is a cryptographic technique that combines encryption key and biometric data to secure key cryptography.

I.1.2 Cryptography as a service to Biometric

Cryptography can significantly enhance biometric systems by providing security, privacy, and integrity to biometric data and processes [14]. Therefore, encryption processes can enhance biometric systems according to many ways, the most important of which can be described as follows:

1) Biometric Data Protection: Cryptography ensures that biometric data, such as fingerprints or facial images, is securely stored and transmitted (see Fig. I.3). By encrypting this data, even if unauthorized access occurs, the data remains unreadable without the corresponding decryption key.[15]

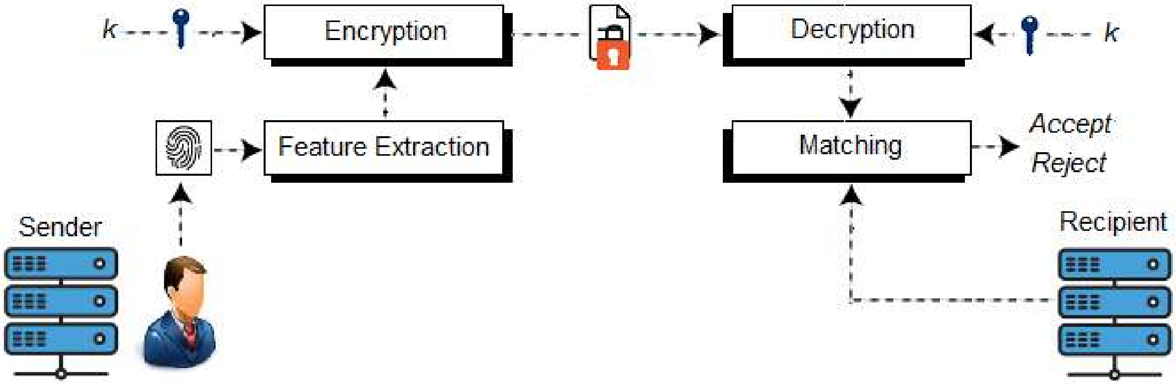


Fig. I.3 Biometric data protection

Protecting biometric data offers numerous advantages that enhance security, privacy, and trust in biometric systems:

- ***Personal Data Protection:*** Protecting biometric data helps ensure that individuals' personal information is not misused or exposed, maintaining privacy and complying with data protection regulations.

- **Minimized Risk of Identity Theft:** Since biometric data is unique and intrinsic to individuals, protecting it minimizes the risk of identity theft and unauthorized use.

- ***Protection Against Data Breaches:*** Encrypting and securely storing biometric data helps protect against data breaches and cyberattacks, reducing the potential damage and costs associated with such incidents.

- **Resilience to Spoofing:** Advanced biometric protection mechanisms, such as liveness detection and multi-modal biometrics, make it harder for attackers to spoof or bypass biometric systems.

By leveraging these advantages, organizations can ensure that their biometric systems not only provide secure and reliable authentication but also protect the privacy and integrity of users' biometric data, fostering a safer and more trustworthy digital environment.

2) Cancelable Biometric: Cancelable biometrics (revocable biometrics) is a technique used to enhance the security and privacy of biometric systems (see Fig. I.4). It involves transforming biometric data into a revocable and renewable format, allowing for the biometric template to be changed if compromised [16]. This method ensures that even if biometric data is exposed, the original biometric trait remains secure and a new, secure version can be generated.

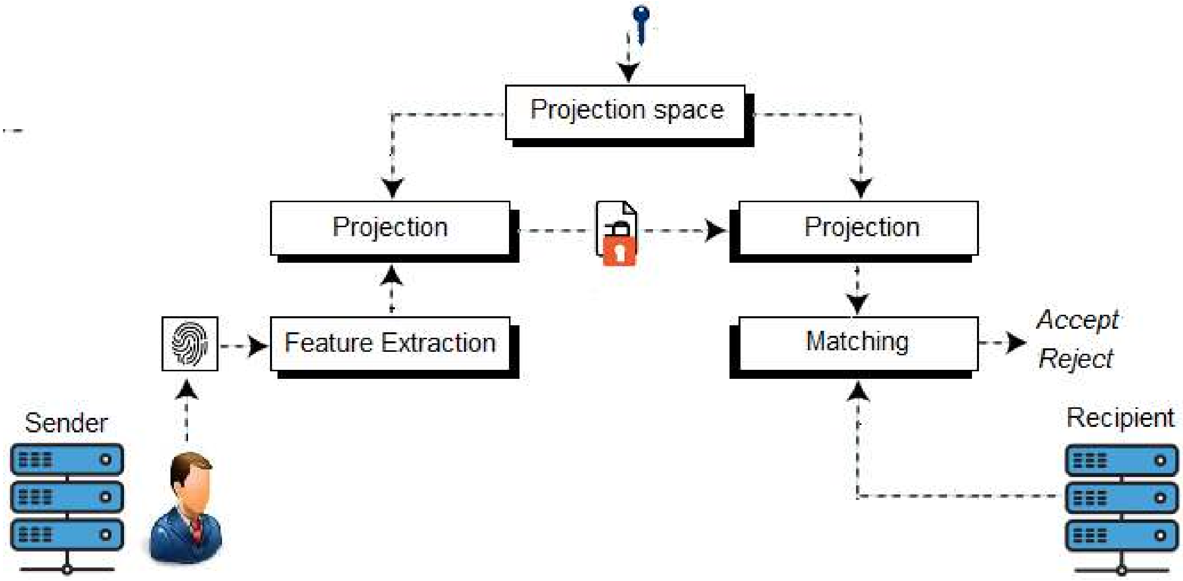


Fig. I.4 Cancelable biometrics

Implementing cancelable biometrics allows organizations to substantially improve the security and privacy of their biometric systems, offering a robust solution to the challenges associated with protecting biometric data. Cancelable biometrics offers numerous advantages that enhance security, privacy, and trust in biometric systems:

- ***Enhanced Security:*** By transforming the biometric data, cancelable biometrics protect against template theft and misuse. Even if the transformed template is compromised, the original biometric trait remains secure.

- ***Privacy Protection:*** The non-invertibility of the transformation function ensures that the original biometric data is not exposed, protecting user privacy. Also, users can have different transformed templates for different applications, preventing linkage across systems.

- ***Revocability and Renewability:*** If a transformed biometric template is compromised, a new template can be generated using a different transformation, similar to changing a password. This provides a practical solution for managing compromised biometric data.

I.2 Biometrics

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying individuals who are under surveillance [17]. The basic premise of biometric authentication is that every person can be accurately identified by intrinsic physical or behavioral traits.

I.2.1 Biometrics importance

Currently, biometric recognition is an important issue for securing systems. Indeed, the growing interest in biometrics is due to several factors, including:

- ***High security*:** Combined with other technologies such as encryption or smart cards, certain systems make fraud very complicated.

- ***Comfort:*** By replacing only traditional methods, such as passwords, biometrics makes it possible to respect basic security rules. When these rules are followed, biometrics saves administrators from having to respond to numerous password change requests.

- ***Security/psychology:*** In certain cases, notably for e-commerce and e-banking, the customer does not trust. It is essential for these organizations to convince the customer to transact. Biometric authentication can change customer behavior.

I.2.2 Biometrics application

Generally, biometrics meets security requirements in almost all areas [18]. Biometric security applications can be classified into four main sections

- ***Public service:*** Biometrics is used in the public service to control and secure government and border buildings, to control immigrants entering and leaving a territory, to identify people in airports (Iris, face and digital fingerprint) and also in public health.

- ***Judiciary:*** Biometrics is used in the judiciary to prove certain facts regarding criminal offenses, to identify the identity of such a criminal using biometric traits extracted from the crime scene, in electoral voting by Internet and in the identification of missing children and finally in the electronic protection of documents.

- ***Banking sector:*** Biometrics are used in the banking sector to carry out banking transactions (cash withdrawals, bank cards, payment by telephone and internet) and to reduce the proportion of fraud thanks to the integration of smart cards with fingerprint recognition digital.

- ***Physical and logical access:*** Biometrics are effectively used to control physical and logical access. It is used either to control physical access such as securing a location (building or room) or to control logical access such as securing a computer session.

I.3 Biometrics technologies

Biometric modalities refer to the various physiological, behavioral and biological characteristics that are used for identification and authentication purposes. These modalities encompass a wide range of unique attributes that can be measured and analyzed to establish an individual's identity with a high degree of accuracy. It’s an integral part of human bodies or behaviors, meaning that they are necessarily subject to evolution over time and to the hazards of everyday life [19,20]. Biometric technology is developing rapidly and tends to be associated, in the short term, with current technologies such as smart cards, badges, keys, etc. Thus, Fig. I.5 shows important biometric modalities.

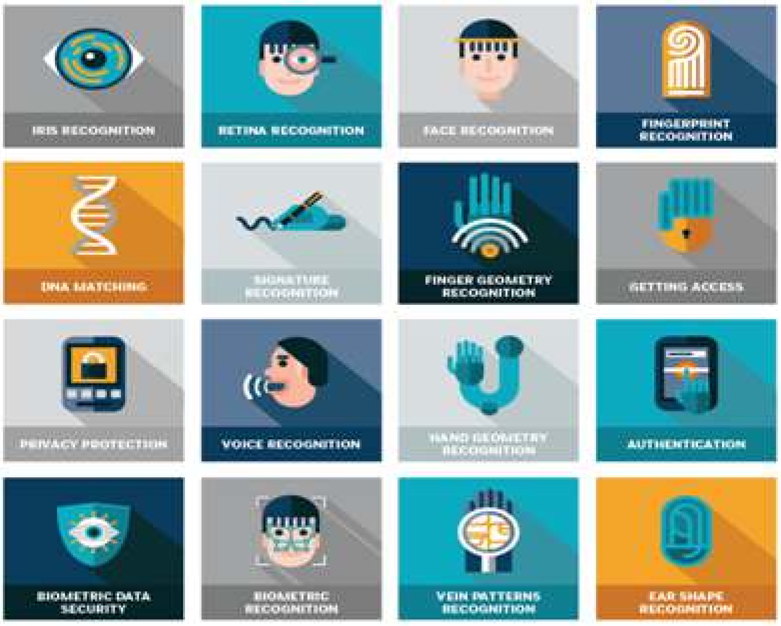


Fig. I.5 Biometric modalities

I.3.1 Properties of a biometric modality: The biometric modalities used must have certain properties to allow the development of reliable and robust biometric systems. The essential properties for each biometric modality are as follows:

- ***Universality:*** The entire population must have this modality;
- ***Uniqueness:***Two different persons must have different representations of their biometrics;
- ***Stability:*** A biometric must be relatively stable over time and above all must be stable for a person whatever the circumstances of acquisition (external conditions, emotional conditions of the person, etc…);
- ***Acceptability:*** Refers to the constraints to the acquisition and use of a biometric modality, it must be accepted by the public;
- ***Non-reproducibility:*** concerns whether or not it is easy to falsify a biometric modality to avoid fraudulent use of the system;
- ***Permanence:*** the information must be constant over time;
- ***Performance:*** effectively recognize a person, a predetermined criterion established to evaluate the performance of a biometric system;
- ***Measurability:*** it can be measured with different sensors.

I.3.2 Types of biometric modalities: All biometric modalities share the objective of verifying an individual's identity through the analysis of their physical (morphological), behavioral, or biological attributes [21, 22]. Among the different existing biometric modalities, there are three main categories:

1) Physical biometric modalities (morphologies): In biometrics, morphology refers to the measurement of a person's physical features to create a biometric template. This category focuses on identifying and verifying specific physical traits, including, but not limited to, fingerprints, face, iris, and palmprint.

- ***Fingerprint***: Fingerprint recognition (Fig. I.6) relies on capturing and analyzing the unique patterns of ridges and valleys present on a person's fingertips. It is one of the oldest and most widely used biometric due to the distinctiveness and permanence of fingerprints.

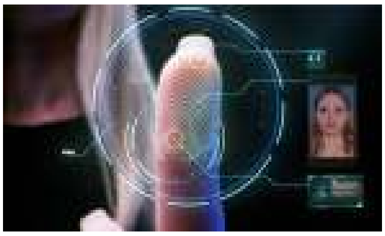


Fig. I.6 Fingerprint modality

- ***Face:*** Facial recognition technology (Fig. I.7) utilizes facial features such as the distance between the eyes, nose shape, and jawline to identify individuals. It has gained significant popularity in recent years, especially in surveillance and security applications.

Fig. I.7 Face modality

- ***Iris*:** Iris recognition (Fig. I.8) involves capturing high-resolution images of the unique patterns in the colored part of the eye (iris). The intricate patterns of the iris are highly distinctive and stable over time, making it a reliable biometric modality.

Fig. I.8 Iris modality

- ***Palmprint Recognition:*** Palmprint recognition (Fig. I.9) analyzes the unique patterns of lines, ridges, and creases on the palm of the hand. It is particularly useful in situations where fingerprint recognition may not be feasible, such as in outdoor environments or industrial settings.

Fig. I.9 Palmprint modality

2) Behavioral biometric modalities: Behavioral biometrics modalities encompass distinct characteristics based on individuals' actions, habits, or mannerisms. They provide continuous authentication, non-intrusive verification, and resistance to spoofing attempts. Leveraging these characteristics, organizations can enhance security measures and user experience across various applications requiring identity verification.

- ***Voice Recognition*****:** Voice recognition (Fig. I.10) technology identifies individuals based on the unique characteristics of their voice, including pitch, tone, and speech patterns. It is commonly used in telephone-based authentication systems and voice-controlled devices.

Fig. I.10 Voice modality

- ***Signature Recognition:*** Signature recognition (Fig. I.11) examines the distinct features of an individual's handwritten signature, including stroke dynamics, pressure, and speed. Widely used in financial transactions and legal documents, signature recognition provides a reliable means of identity verification.

Fig. I.11 Signature modality

- ***Gait recognition:*** Gait recognition (Fig. I.12) identifies individuals based on their walking patterns, including stride length, speed, and rhythm. By capturing and analyzing these unique characteristics, gait recognition systems can accurately verify identity, offering applications in security and surveillances.

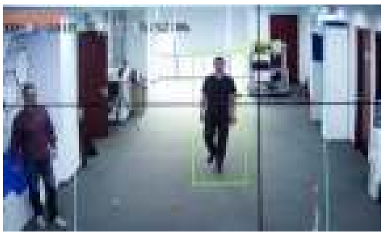


Fig. I.12 Gait modality

3) Biological biometric modalities: Biological biometrics is based on the analysis of a person's biological traces, such as DNA, hand veins, and facial thermography.

- ***Hand Veins:*** Hand vein recognition technology (Fig. I.13) analyzes the pattern of veins in the hand, which is unique to each individual. It utilizes infrared imaging to capture the vein pattern and is used in access control systems and banking applications.

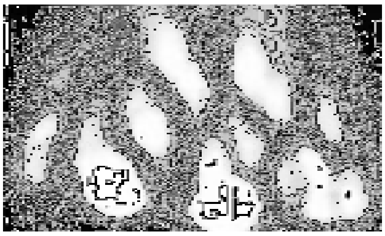


Fig. I.13 Hand vein modality

- ***DNA:*** Deoxyribonucleic acid is the most accurate way to determine a person's identity. It is impossible to find two persons with the same DNA (Fig. I.14). This biometric has the advantage of being unique and permanent throughout life.

Fig. I.14 DNA modality

- ***Facial thermography:*** The amount of heat emitted by the different parts of the face characterizes each person (Fig. I.15). It depends on the location of the veins but also on the thickness of the skeleton, the amount of tissue, muscle, fat, etc. A thermal camera takes an infrared image of the face. This makes it possible to highlight a distribution of heat specific to each person.

Fig. I.15 Facial thermography modality

I.3.3 Biometric System Description

A biometric system is a pattern recognition system that identifies a person based on a feature vector derived from their unique physiological or behavioral traits. Depending on the application, a biometric system typically operates in either verification mode or identification mode.

1) Biometric system phases: The design of biometric systems involves two fundamental phases: the registration (enrollment) phase and the recognition phase, which can operate in either authentication mode or identification mode.

- ***Enrollment phase (creation of the database):*** The first phase of any biometric system is the registration (or enrollment). During this phase, a user's biometric data is captured and stored in a biometric database (as a form of feature vector) for the first time (Fig. I.16).

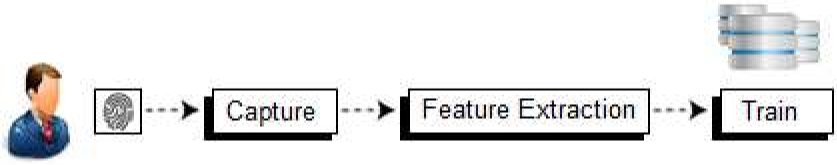


Fig. I.16 Enrollment phase

This process may also include adding the user's biographical information to the database.

- ***Reconnaissance Phase (Test):*** The task of the recognition phase (Fig. I.17) is to verify or identify the identity of a person attempting to access the system. During this phase, the biometric data is captured, and a set of parameters (biometric template or feature vector) is extracted, similar to the enrollment process. The extracted feature vector is then compared with the stored feature vectors in the enrollment phase, and a decision is made based on the score obtained in the comparison task.

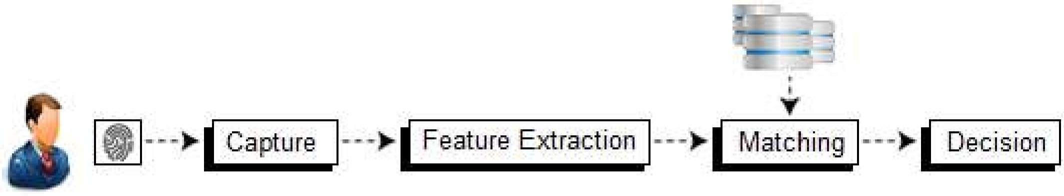


Fig. I.17 Recognition phase

The sensor used should closely match the one used during enrollment to ensure accuracy.

2) Operating modes: In biometric systems, the recognition process depends on whether the system operates in verification or identification mode.

- ***Verification mode:*** In verification mode, also known as authentication, the person attempting to access the system declares their identity. The algorithm then compares the biometric template of the declared identity with the corresponding pre-stored template in the database. The system responds with a binary decision (yes or no) indicating whether the templates match. This process involves comparing the input template with a single template in the database (1:1).

- ***Identification mode:*** In this mode, the person attempting to access the system does not declare their identity. Instead, the system determines "Who am I?" by checking if the user's biometric template matches any template in the database. The user provides a biometric sample, which is then compared against all stored templates from the enrollment phase

(1: N comparison). The system either accepts the user if a match is found or rejects them if no match exists. The identification mode can be divided into two operating modes:

Closed set mode: The output of the biometric system is the identity of the person whose stored template shows the highest degree of similarity to the biometric sample provided.

Open set mode: If the highest similarity between the tested biometric sample and all pre-registered templates falls below (or exceeds) the security threshold, the person is rejected, indicating that the user is not enrolled. Otherwise, the person is accepted.

3) Biometric system modules: A typical biometric system can be represented by four main modules:

- ***Capture module:*** This module captures the raw biometric data of the user using biometric sensors or scanners. Factors like cost and size impact the design of the sensor module.

- ***Feature extraction module:*** Here, raw data from the sensor module is processed to generate a digital representation of underlying traits or modalities. Extracted features are then passed to the matching module for comparison.

- ***Matching module:*** Extracted features are compared with templates stored in the database to generate a match score. This score's quality depends on the given biometric data's quality. The matching module also incorporates a decision-making module, where the match score validates the claimed identity.

- ***Decision module:*** This module determines whether the user is a genuine user or an impostor based on match scores. These scores are either used to validate a person's identity or provide a ranking of enrolled identities for individual identification.

I.4 Multimodal biometrics

A Multimodal Biometric System is an advanced identification system integrates multiple biometric traits to enhance individual identification, which uses more than one behavioral or physical characteristic. The advantage of multimodal biometric traits compared to token based or password is, these traits cannot be lost, stolen or shared; ensuring higher accuracy and security compared to unimodal systems combining independent biometric modalities mitigates the limitations of any single modality, such as non-universality or unreliable data due to worn fingerprints. The system's reliability is further strengthened as failures in one technology do not significantly impact individual identification, thanks to the successful employment of different modalities. This reduces susceptibility to spoofing attempts, thereby enhancing overall system efficiency. Particularly noteworthy is the significant reduction in the Failure to Enroll rate, a key advantage of multimodal systems.

I.4.1 Data Fusion

Data fusion is the process of combining information from multiple sources to produce a more accurate, reliable, and comprehensive understanding of a situation or phenomenon than could be achieved by using individual sources alone. In the context of biometric systems, data fusion involves integrating data from various biometric modalities. The goal of data fusion is to improve data quality of that object, which can be achieved if the information is stored separately, obtaining synergy [23]. Synergy can be defined as: the representation of a whole is better than the representation of the individual components.

The advantages of data fusion in biometric systems are multiple. By integrating multiple biometric modalities, data fusion improves identification accuracy and reliability, even in challenging environments or for individuals with unique characteristics. It also improves security measures by reducing the likelihood of unauthorized access or fraudulent attempts to impersonate the system. Additionally, data fusion allows biometric systems to adapt to changing conditions or user constraints, ensuring reliable performance in various scenarios.

I.4.2 Fusion Scenarios

In the context of multimodal biometric systems, fusion scenarios represent the various approaches or methodologies employed to combine information from multiple biometric modalities [24]. We can differentiate 5 possible scenarios of multimodal systems (Fig. I.18)

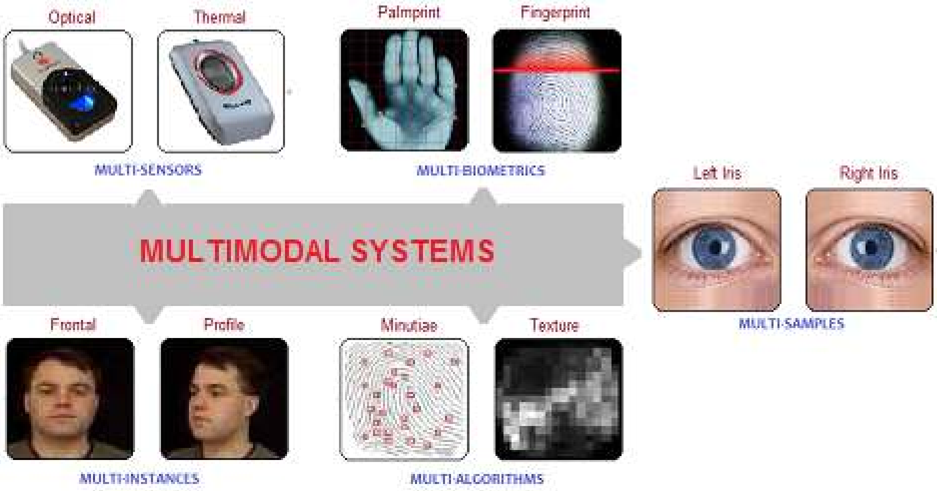


Fig. I.18 Fusion scenarios

1) Multi-sensor systems: Several sensors make it possible to capture the same biometric modality. So, capturing a face using a conventional camera and an infrared camera falls into this scenario.

2) Multi-biometric systems: This type of system combines different biometric traits of a person. Face and iris fusion, or face and fingerprint fusion are part of this type of approach. These systems require different sensors as well as algorithms dedicated to each biometric trait. The main characteristic of this type of system is that the biometric modalities considered can be more decorrelated than for multi-sensor systems.

3) Multi-sample systems: A single sensor can capture multiple instances of the same biometric modality with the aim of making feature extraction more robust or enriching a person's biometric model. For example, of several captures of a person's face from different angles. The use of videos also falls into this context.

4) Multi-instance systems: This type of system allows multiple instances of the same biometric modality to be captured. The acquisition of several fingerprints via the same sensor is the typical example of this type of system. These systems do not result in additional sensor costs or the development of new algorithms. Not to be confused with multi-sample systems.

5) Multi-algorithms systems: In these systems, the same biometric data is processed using multiple algorithms. This multiplicity of algorithms can occur in the extraction module, by considering several sets of features, and/or in the comparison module, by using several comparison algorithms. For example, texture analysis and minutiae algorithms can be combined to process the same fingerprint image to extract various features that can be used to improve system performance.

These fusion scenarios represent different strategies for integrating information from multiple biometric modalities, each with its own advantages and considerations. Understanding and appropriately applying these fusion scenarios are essential for designing effective and efficient multimodal biometric systems that achieve optimal recognition performance and robustness.

I.4.3 Fusion level

Fusion levels in multimodal biometric systems encompass various combinations of biometric modalities and fusion strategies [25]. Here, we explore four common fusion scenarios in detail, including sensor level fusion, feature extraction level fusion, matching score-level fusion, classification and class decision level fusion.

- ***Fusion at the sensor level:*** This process involves fusing raw data from different sensors (Fig. I.19). It allows for the utilization of either samples of the same biometric trait acquired from multiple compatible sensors or multiple instances of the same biometric trait obtained using a single sensor.

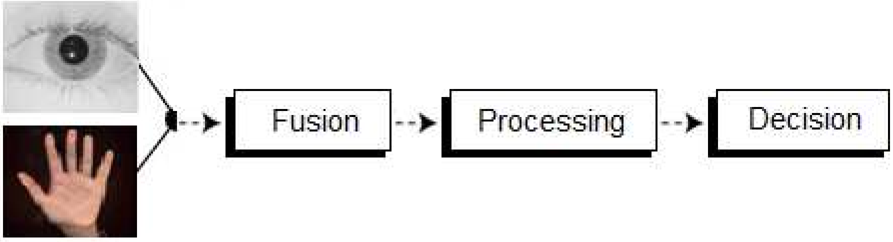


Fig. I.19 Fusion at the sensor level

Since the fusion occurs at a very early stage, this method contains a substantial amount of information compared to other fusion levels. Various techniques can achieve this, such as Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA), for fusing multiple modalities.

- ***Fusion at the Feature Extraction Level:*** At this level, feature vectors are combined to create a unified vector (Fig. I.20). It entails using either the same feature extraction algorithm or a different one across multiple modalities whose features need to be fused.

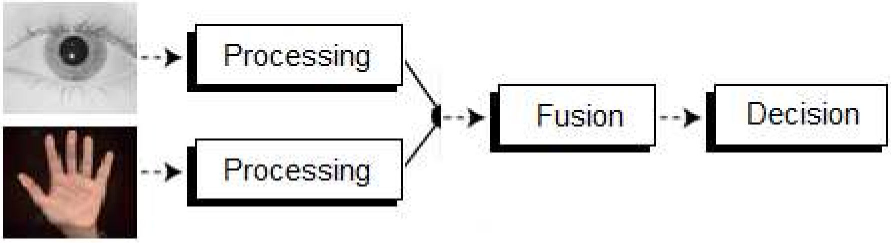


Fig. I.20 Fusion at the feature extraction level

These types of fusion poses challenges because the relationships between features are often unknown, structurally incompatible features are prevalent, and there's a risk of encountering the curse of dimensionality. When the feature vectors are homogeneous, a single resulting feature vector can be calculated as a weighted sum of the individual feature vectors. When the feature vectors are heterogeneous, we can concatenate them to form a single vector.

- ***Fusion at Matching Score Level:*** Each system produces a matching score reflecting the similarity between the feature vector and the template vector (Fig. I.21). These scores can be combined to verify the accuracy of the claimed identity [26]. However, scores obtained from different matchers may not be directly comparable, so a score normalization technique is employed to align them onto the same scale.

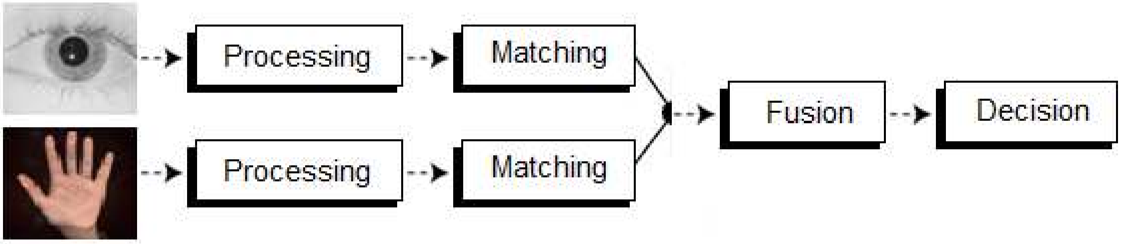


Fig. I.21 Fusion at the matching score level

To combine scores obtained from multiple search modules using schemes such as sum of scores (SUM), maximum of scores (MAX), minimum of scores (MIN) and multiplication of scores (MUL), weighted sum of scores (WHT).

- ***Fusion at the Decision Level:*** The fusion at the decision level concerns the combination of decisions obtained from each source (Fig. I.22). Decision-level fusion is often used for its simplicity. Indeed, each system provides a binary decision, and the decision fusion system consists of making a final decision based on this series of binary decisions.

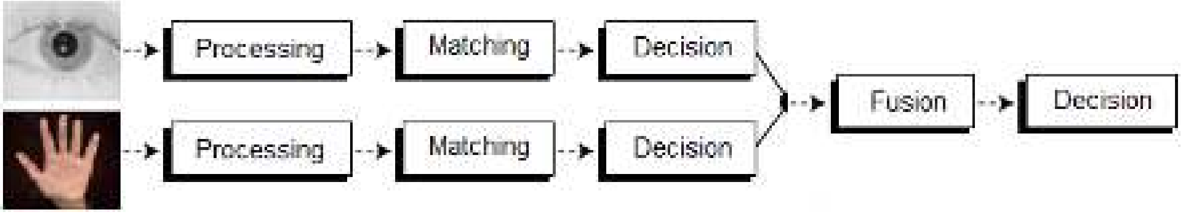


Fig. I.22 Fusion at the decision level

The most used methods are vote-based methods such as OR (if one system decided 1 then YES), AND (if all systems decided 1 then YES) or majority voting (if the majority systems decided 1 then YES).

Conclusion

Biometrics has become an integral part of many applications, serving to strengthen security measures and streamline the process of identifying individuals. In this chapter, our exploration focused on the multifaceted field of biometrics, delving into various biometric modalities and the complex systems they comprise. We have carefully considered the architecture and functionality in biometric systems. Additionally, we delved into the fusion scenarios suitable for multimodal biometric systems, illuminating strategies for fusing diverse biometric data to boost accuracy and efficiency.

Chapter 2

Remote Access Authentication

Abstract

Remote access authentication is a crucial component of modern cybersecurity, serving as the initial line of defense against unauthorized access to network resources and sensitive information. It involves the verification of users' identities who are attempting to connect to a network or system from a remote location, typically outside the confines of a physical office or facility. Upon successful authentication, users are granted access privileges commensurate with their credentials, enabling them to leverage resources and services remotely. In this chapter, after illustrating some concepts about remote access authentication, the structure of the proposed biometric encryption system will be carefully presented.

Introduction

Remote access authentication and authorization are mechanisms for controlling user access to remote systems. Biometric authentication enhances security by ensuring that access is granted only to authorize individuals based on their unique biometric data [27]. In this chapter, we will illustrate the key aspects of implementing biometric authentication for remote access and its associated benefits. Additionally, we will present the proposed system for authentication and information security during transmission.

II.1 Remote Access Scenario

A distinct authentication scenario involves granting remote access to a network using a combined client-server model that integrates cryptographic mechanisms with biometrics. In this setup, the client terminal functions as a biometrics-based host, equipped with a capture device and a processing unit to measure biometric features and generate the feature vector (biometric template) [27]. This access scenario typically includes mechanisms to detect liveness and prevent biometric replay attacks.

II.2 Benefits of biometrics-based remote access

Biometrics provides numerous advantages for user authentication in remote work scenarios, including enhanced security, convenience, compliance, and user experience. Difficult to forge, share, lose, or forget, biometrics effectively prevents unauthorized access. They are user-friendly, eliminating the need to remember complex passwords or carry extra devices. Moreover, biometrics aid organizations in meeting regulatory and industry standards for data protection, privacy, and auditability [28]. Finally, they offer a seamless and personalized authentication process, boosting user satisfaction and trust.

II.3 Crypto-biometric based remote access

The system uses symmetric cryptographic and multi-factor authentication methods. In this system, users authentications are based on a card combined with a PIN code and a biometric trait [29]. The e-security system based on multi-factor authentication is shown in Fig. II.1.

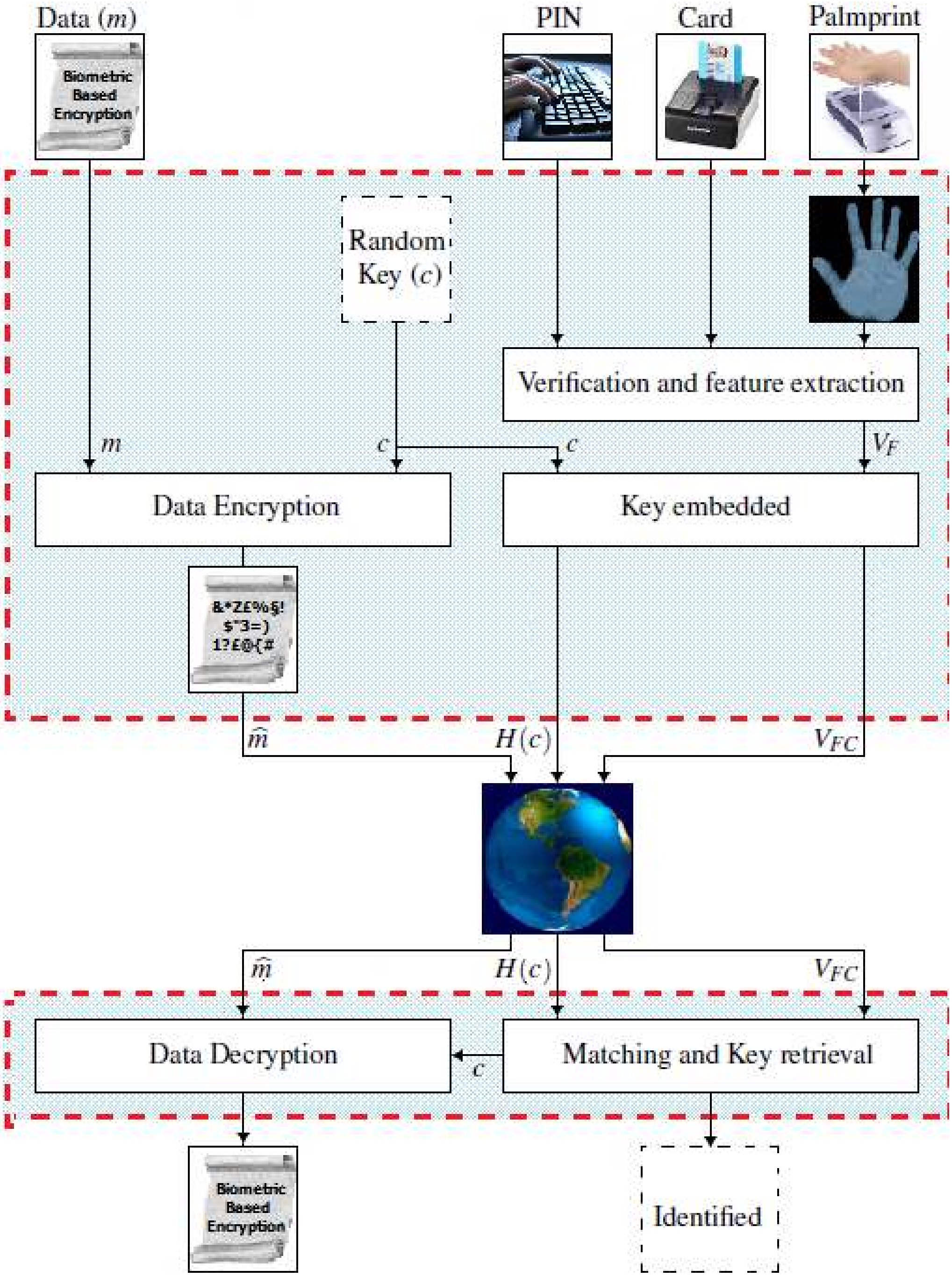


Fig. II.1 An example of biometric based remote access

In any biometric system, there are two essential phases: enrolment and identification. Thus, all the authorized users must be previously enrolled (registered) in system database. For each user, during the enrollment process, the feature vectors (or template) are generated from their biometric modalities (*e.g.,* Palmprint modality) and stored in the database for later use (identification process) as well as in the user ID card. In addition, a PIN code is randomly generated and stored in this card. Hence, the PIN code is used for security purposes and to authenticate the user in the electronic transmission device (logical access control).

II.4 Biometric and Cryptography

Biometrics and cryptography are two fields that intersect in various applications, such as secure authentication systems or encrypted data transmission (Fig. II.2).

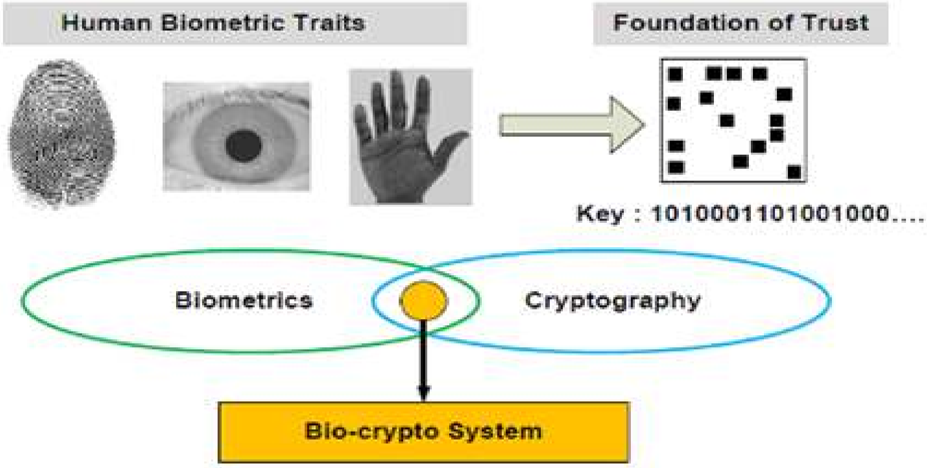


Fig. II.2 Biometric and Cryptography relationship

While biometrics focuses on unique physical or behavioral characteristics for identity verification, cryptography deals with secure communication through encoding and decoding information. Combining biometrics with cryptography offers a robust approach to enhancing security systems [30]. This integration leverages the unique strengths of each technology to provide secure, reliable, and user-friendly authentication mechanisms.

II.5 Proposed Systems

Generally, in the cryptographic process, the shared key (random key) must be exchanged between the different clients in order to decrypt the transmitted information (symmetric cryptography). For that, one of efficient solution is to use biometric traits of the user to secure this key during transmission in order to attain a higher security against cryptographic attacks. These systems, called biometric cryptosystems or crypto-biometric systems, can benefit of the advantages of both fields (cryptography and biometrics). In such systems, while cryptography endows with high and modifiable security levels, biometrics ensured that user requesting the information is legitimate. Furthermore, biometrics can secure effectively the cryptographic key. Among several scenarios, the cryptographic commitment scheme draws greater attention from researchers. In this scenario, the cryptographic key is embedded in a feature vector without disclosing it (hiding the cryptographic key). Thus, the fuzzy commitment is one of the used commonly method of this scenario.

II.5.1 Preliminary

Feature extraction is a crucial task in biometric applications because of the vast array of features present in images. Due to this necessity, researchers have dedicated significant effort to improving this process. Indeed, many challenges related to the final design of a biometric system are typically linked to feature extraction. In this sub-section, we discuss our feature extraction method and the classifier used.

1) HOG descriptor: Feature extraction is a critical task in biometric applications due to the vast array of features present in images. Consequently, researchers have dedicated significant effort to this area. In fact, many challenges associated with the final design of a biometric system are typically linked to the feature extraction process [31]. In our work, we use an important feature extraction method namely Histogram of Oriented Gradient (HOG) descriptors.

HOG descriptors are like an edge map, but it stores both the gradient magnitude information and the cell-level edge locations. The location coarseness and normalization of HOG features are crucial because they provide some degree of invariance to small geometric and photometric changes. Assume that the input is the $H \times W$ sized window I of a grayscale image, or even the whole image, to create a HOG feature, we follow the steps:

- Calculate gradients*:* Find the components of the gradient (I_x, I_y) by:

$$\begin{cases} I_x(i,j) = I(i,j+1) - I(i.j-1) \\ I_y(i,j) = I(i-1,j) - I(i+1,j) \end{cases} \qquad i = 1 \ldots H \,,\; j = \; 1 \ldots W \tag{1}$$

The gradient is then transformed to polar coordinates with the angle limited between 0° and 180° degrees to identify opposite gradients.

$$\begin{cases} \mu = \sqrt{I_x^2 + I_y^2} \\ \theta = \frac{180}{x} \left(\tan^{-1}(I_x, I_y)\right) \, mod \; \pi \end{cases} \tag{2}$$

where $\tan^{-1}$ is the inverse tangent, which yields values between -π and π, and μ and θ denote respectively the magnitude and the direction (angle) of the gradient of each pixel.

- Cell Orientation Histograms*:* The window is partitioned into nonoverlapping neighboring $c \times c$ sized cells (*i.e.* c = 8). Then, for each cell, a histogram of the gradient directions sorted in B bins (*i.e.* B = 9). Thus, the bins are numbered from 0 to $B - 1$ and each has a width of

$\omega = \frac{180}{B}$ It is important to note that with so few bins, a pixel at a bin boundary could wind up in a different bin if the image changes significantly. Voting by bilinear interpolation is used to overcoming these quantization artifacts. This method lets each pixel in a cell contribute to two adjacent bins. This method divides the gradient magnitude between the two bins for each pixel based on the distance between the gradient orientation and the center of each bin. In other words, it calculates how much of the gradient magnitude is in each bin:

$$\mathcal{F}_{vote}(\mu_i, \theta_i, B_i, B_{i+1}) = \begin{cases} K_1\mu \rightarrow B_i \\ K_2\mu \rightarrow B_{i+1} \end{cases} / \; K_1 + K_2 = 1 \tag{3}$$

Since the gradient magnitude is always positive, the resulting cell histogram is a B-valued vector.

- **Block Normalization:** In this phase, the cells are organized into overlapping $2c \times 2c$ pixel blocks with a vertical and horizontal overlapping step of $\boldsymbol{c}$ pixels. Next, the histograms of the four cells in each block are concatenated into a single block feature, which is then normalized using the Euclidean norm:

$$b_k = \left[h_{(i,j)}, h_{(i,j+1)}, h_{(i+1,j)}, h_{(i+1,j+1)}\right] \tag{4}$$

Where b_k denotes the feature of the block k and $h_{(i,j)}$,the histogram of the cell (*i, j*). This block feature is normalized as follows:

$$\widetilde{b_k} = \frac{b_k}{\sqrt{\|b_k\|^2 + \in}} \tag{5}$$

Where ∈ is a small positive constant that prevents division by zero in gradient-free blocks.

- **HOG Feature:** Lastly, to represent the whole window feature, all the normalized block features ($\widetilde{b_k}$) are concatenated to produce one HOG feature vector ($\mathcal{H}$), as shown below:

$$\mathcal{H} = [\widetilde{b_1}, \widetilde{b_2}, \dots, \widetilde{b_k}, \dots, \widetilde{b_p}] \tag{6}$$

Where p is the number of blocks in the window. Finally, the resulting HOG function is also normalized using Eq (5).

2) Codebook formulation: The feature vectors extracted from all the training images represent the various features that can be found in the work context. Intuitively, all of these features (palmprint features of several persons) have a finite dimension. Consequently, many feature vectors in the training base after the transformation can be very close. Therefore, an unsupervised clustering process was conducted to select only the most discriminative feature vectors relevant to the work context. After clustering, the resulting vectors form a so-called codebook (C_k), which represents prior knowledge that is presented to the feature extraction method to effectively represent the image's features.

In our study, we used the Linde-Buzo-Gray (LBG) algorithm [12] as the clustering technique. This algorithm takes a set of biometric feature vectors ($\mathcal{V}$) as input and generates a representative subset of feature vectors (codebook, C_k) according to the similarity measure. The initial codebook, the distortion, and the threshold are the parameters that control the convergence of the LBG algorithm, which generally requires a maximum number of iterations to ensure this convergence.

3) Deep Rule-Based classifier: A novel multi-layer neuro-fuzzy architecture called the deep rule-based (DRB) system has been developed by combining the strengths of self-organizing non-parametric fuzzy rule-based (FRB) systems with the massively parallel multi-layer structure characteristic of deep learning. This innovative approach has shown exceptional performance across various image classification tasks.

- Massively Parallel Rule Base Layer: This layer comprises a collection of massively parallel (IF...THEN) rules, constructed based on multiple prototypes interconnected through logical OR operators. These rules constitute the fundamental core of the DRB classifier. This classifier involves organizing a parallel set of (IF...THEN) rules, one for each of the C class present in the image set. These rules are formed based on prototypes extracted from data clouds within images of each class during the learning process. Once the learning process is completed, the rule base will contain C rules, each formulated in the form (IF...THEN) for classes $c = 1, 2, 3, .., C$.

$$\begin{array}{l}\text{IF } \left(I \backsim P_{c,1}\right) \text{ OR } \left(I \backsim P_{c,2}\right) \text{ OR} \cdot\cdot \text{ OR } \left(I \backsim P_{c,N_c}\right) \\ \text{THEN} \quad (\text{class c})\end{array} \tag{7}$$

where the $\backsim$ denotes similarity, representing the fuzzy degree of membership. I represents an input image and $P_{c,i}$ represents the i^{th} prototype of the c^{th} class. N_c represents the number of prototypes from the images of the c^{th} class identified by the DRB classifier. The learning process of the DRB classifier has been described in detail in [8].

Once the identification procedure is complete, the DRB system generates C fuzzy rules corresponding to the C classes. For every testing image I, each of the C fuzzy rules will produce a confidence score $\lambda_c(I)$ through its local decisionmaker. This score is determined based on the feature vector of I, denoted as $\mathcal{V}$.

$$\lambda_c(I) = \arg\max_{\mathrm{j}=1,2,\ldots N_c}(\mathrm{e}^{-\|\mathcal{V}-P_{c,i}\|^2}) \quad (8)$$

As a result, one can get C scores of confidence per image:

$$\lambda(I) = [\lambda_1(I),\ \lambda_2(I), \ldots, \lambda_c(I)] \quad (9)$$

These scores are the inputs of the overall decision-maker.

- **Decision-Maker Layer:** In the final layer, the overall decision-maker employs the winner-takes-all principle to determine the label (person identity (P_{id})) of the test palmprint ROI sub-image.

$$P_{id}(I) = \arg\max_{\mathrm{c}=1,2,\ldots N_c}[\lambda_c(I)] \quad (10)$$

This means that the decision-maker selects the class label associated with the highest confidence score obtained from the previous layer's fuzzy rules.

4) Logistic Maps: In recent years, the dynamic behavior of nonlinear systems has garnered significant practical interest across numerous applications due to their simplicity, and richness. Among these systems, chaotic systems stand out as some of the most important. They are characterized by extreme sensitivity to initial conditions, periodicity, pseudo-random behavior, and high complexity. Indeed, in a chaotic system, sensitivity to initial conditions is undoubtedly the essential feature of chaotic behavior, making long-term evolution unpredictable. Such systems are highly sensitive to even the slightest perturbation in the initial condition (initial state) [31]. Even if the starting points are nearly identical, the trajectories quickly diverge. A chaotic system in discrete time is defined by the following equation:

$$x_{n+1} = \Gamma(x_n)\,, \quad n = 0,1,2 \ldots \quad (11)$$

Where $x_n \in R^n$ is called state, and Γ plots the next state ⟦x_{n+1}. From an initial state x_0, the repeated application of this function (Γ) causes a sequence of N points ($\{x_n\}_{n=0}^{N}$) called the orbit of the discrete-time system.

Undoubtedly, these systems have been successfully used in information security applications, for the generation of dynamic secret keys in encryption, steganography and digital watermarking algorithms. Chaotic cards are one of the simplest systems to use for generating a chaotic sequence. In the literature, several one-dimensional (1D), two-dimensional (2D) and three-dimensional (3D) chaotic maps are proposed. In our proposal, we used several one-dimensional logistics maps, each one is defined by:

$$\mathcal{L}_{\mathrm{i}}^{\mathrm{c}}(x_0,\mu_{\mathrm{i}}): \qquad \mathrm{x}_{\mathrm{n}+1} = \mu_{\mathrm{i}} \times \mathrm{x}_{\mathrm{n}}(1-\mathrm{x}_{\mathrm{n}}) \tag{12}$$

Where $\mathrm{x}_{\mathrm{n}} \in [0,\ 1]$ denotes the system state, $x_0 \in [0,\ 1]$ denotes the initial system state and $\mu_{\mathrm{i}} \in [3.57,\ 4]$ is the control parameter. In such systems, x_0 and μ_{i} can be used as a cryptography secret key.

5) Fuzzy commitment: The template protection method during transmission is carried out using the principle of Key binding. In this method, the biometric system is combined with the fuzzy commitment approach to strengthen the system security [32]. Fuzzy commitment uses the biometric data and the cryptographic key to recalculate new biometric data which will then be used for authentication and key release simultaneously in a single step.

- **Key Insertion:** This task is performed only during transmission (transmitter). The system extracts the template for each user using the feature extraction and encoding method (HOG and codebook), resulting in a binary template of size $\eta \times \rho$ (where η is the number of vectors in the biometric template and ρ is the number of bits used to encode the maximum rank in the codebook). A binary vector of size c is then randomly generated, and its coefficients constitute the binary key. Next, a new key C is formed by concatenating several keys, ensuring that the size of C matches the size of the template.

$$\mathrm{C} = [\mathrm{c}, \quad \mathrm{c}, \quad \mathrm{c}, \quad \cdots \quad \mathrm{c}] \tag{13}$$

Now, calculate the offset δ by an exclusive-or (XOR function) between each code coefficient (in the form of a bit) and each Template coefficient. Note that the latter has the advantage of being stable in size and ordered.

$$\delta = \mathrm{V_o} \oplus \mathrm{C} \tag{14}$$

The user's commitment P is then defined as the set of $(\delta, H(c))$, with H is a hash function.

- **Key Extraction:** This task is performed only during reception (receiver). The key (C) extraction process (key recovery operation) in the receiver is shown in Fig. II.2.

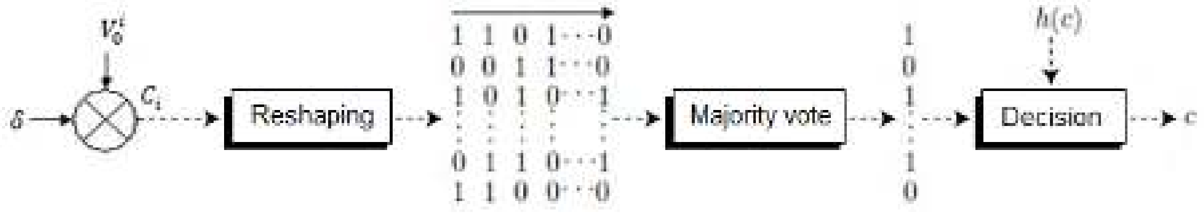


Fig. II.3 Key recovery process

The system examines all models that are already recorded in the database when enrolled in the system. For each sample in the database, calculate the vector C_i by an exclusive-or (XOR function) between the binary string δ and the biometric test model.

$$C_i = \delta \oplus V_0^i \tag{15}$$

Now the key can be recovered. To achieve this, the bits of the binary vector C_i are mapped into a matrix M_x (with a size of $n_1 \times n_2$, where n_1 represents the key length and n_2 is the number of keys in C_i) and key recovery is carried out by taking the majority vote among M_x. After that, to check if the retrieved key (c) is the same as the inserted key $(\tilde{c})$ in the transmitter, the system checks if $H(c) = H(\tilde{c})$. If this key is correct, the system must also extract the biometric template from the binary string δ by:

$$\tilde{V}_o^i = \delta \oplus C_i^1 \qquad \text{with} \qquad C_i^1 = [\text{c}, \quad \text{c}, \quad \text{c}, \quad \cdots \quad \text{c}] \tag{16}$$

Finally, the biometric templates $\tilde{V}_o^i$ and V_0^i must be compared, if they are from the same person, the key can be used to decrypt the message using the AES algorithm. It is important to note that the success of the key extraction process depends on the intra/interclass variation of client users. Thus, it is very necessary to use a very efficient feature extraction technique that reduces intraclass variability and increases interclass variability.

II.5.2 Biometric System

1) Encryption and data transmission side: In the terminal system, the user sends data, such as an image, in an encrypted data format over the network. This system involves two primary steps (Fig. II.3):

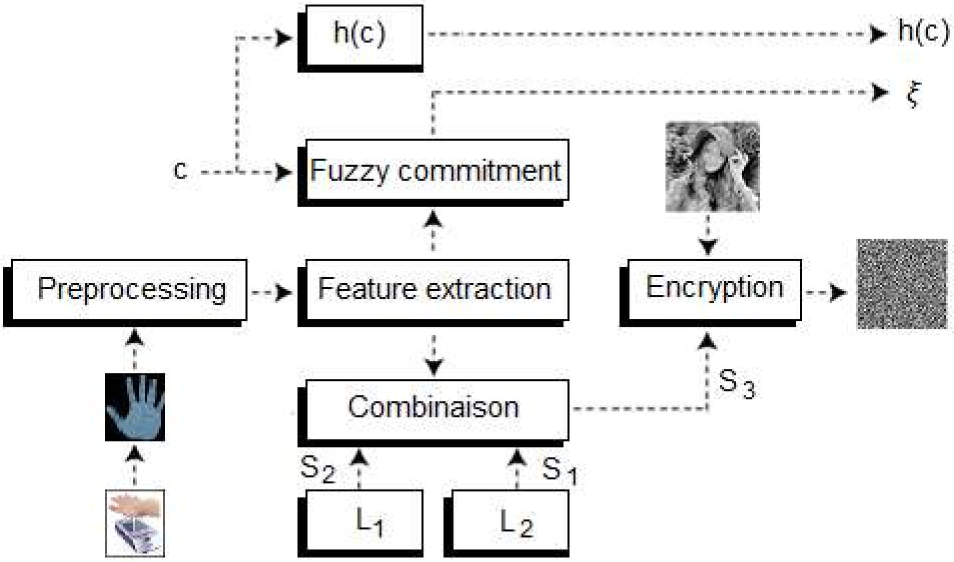


Fig. II.4 Encryption and data transmission side

- ***Verification and Feature Vector Generation:*** Initially, the system verifies and generates the feature vector based on the user's ID card secret code. If the code is correct, a feature extraction technique is applied using the sender's fingerprint method to create the feature vector, which is then compared with the one stored on the ID card. If the card PIN or extracted feature does not match the one on the ID card, access is denied.

- ***Encryption and Transmission:*** Upon successful verification and feature vector extraction, a fuzzy commitment scheme is applied, where the extracted vector is secured using the encryption key (c). A composite function associates the encryption key with the user and calculates the offset (ξ), combining the key and the feature vector. The fuzzy commitment is represented by the pair of feature vector and a one-way hash function ($h(c)$). Importantly, neither the biometric feature nor the key (c) is transmitted publicly.

After the initial verification, the system uses the feature vector and two chaos systems (L_1, L_2) to encrypt the image for secure transmission. Finally, the client sends the offset (ξ), the hash function $h(c)$, and the encrypted image to the destination's central server.

2) Data decryption and user identification side: Upon receipt (Fig.II.4), using users' biometric templates previously stored in the database, the system first attempts to retrieve the key and verify its authenticity using a one-way hash function ($h(c)$).

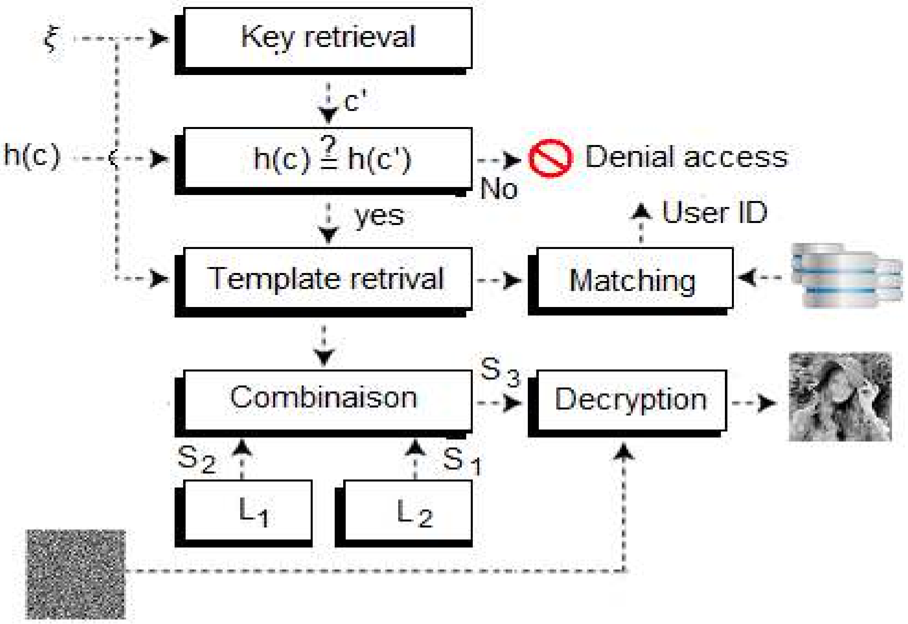


Fig. II.5 Data decryption and user identification side

If the result is positive, this key (c) is used to retrieve the biometric feature vector and compare it with the feature vector corresponding to the user's authentication. The encrypted image is then decrypted using the transmitted feature vector and chaos systems (L_1, L_2).

II.5.3 Cryptography system

Cryptosystems are essential for securing data through two critical phases: encryption and decryption. In the encryption phase, data is transformed into incomprehensible data using an encryption algorithm and a key, ensuring that the data becomes unreadable to unauthorized users. Decryption, the reverse process, converts incomprehensible data back into data using the corresponding decryption algorithm and key, allowing authorized access to the original information.

1) Encryption process: In our system, the image encryption process based on blocks (Fig. II.5), dividing the image into multiple blocks and encrypting each block sequentially based on the encryption of the previous block. This method ensures that each block's encryption is dependent on the prior block, enhancing security through inter-block dependency. The blocks are organized using a chaos sequence algorithm combined with feature vectors to construct a tree structure that determines the encryption sequence. This approach leverages the unpredictability of chaos theory and the specificity of feature vectors to create a robust and secure encryption process.

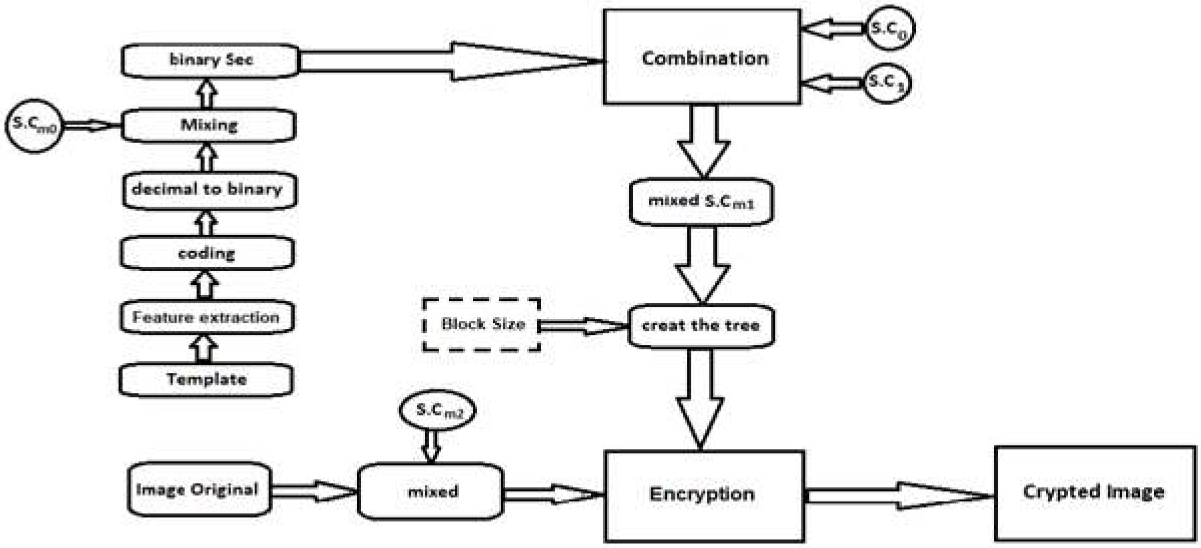


Fig II.6 Image encryption system structure

Fig. II.6 L illustrates the image encryption process. In this system, the biometric template serves as the key for the encryption process. The diagram below depicts the proposed encryption algorithm, which utilizes the biometric template to ensure that the encryption is uniquely tied to the user's biometric data. This method enhances security by making the encryption key specific to the individual, thereby preventing unauthorized access and ensuring that the encrypted data remains protected.

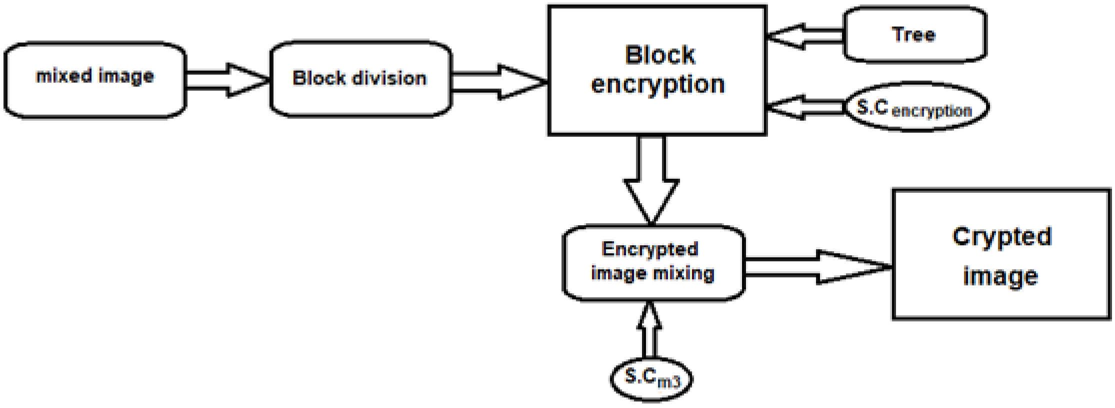


Fig II.7 Image block encryption phase

(1) Load the biometric template $\mathcal{T}$ and the codebook $\mathcal{B}$ to transform it into binary format

$$\mathcal{F}_B\ (\mathcal{T},\mathcal{B}) = \mathcal{T}_B \tag{17}$$

(2) Rearrange the binary sequence with the first chaotic system logistic maps $(\mathcal{L}_m)$ with parameters $(\mathcal{X}_0, \mathcal{U}_m)$.

$$\mathcal{F}_{rea}\left(\mathcal{T}_B, \mathcal{X}_{0_m}, \mathcal{U}_m\right) = \mathcal{T}_r \tag{18}$$

(3) Using the combination of the binary sequence $\mathcal{T}_r$, the second chaotic system $\mathcal{L}_{T_1}$ with parameters $(\mathcal{X}_{0T}, \mathcal{U}_T)$ and a third chaotic system $\mathcal{L}_{T_2}$with parameters $(\mathcal{X'}_{0_T}, \mathcal{U'}_T)$ to create another chaotic system $\mathcal{L}_T$, with the following conditions:

$$\mathcal{F}_{seq}\left(\mathcal{L}_{T_1}, \mathcal{L}_{T_2}, \mathcal{T}_r\right) = \begin{cases} \mathcal{L}_{T_1}(i) & if \quad \mathcal{T}_r(i) = 0 \\ \mathcal{L}_{T_2}(i) & if \quad \mathcal{T}_r(i) = 1 \end{cases} \tag{19}$$

(4) Using the block size $\mathcal{B}_s$ to calculate how many blocks the image $\boldsymbol{\mathcal{I}}$ can be divided into, the first half of the chaotic sequence will be used to determine the tree levels and the second half to calculate the connection between the nodes.

$$\mathcal{F}_{Tree}(\mathcal{B}_s, \mathcal{L}_T) = Tree \tag{20}$$

(5) A rearrange step is performed on image $\mathcal{I}$ using a fourth chaotic system $\mathcal{L}_{T_m}$ with parameters ($\mathcal{X}_{0_r}, \mathcal{U}_r$).

$$\mathcal{F}_{mix}(\mathcal{I}, \mathcal{X}_{0_r}, \mathcal{U}_r) = \mathcal{I}_m \tag{21}$$

(6) The shuffled image $\mathcal{I}_m$ will be divided into several blocks chained together by the $Tree$ which will decide the parents' block and the children blocks.

$$\mathcal{F}_{blocks}(\mathcal{I}_m, Tree) = \left\{\mathcal{B}_{\mathcal{P}},\ \mathcal{B}_{\mathcal{C}}, \mathcal{B}_{c_1}, \mathcal{B}_{c_2}, \dots, \mathcal{B}_{c_{\mathcal{N}}}\right\} \tag{22}$$

(7) Including the fifth chaotic system with parameters ($\mathcal{X}_{0_\mathcal{C}}, \mathcal{U}_\mathcal{C}$) to generate chaotic slaves as the same number of blocks $\mathcal{N}$.

$$\mathcal{F}_{chao}(\mathcal{N},\ \mathcal{X}_{0_\mathcal{C}}, \mathcal{U}_\mathcal{C}) = \{\mathcal{L}_{\mathcal{S}_1},\ \mathcal{L}_{\mathcal{S}_2}, \dots, \mathcal{L}_{\mathcal{S}_\mathcal{N}}\} \tag{23}$$

(8) Parents block $\mathcal{B}_\mathcal{P}$ encryption will be the projection of blocks in the $\mathcal{Q}$ matrix of the first chaotic share $\mathcal{L}_{\mathcal{C}_1}$.

$$\{\mathcal{Q}_\mathcal{P}, \mathcal{R}_\mathcal{P}\} = \mathcal{qr}\left(\mathcal{L}_{\mathcal{S}_1}\right), \qquad \mathcal{C}_\mathcal{p} = \ \mathcal{B}_\mathcal{p} * \mathcal{Q}_p \tag{24}$$

(9) The encryption of the children block $\mathcal{B}_{c_n}$ will be connected with the parent block $\mathcal{B}_\mathcal{P}$ of each child as shown in the tree in the figure. And the $\mathcal{Q}$ matrix of its corresponding chaotic slave as demonstrated below:

$$\{\mathcal{Q}_\mathcal{P}, \mathcal{R}_\mathcal{P}\} = \mathcal{qr}\left(\mathcal{L}_{\mathcal{S}_1}\right), \qquad \mathcal{C}_c = ((\mathcal{B}_\mathcal{p} *\ \mathcal{Q}_\mathcal{P}) + \mathcal{B}_{c_n}) \tag{25}$$

(10) After encrypting all the blocks one by one the reconstructed image $\mathcal{I}_\mathcal{R}$ after arranging the block will be shuffled using the sixth chaotic system $\mathcal{L}_\mathcal{K}$ with the parameters ($\mathcal{X}_{0_\mathcal{K}}, \mathcal{U}_\mathcal{K}$) to get the final encrypted image $\mathcal{J}_\mathcal{C}$.

$$\mathcal{F}_{Shuf}\left(\mathcal{I}_\mathcal{R}, \mathcal{X}_{0_\mathcal{K}}, \mathcal{U}_\mathcal{K}\right) = \ \mathcal{J}_\mathcal{C} \tag{26}$$

2) Image Decryption: During the decryption process (Fig. II.6), the biometric template acts as the key to unlock the encrypted image. Once the template undergoes binarization to convert it into a binary format, it is employed to reverse the encryption, guaranteeing that solely the accurate biometric data can decrypt the image successfully.

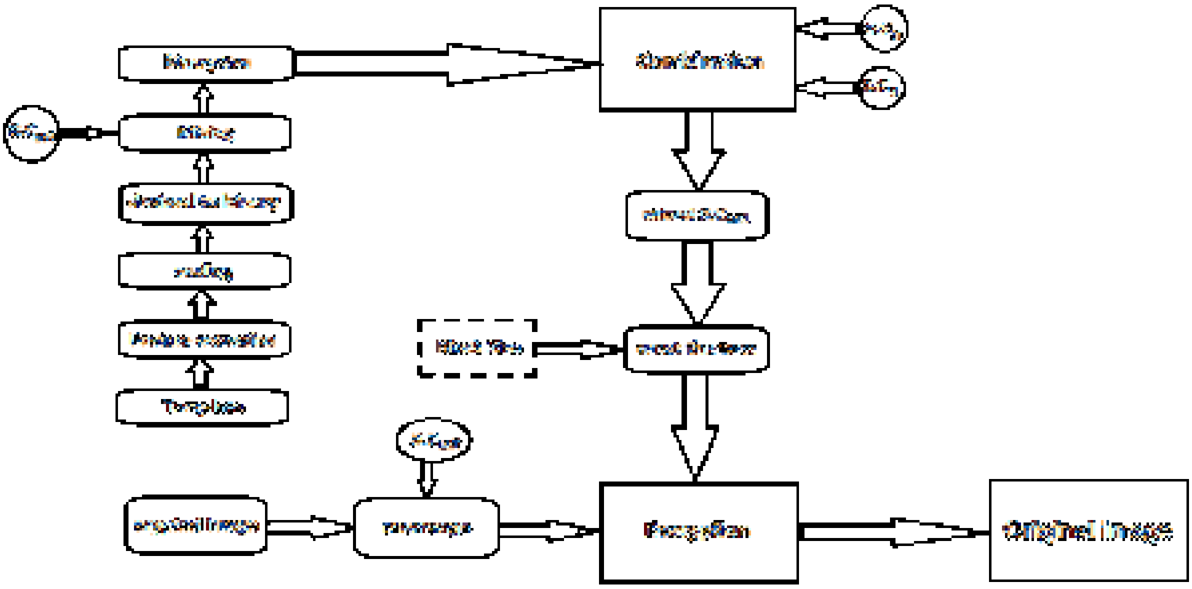


Fig II.8 Image decryption system structure

The decryption algorithm, depicted in the block diagram below (Fig. II.7), precisely reconstructs the original image from the encrypted data. This approach guarantees a high level of security since the distinct biometric template serves as a strong key that is challenging to replicate or counterfeit.

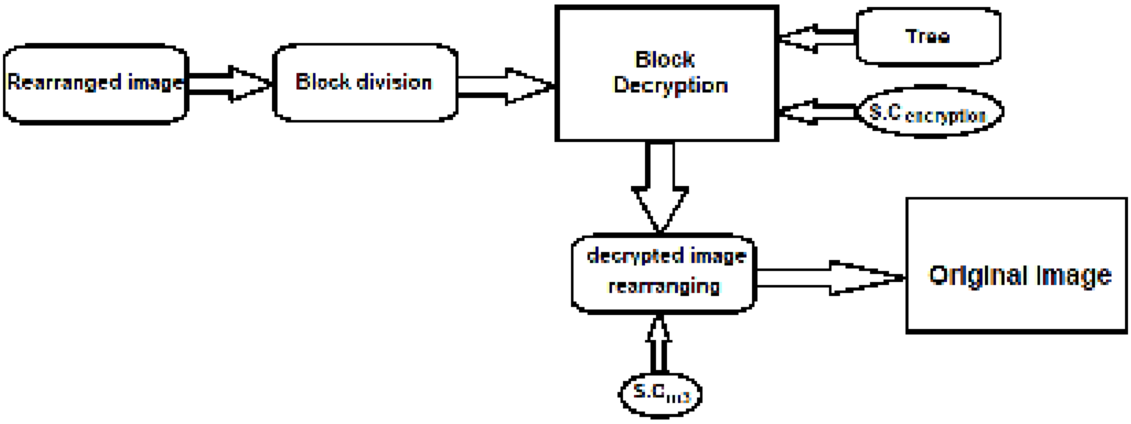


Fig II.9 Image block encryption phase

(1) Load the biometric template $\mathcal{T}$ and the codebook $\mathcal{B}$ to transform it into binary format.

$$\mathcal{F}_B\ (\mathcal{T},\mathcal{B}) = \mathcal{T}_B \tag{27}$$

(2) Rearrange the binary sequence with the first chaotic system (logistic maps,$\mathcal{L}_m$) with parameters $(\mathcal{X}_0, \mathcal{U}_m)$.

$$\mathcal{F}_{rea}\left(\mathcal{T}_B, \mathcal{X}_{0_m}, \mathcal{U}_m\right) = \mathcal{T}_r \tag{28}$$

(3) Using the combination of the binary sequence $\mathcal{T}_r$, the second chaotic system $\mathcal{L}_{T_1}$ with parameters $(\mathcal{X}_{0T}, \mathcal{U}_T)$ and a third chaotic system $\mathcal{L}_{T_2}$ with parameters $(\mathcal{X}'_{0_T}, \mathcal{U}'_T)$ to create another chaotic system $\mathcal{L}_T$, with the following conditions:

$$\mathcal{F}_{seq}\left(\mathcal{L}_{T_1}, \mathcal{L}_{T_2}, \mathcal{T}_r\right) = \begin{cases} \mathcal{L}_{T_1}(i) & if \quad \mathcal{T}_r(i) = 0 \\ \mathcal{L}_{T_2}(i) & if \quad \mathcal{T}_r(i) = 1 \end{cases} \tag{29}$$

(4) Using the block size $\mathcal{B}_s$ to calculate how many blocks the image $\mathcal{I}$ can be divided into, the first half of the chaotic sequence will be used to determine the tree levels and the second half to calculate the connection between the nodes.

$$\mathcal{F}_{Tree}(\mathcal{B}_s, \mathcal{L}_T) = Tree \tag{30}$$

(5) A rearrange step is performed on the encrypted image $\mathcal{J}_C$ to restore the original order of encrypted blocks $\mathcal{B}_C$ using the chaotic system $\mathcal{L}_K$ with parameters ($\mathcal{X}_{0_K}, \mathcal{U}_K$).

$$\mathcal{F}_{Rea}(\mathcal{I}_C, \mathcal{X}_{0_K}, \mathcal{U}_K) = \mathcal{I}_R \tag{31}$$

(6) The block decryption phase will be performed by reversing the encryption phase as shown below by starting from the parent block. $\mathscr{qr}$ decomposition of the first chaotic slave:

$$\{\mathcal{Q}_{\mathcal{P}}, \mathcal{R}_{\mathcal{P}}\} = \mathscr{qr}(\mathcal{L}_{\mathcal{S}_1}) \quad , \quad \mathcal{B}_{\mathcal{P}} = \mathcal{C}_{\mathcal{P}} * \mathcal{Q}'_{\mathcal{P}} \tag{32}$$

(7) The children blocks will be decrypted by inversing the previous encryption process and by obtaining the decrypted parent block as follow:

$$\{\mathcal{Q}_{\mathcal{S}}, \mathcal{R}_{\mathcal{S}}\} = \mathscr{qr}(\mathcal{L}_{\mathcal{S}_{\mathcal{N}}}) \tag{33}$$

$$\mathcal{B}_{\mathcal{P}} = (\mathcal{C}_{\mathcal{S}} * \mathcal{Q}'_{\mathcal{S}}) - (\mathcal{B}_{\mathcal{P}} * \mathcal{Q}_{\mathcal{P}})$$

(8) After obtaining the decrypted blocks and reconstruction the image $\mathcal{I}_m$, another rearrange process is conducted to restore the decrypted image using the chaotic system $\mathcal{L}_{\mathcal{M}}$ with the parameters ($\mathcal{X}_{0_r}, \mathcal{U}_r$).

(9)

$$\mathcal{F}_{restor}(\mathcal{I}_m, \mathcal{X}_{0_r}, \mathcal{U}_r) = \mathcal{I} \tag{34}$$

Conclusion

The combination of biometric systems with cryptography, particularly utilizing chaos-based cryptographic methods like the logistic map, has sparked a revolution in security and identity verification. By intertwining distinctive biometric identifiers with sophisticated encryption techniques, biometric cryptosystems offer a potent defense against unauthorized access and cyber threats. The intricate processes of key generation, template protection, and encryption safeguard the confidentiality, integrity, and uniqueness of biometric data, fortifying the overall security framework. Furthermore, the integration of advanced machine learning algorithms into palmprint recognition systems signifies the ongoing evolution and innovation in biometric security technologies. This seamless collaboration between biometric systems and cryptography not only establishes a resilient security infrastructure but also enhances the safeguarding of sensitive data, effectively mitigating vulnerabilities to breaches and unauthorized intrusions.

Chapter 3

Experimental Results

Abstract

Recently, in the field of cybersecurity, biometric technologies are increasingly used due to their impacts on the degree of security and reliability of the information security system. In this chapter, we will show the results of our experiments on a typical database, which indicate that the contribution we proposed is robust and gives good results comparable to several state-of-the-art works. By showcasing the performance and effectiveness of our biometric authentication system, we aim to provide valuable insights into its potential applications and implications for bolstering cybersecurity defenses in various domains.

Introduction

Biometric cryptosystems are increasingly used due to their significant impact on the reliability of information security. A biometric cryptosystem must meet two essential constraints: the precision required by the biometric system and the robustness of information security. In this chapter, we focus on discussing the performance of our proposed biometric system based on palmprint, as well as the level of security it achieves. The experiments conducted in this chapter, which are based on a recent biometric database, demonstrate that our method is more efficient than several existing methods.

III.1 Dataset Description

The aim of this section is to evaluate the performance of the proposed biometric system. The experiments were conducted using the *Tongji Contactless Palmprint Dataset* [34], which is a publicly available dataset comprising 12,000 images from 600 different palms. The dataset includes data from a diverse group of 300 volunteers (192 males and 108 females) ranging in age from 20 to 50 years old, with 235 volunteers aged between 20 and 30 and the remaining between 30 and 50. Data collection involved two separate sessions to capture samples of both left and right palms. Each volunteer provided 10 images per palm in each session, resulting in a total of 40 images per individual. The time interval between the first and second sessions averaged approximately 61 days, with the shortest interval being 21 days and the longest being 106 days.

III.2 Test Protocol

The comprehensive test protocol ensured a systematic evaluation and validation of the biometric authentication system, offering valuable insights into its performance and potential applications in information security. Thus, to test the performance of our proposed biometric system, we divided the database into two sets for each palm (left and right). The first set, representing 50% or 3000 images equally distributed among all participants (10 images per person), was used for the enrollment phase. The remaining set, also 50% or 3000 images (10 images per person), was used for the testing phase. This division allowed us to obtain a total of 451,500 scores for each palm. Among these scores, 3000 are genuine scores and 448,500 are imposter scores.

III.2.1 Test methodology

The biometric system's performance was evaluated in both open-set and closed-set modes, taking into account various environmental factors and user interactions to ensure its robustness. Additionally, the encryption system's resilience against several potential cyber-attacks was assessed. These rigorous testing procedures provide a comprehensive understanding of the system's capabilities and areas needing improvement, guiding future enhancements. This thorough evaluation not only demonstrates the system's current efficacy but also informs strategic directions for its ongoing development and optimization.

We divided our series of tests into two main parts: evaluating the performance of the biometric system and assessing the performance of the encryption system. The first part is further divided into three sub-parts. In the first sub-part, we conducted several experiments to determine the optimal parameters for the feature extraction method applied to the entire image. In the second sub-part, we examined the system's performance using block-based image analysis with the best-selected parameters of feature extraction method. Finally, the third sub-part focuses on quantifying the feature vector and evaluates the biometric system's performance using the codebook. The second part of our experiments evaluates the robustness of the encryption system.

III.2.2 Performance Metrics

Evaluating the performance of a biometric system is a critical phase in its design and implementation, as it determines whether the system is adequately efficient for its intended use. It also enables the comparison of different systems. This performance is primarily assessed through various metrics and can be visualized using different performance curves.

In the open-set identification mode, the False Accept Rate (FAR) [35] and False Reject Rate (FRR) [35] are crucial metrics for assessing the system's security and user accessibility, respectively. The Equal Error Rate (EER) [35], where FAR equals FRR, offers a comprehensive measure of the system's overall accuracy. Additionally, the Genuine Accept Rate (GAR) indicates the system's effectiveness in correctly identifying legitimate users. In the closed-set identification mode, the most commonly used evaluation metrics are Rank-One Recognition (ROR) and Rank of Perfect Recognition (RPR).

Performance curves make it possible to represent performance for all threshold values without setting an a priori threshold. In the open-set identification mode, the Receiver Operating Characteristic (ROC) curve helps visualize the trade-off between FAR and FRR, facilitating the selection of an optimal operating point. Conversely, in the closed-set identification mode, the Cumulative Match Characteristic (CMC) curve is utilized to illustrate performance.

III.3 Tests Results

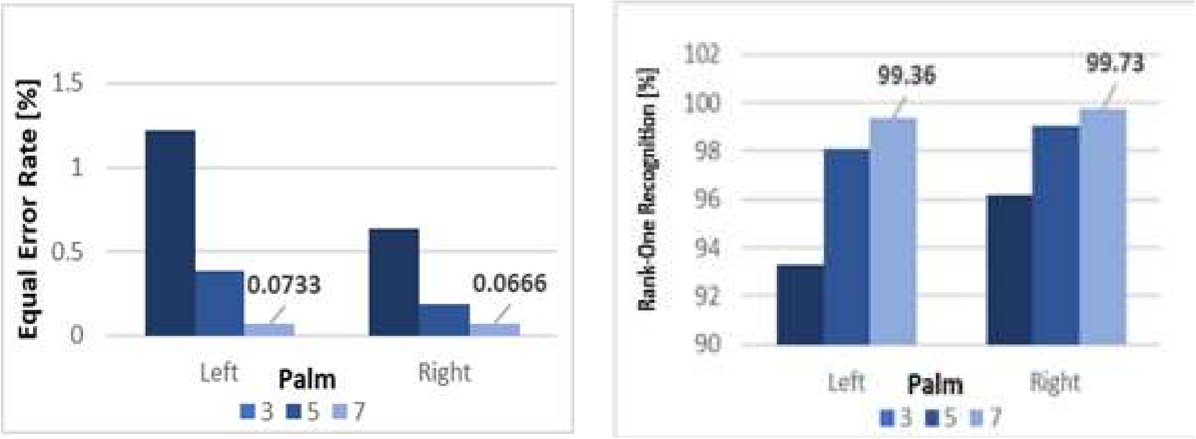
Assessing a system's performance is indeed crucial in its design and implementation, allowing us to ascertain its suitability for the intended application. In this section, we'll evaluate the biometric cryptosystem from two main perspectives: the performance of the biometric system itself and the level of security provided by its cryptography. This section aims to test the proposed biometric cryptosystems. As mentioned earlier, it is divided into two main parts: the first part involves preliminary experiments to assess the performance of the biometric system, while the second part focuses on evaluating the performance of the encryption algorithm.

III.3.1 Biometric System Performance Evaluation

Biometric systems, utilizing distinctive characteristics for identification purposes, require evaluation to ensure they meet essential standards of accuracy, reliability, and user convenience. As previously mentioned, this part is divided into three subparts, arranged in a sequence that enables us to fulfill all requirements, which are Whole Image Analysis (HOG-I), Block Based Image Analysis (HOG-B): and Codebook based image analysis (HOG-Q). The primary goal is to represent the biometric modality with a distinctive biometric feature vector of small size.

1) HOG-I based biometric system: In biometrics, it is difficult to obtain an exact result for a person recognition system. This is mainly due to the choice of features that should accurately represent person's identities. This choice is important because it conditions the entire methodology used for recognition. Thus, as we showed in the previous section, our method (HOG) includes two parameters (number of zones $p = \mathcal{w} * \mathcal{w}$ and number of bins) to control the precision of the extracted biometric feature vector. It is therefore imperative to evaluate the performance of the identification system to select the appropriate parameters giving the best results. Mathematically, there is no magic formula to directly determine the optimal settings that provide the best system performance. In general, in these cases, experimental tests are carried out by varying the different parameters in predefined sets and then selecting the combination that optimizes an objective function (empirical tests). It should be noted that our tests are carried out on a biometric identification system based on the right palm of the palmprint, which operates in open-set/closed-set modes. Additionally, one parameter was examined and chosen for the HOG-based feature extraction method, which is the number of regions (w). Furthermore, the cryptosystem biometric system is developed and implemented using MATLAB 2015a on a Windows 10 platform and an embedded PC with a 2.2 GHz Intel Pentium processor with 6 GB DRAM.

In this subsection, we attempt to select the number of regions (w) from among three predefined values ($w = 3, 5, 7$), resulting in (9, 25, and 49 regions). It is important to note that our systems utilize the DRB classifier due to its efficiency in classification applications. To examine the effect of this parameter on the accuracy of the biometric identification system (both open-set and closed-set modes), we illustrate the performance of the systems in terms of EER and ROR for different palms (right and left) in Fig. III.3.



(a) *(b)*

Fig III.1 HOG-I Based Biometric Identification System performance. *(a)* Open-set biometric identification system and *(b)* Closed-set biometric identification system

From these Figures, we can make three important observations:

- A very acceptable performance can be achieved with all possible values of w, where an effective error rate (open-set), EER, of less than 1.500% has already been obtained.
- In general, the higher the number of regions, the lower the error rate. The best results were obtained with 49 regions ($w = 7$), which is better than the performance achieved with 9 regions ($w = 3$).

- A similar performance is achieved when configuring the system in closed-set identification mode. The system's performance can also be improved with 49 regions ($w = 7$), which can deliver excellent results.

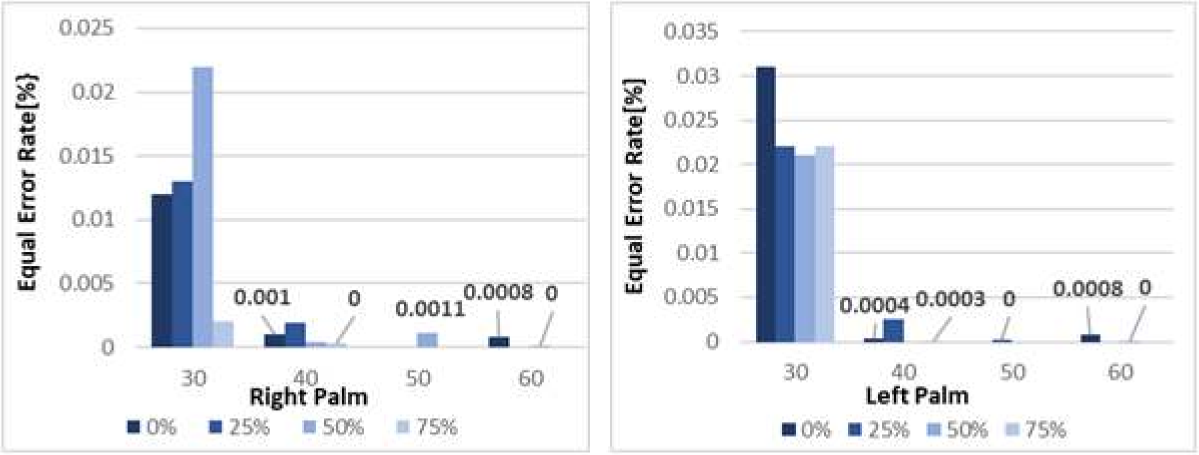
According to Fig. III.1.*(a),* it is clear that 49 zones offer better results in terms of EER. In this case, the open-set identification system can achieve an error rate (EER) of 0.0733% (at a threshold T_0 equal to 0.9013) and 0.0666 ($T_0 = 0.8771$) for systems based on the right and left palm, respectively. Improvements of 94.43% and 94.94% can be obtained compared by case of using 9 zones; the system therefore operates with an EER of 1.2170% ($T_0 = 0.923$). We also examined the closed-set identification mode, and for both biometric modalities (right palm and left palm), the system continues to perform efficiently with a Rank-One Recognition (ROR) of 99.36% and 99.73%, and a Perfect Recognition (RPR) of 111 and 109, respectively.

The experimental results tests obtained in this part clearly indicate that the use of palm-based biometric modalities in conjunction with the feature extraction method based on the HOG technique can provide better performance. This can lead to an efficient biometric system that can be used in many applications requiring high security, especially if these applications deal with small or medium-sized databases.

In most image recognition systems, block-based image analysis has evolved as a processing paradigm over the past decade. It has been widely used in image processing, particularly for data compression and pattern recognition. Therefore, in the following subpart, we attempt to improve the system performance using block-based image analysis.

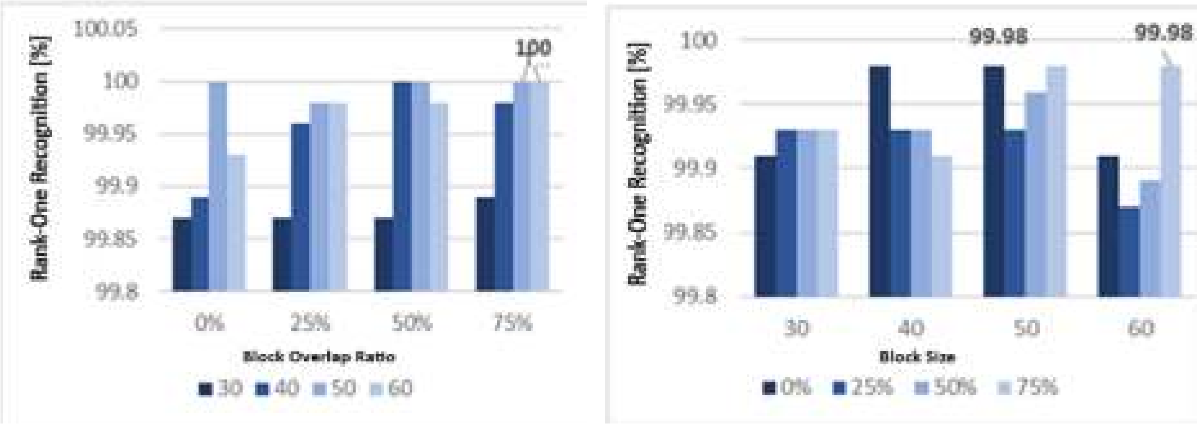
2) HOG-B based biometric system: In block-based analysis, the image is divided into sub-images or smaller blocks. Indeed, the computational time and memory space required for image processing are crucial. Therefore, it is more practical to process several sets of reduced data rather than the entire image. In this part of the tests, the effectiveness of block-based image analysis in the biometric identification system will be evaluated. Thus, in our experiments, we adopted the following strategy: For each block size from the set ({30×30, 40×40, 50×50, 60×60}), the original image (right palm and left palm) is divided into blocks with one of the four provided overlap rates ({0%, 25%, 50%, 75%}). The EER and ROR are then calculated after performing HOG (best case previously selected, w = 9) on the blocks. For each biometric modality, 16 tests can be performed, and the parameters (block size and overlap rate) with the lowest EER values are chosen as the best settings. In Fig. III.2 and Fig. III.3, the performance of the open-set and closed-set biometric identification system (EER and

ROR) is plotted against block size and block overlap for both identification biometric modalities (right palm and left palm).



(a) *(b)*

Fig III.2 HOG-B Based open-set identification biometric system. *(a)* Right palm based biometric system, and *(b)* Left palm based biometric system.

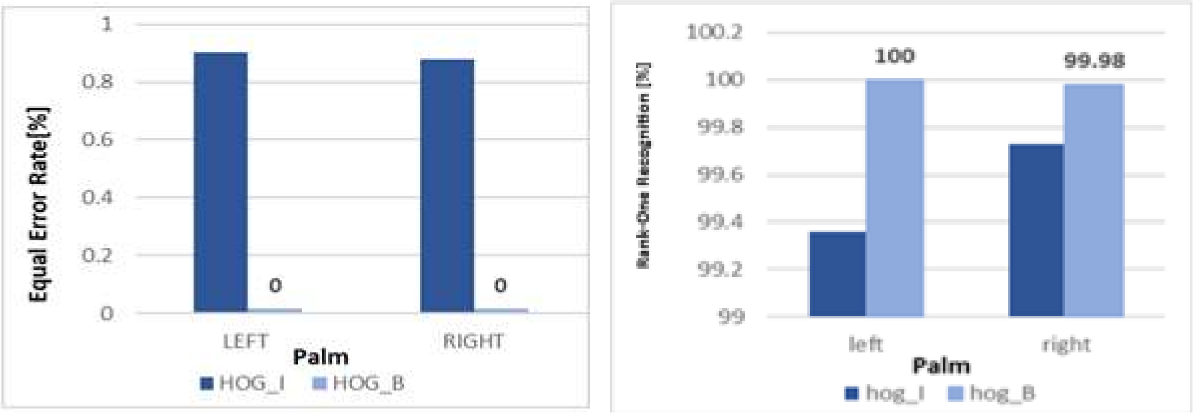


(a) *(b)*

Fig III.3 HOG-B Based closed-set identification biometric system. *(a)* Right palm based biometric system, and *(b)* Left palm based biometric system.

For the open-set identification mode, by observing and analyzing Fig. II. *(a)* and Fig. II. *(b),* we can see that: *(i)* In the case of the right palm, block-based analysis significantly increased the system's performance (improvement of 100.00%) compared to whole image analysis. In the best case (40×40 and 75% overlap), the system can operate with perfect error values (EER, T_0) of (0.000%, 0.99), and *(ii)* a block size of 50×50 with 75% overlap is best for the left palm, where an EER improvement of 100.00% was obtained. Thus, the system can operate with values (EER, T_0) of (0.000%, 0.939).

In previous experiments, the performance of the open-set identification system was examined. Here, we will try to determine the optimal values for block size and overlap degree to achieve the best performance in closed-set identification. In these tests, we will examine the same block size and overlap values, and the results obtained after testing all the values are presented in Fig. III.3. From this figure, compared to previous results, we can easily see that the performance of the closed-set identification system is improved by 100.00%. It is clear that in both cases (right palm and left palm), a block size of 60×60 with 75% overlap produced the best results. In the case of the left palm, the system operates with values (ROR, RPR) of 100.00%, 1. And with values (ROR, RPR) of 99.98 %, 3 for the right palm, the system can also operate with the same rate values. Fig. III.4. *(a)* et Fig. III.4. *(b)* compares the two approaches: whole image analysis and block-based analysis. In this figure, the significant difference between the two approaches and the ideal improvement achieved are clearly visible.



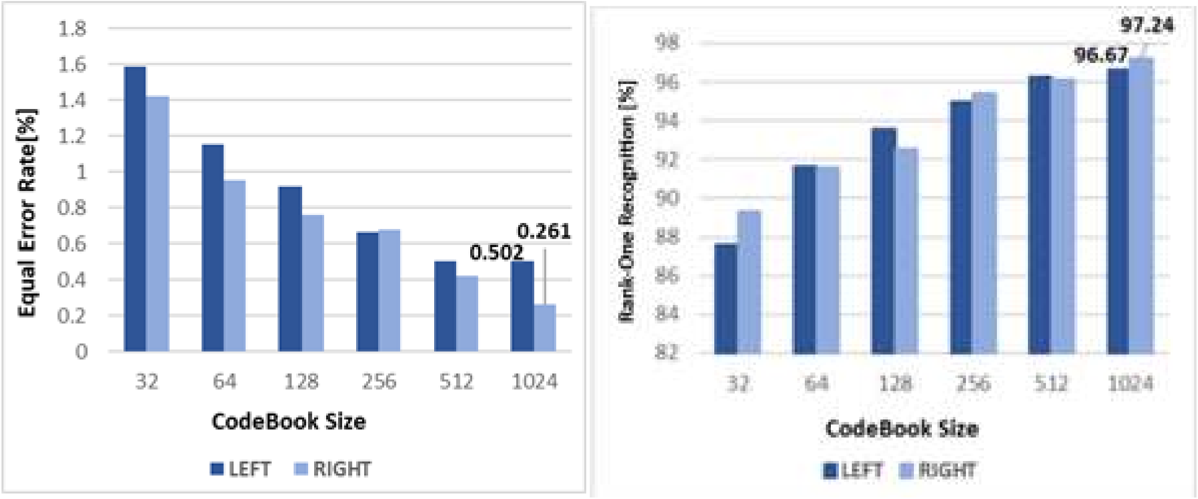
(a) *(b)*

Fig III.4 Comparison of whole image-based analysis and block-based analysis. *(a)* Open-set biometric identification system, and *(b)* Closed-set biometric identification system

The biometric feature vector in our study plays a major role in the data encryption process for the transmitted image, as it is used to produce the tree that determines the sequence of image blocks. Thus, the process of determining this tree depends on certain relationships between the components of a sequence produced using two chaos systems and a feature vector with binary components. Since the biometric feature vector components contain real and large components, they must be transformed into a binary feature vector. The proposed method is based on a codebook that quantizes the sub-vectors in the feature vector. In the next series of experiments, we will re-evaluate the biometric system based on the codebook.

3) HOG-Q based biometric system: In a biometric system, the final representation of image features has a significant impact on the system's identification rate. Since the proposed method depends on several factors, we conducted experimental tests to select the best factors that could improve the system's accuracy. It should be noted that the previously selected parameters, namely the block analysis size and the overlap ratio between blocks, were used. In these tests, we will try to choose the codebook length from the predetermined lengths, which are {128, 256, 512, 1024}.

By altering this parameter, numerous feature representations can be generated. Experimentally, we can select the optimal codebook size that enhances the system's accuracy by adjusting the codebook size and opting for the one that delivers the best performance. Thus, in order to see the effect of codebook length on the biometric system performance, we clearly illustrate, in Fig. III.5, the results of the open-set/closed-set identification system. From these curves, we can find two important cases: *i)* Acceptable performance is achievable across all potential codebook lengths, as an effective error rate (EER) below 1.600% has already been attained in the open-set identification system. Similarly, in the closed-set identification system, the same trend was observed, with the system consistently operating at a rate exceeding 68.00% for both the right and left palms, and *ii)* typically, a smaller codebook length results in a higher EER (as well as ROR). In the case of the open-set identification system, the average EER achieved with a codebook length of 1024 is superior to those attained with a codebook length of 32.



(b) *(b)*

Fig III.5 HOG-Q Based biometric identification system performance. *(a)* Open-set biometric identification system, and *(b)* Closed-set biometric identification system

In the best case (codebook length equal to 1024), the system operates with minimum error rates (EER) of 0.261% (T_0= 0.892) and 0.502% (T_0= 0.842) in the open-set identification system (see Fig. III.5. *(a)*) for the right palm and left palm, respectively. In the closed-set biometric identification mode (see Fig. III.5. *(b)*), the biometric system operates with 97.240% (RPR = 71) and 96.670% (RPR = 109) for the right palm and left palm, respectively Fig. III.6. *(a)* and Fig. III.6. *(b)* also compare the two approaches: block-based analysis and codebook-based analysis.

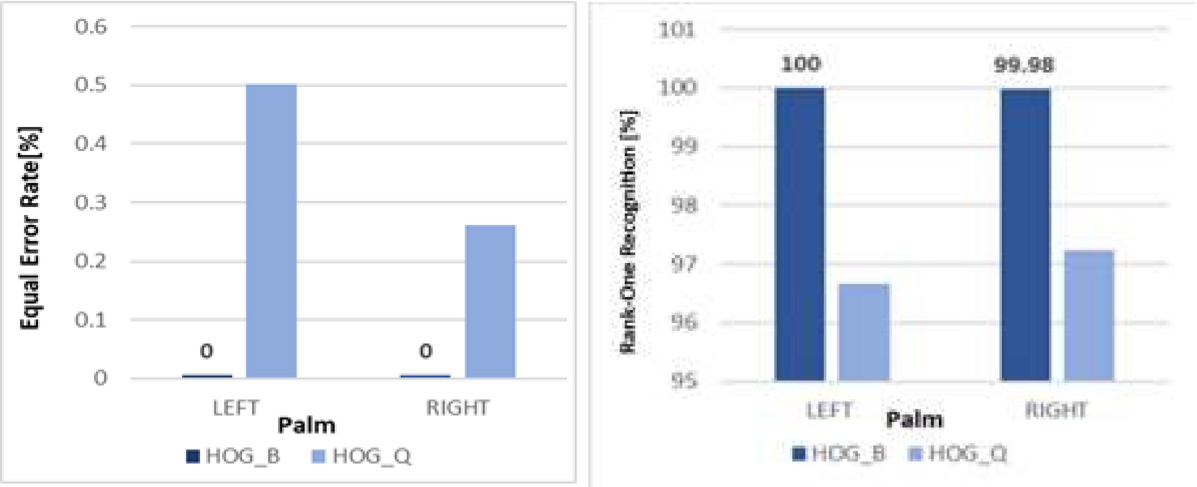


Fig III.6 Comparison of block-based analysis and codebook-based analysis. *(a)* Open-set biometric identification system, and *(b)* Closed-set biometric identification system.

From this figure, it is clear that the performance of the codebook-based biometric identification system has slightly deteriorated compared to the system based directly on biometric feature vectors. However, this result is still very effective because the size of the biometric feature vector has been significantly reduced and is now ready to be used in the encryption process. Furthermore, since our biometric identification system relies on coding the biometric feature vector using the codebook, it is easily capable of producing revocable biometric feature vectors to enhance the security of the biometric identification system, which can be achieved by reorganizing the codebook vectors.

The proposed biometric identification system demonstrated significant improvements in both open-set and closed-set identification modes when optimal parameters were employed. For open-set identification, using a codebook length of 1024 resulted in remarkably low error rates (EER) of 0.261% for the right palm and 0.502% for the left palm. Similarly, in closed-set identification, the system achieved high performance rates of 97.240% and 96.670% for the right and left palms, respectively. Finally, Figures III.7.*(a)* and III.7.*(b)* compare all the proposed methods using Detection error tradeoff (DET) curve (for open-set identification system) and Cumulative Match Curve (CMC) (for closed-set identification system).

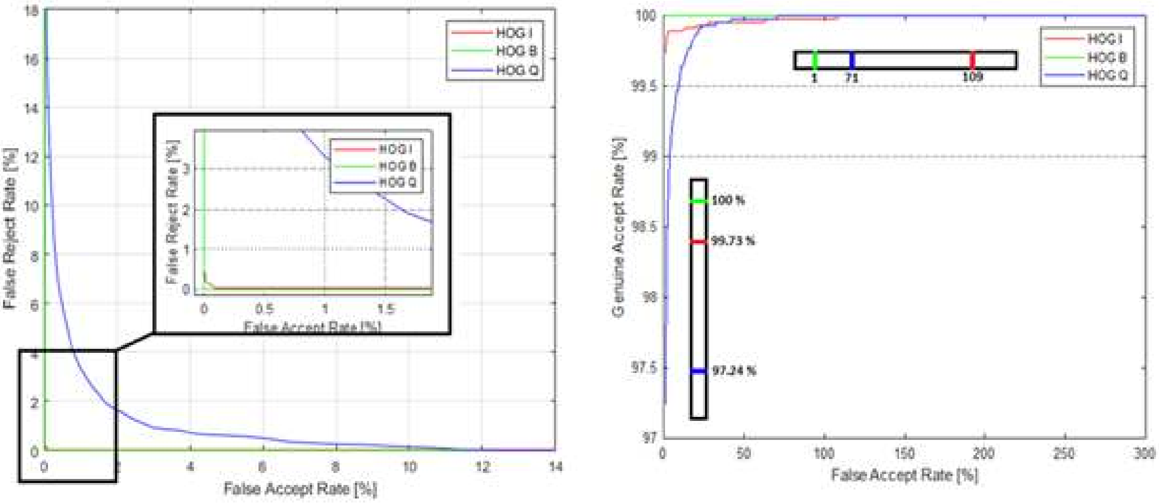


Fig III.7 Biometric identification system performance. *(a)* Open-set biometric identification system, and *(b)* Closed-set biometric identification system

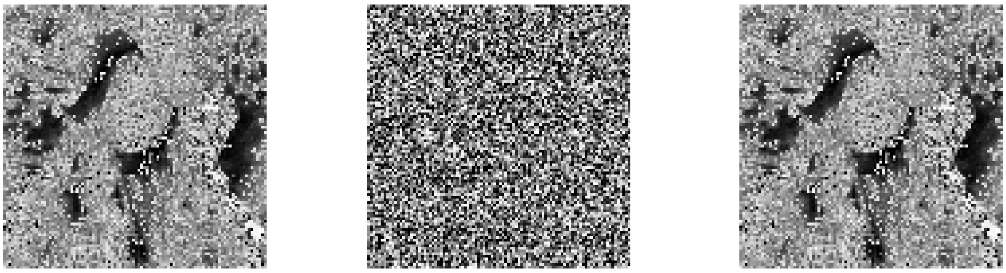
From these figures, we can see the effectiveness of the proposed system, as the efficiency of the methods based on feature vectors is directly demonstrated. These results emphasize the importance of selecting appropriate parameters and highlight the system's strong performance across different configurations, indicating its potential for high-security applications requiring precise biometric identification.

Our biometric identification system is now ready to produce binary biometric feature vectors and is capable of working with high accuracy in both open-set and closed-set identification modes. These biometric feature vectors are used to produce the encryption tree, so in the next part, we will evaluate the security level of the data encryption.

III.3.2 Encryption Algorithm Performance Evaluation

The main objective of our cryptosystem is to ensure remote user authentication and the integrity of transmitted data (encrypted image). In this section, we will conduct a security analysis to test the robustness of our proposals against potential attacks. Generally, to ensure security, three aspects of the system design must be verified: *i)* the robustness of the encryption algorithm against different attacks, *ii)* the impossibility of finding biometric feature vectors through exhaustive search, meaning the key space must be very large, and *iii)* a small modification of the secret key should produce completely different feature vectors.

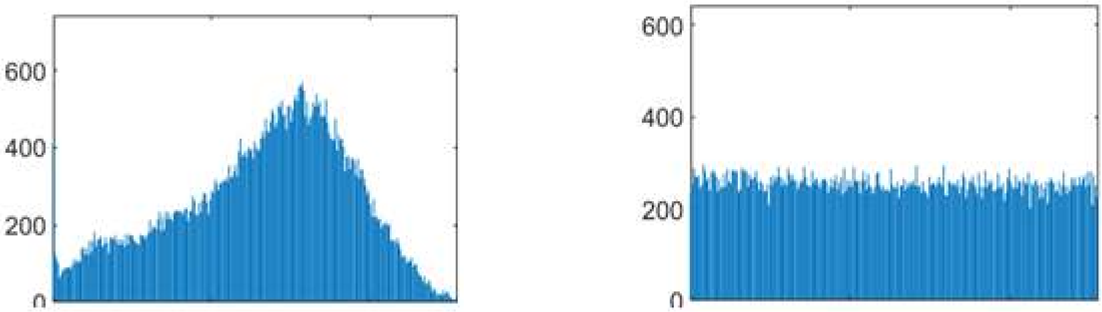
Fig. III.8 shows a test image of size 256 × 256. In the encryption process, multiple chaos systems were used. In this example, the following parameters were defined: the values [0.64, 3.94] for the initial logistic map used to shuffle the images to be encrypted; {[0.74, 3.92], [0.09, 3.78]} to create the tree used in the encryption process; [0.50, 3.82] for block encryption; and [0.48, 3.62] for shuffling the encrypted images. It should also be noted that the encryption process is performed using blocks of size 64 × 64 pixels.



(a) *(b)* *(c)*

Fig III.8 Encryption and decryption of a sample image, *(a)* Original image, *(b)* Encrypted image and *(c)* Decrypted image.

- **Histogram Analysis:** The histogram of an image visually represents the intensity levels of its pixels [36]. A grayscale image typically has 256 distinct intensities, so its histogram displays these intensities and how pixels are distributed among them. Fig. III.9 illustrates that, unlike the histograms of the original image, the distribution of grayscale values in the encrypted image is uniform. Some grayscale values between 0 and 255 are absent in the original image, whereas in the encrypted image, all grayscale values are uniformly spread between 0 and 255. This demonstrates that the resulting image thwarts attackers from launching a statistical attack against the encryption method.



(a) *(b)*

Fig III.9 Histograms comparison. *(a)* Original image and *(b)* Encrypted image

- **Information Entropy Analysis:** The uncertainty level of the encryption scheme is used to determine the information entropy [37]. It is employed to determine the algorithmic efficiency of image encryption, serving as a statistical measure of unpredictability and describing the texture of the input image. An ideal encrypted image should have an entropy of 8, indicating an unexpected source. However, achieving ideal information entropy is impractical. Table III.1 shows the results obtained for 50 test iterations.

Table III.1. Entropies obtained after 50 iterations

	Min	Max	Average
Information Entropy	7.9884870	7.9912799	7.990227348

- **Structural similarity index measure:** The Structural Similarity Index Measure (SSIM) serves as a robust method for predicting the perceived quality of digital television, cinematic images [38], and various other types of digital images and videos. Its utility extends to measuring the similarity between two images, providing valuable insights into their perceptual similarity. The SSIM values obtained serve as invaluable metrics for assessing the fidelity and similarity between images. Table III.2 illustrates the SSIM values after 50 iterations.

Table III.2. SSIM obtained after 50 iterations

	Min	Max	Average
SSIM	0.4559 %	0.9072 %	0.6036 %

- **Peak Signal-To-Noise Ratio:** The term PSNR stands for Peak Signal-to-Noise Ratio, which expresses the ratio between the maximum possible value (power) of a signal and the power of the distortion noise affecting the quality of its representation. To this end, we conducted 50 iterations to observe the PSNR values for each test [39], as indicated in Table III.3.

Table III.3. PSNR obtained after 50 iterations

	Min	Max	Average
PSNR	6.544 dB	6.739 dB	6.632 dB

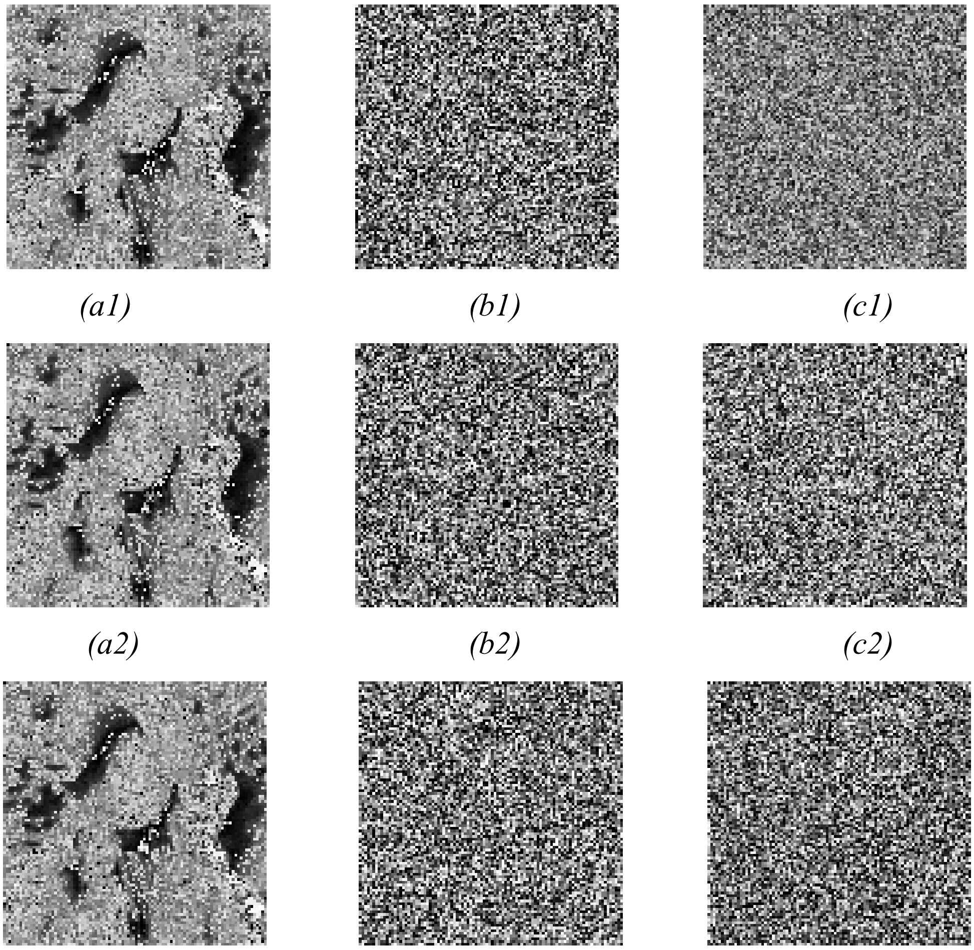
- **Differential Attack:** By changing some of the original, unmodified pixels in the image, an adversary can gain useful information. Evaluations of the resilience of the simple encrypted image to differential attacks often use metrics such as the Number of Pixel Changing Rate

(NPCR) and the Unified Average Changed Intensity (UACI) [40]. Table III.4 shows the NPCR and UACI obtained after 50 iterations.

Table III.4. NPCR and UACI obtained after 50 iterations

	Min	Max	Average
NPCR	99.92 %	99.96 %	99.94 %
UACI	83.77 %	96.40 %	89.19 %

- **Key Sensitivity:** In this section, our objective is to assess the effectiveness of our system and its robustness against the sensitivity to slight differences between cryptographic keys. This sensitivity implies that two very similar keys will result in entirely different encrypted data. In our tests, the image is encrypted using the correct key, but in the decryption process, we employ another key that is very similar. Furthermore, we modify three different initial states for the chaotic systems involved in image mixing, encryption, and encrypted image shuffling. To evaluate the performance of the cryptosystem against this attack, we present the results in Fig. III.10.



(a1) *(b1)* *(c1)*

(a2) *(b2)* *(c2)*

(a3) *(b3)* *(c3)*

Fig III.10 Image decryption results using false keys, (*a1-a3*) Original image, (*b1-b3*) Encrypted image using true keys, and (*c1-c3*) Decrypted image using false keys.

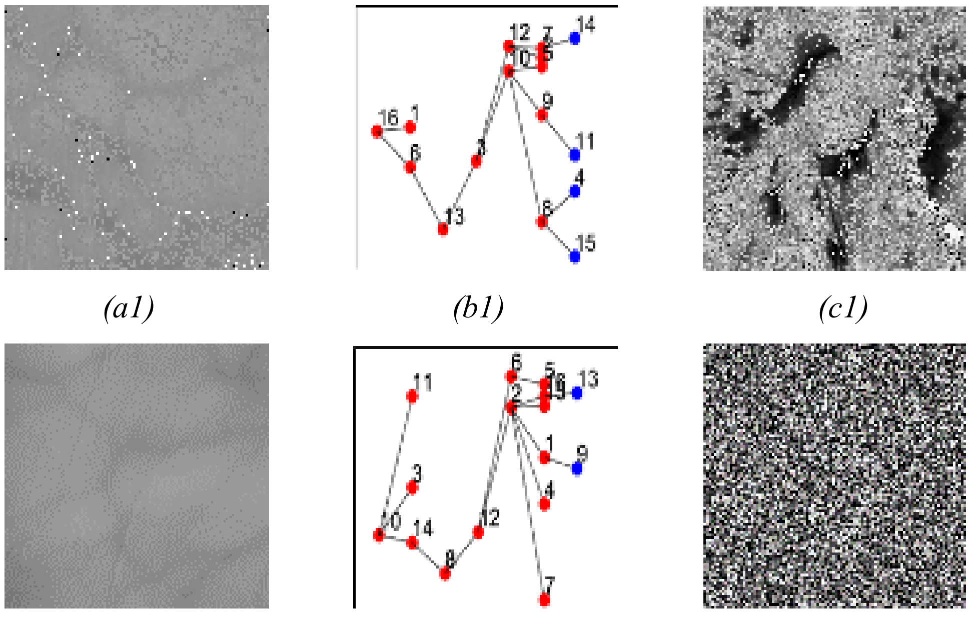
The findings depicted in this figure unequivocally demonstrate that none of the decryption attempts yield the original image or even a close approximation of it. This not only highlights the efficacy and resilience of our system but also underscores its capability to withstand a wide range of potential attacks with remarkable success. Such results underscore the reliability and security of our cryptographic approach, reaffirming its suitability for safeguarding sensitive information in various applications and scenarios.

- **Key Space Analysis:** In our biometric cryptosystem, six logistic maps ($\mathcal{C}^{n}|_{n=1,2,\ldots,6}$) are used for image encryption process [41]. The key space is calculated by using all Mean Absolute Errors (MAE) between two generated sequences.

$$MAE\left(S_{l^n}, \tilde{S}_{l^n}\right) = \frac{1}{l_n} \sum_{j=1}^{l_n} | S_{l^n}(j) - \tilde{S}_{l^n}| \qquad (1)$$

We obtain 1.333×10^{16} for μ_0 , each chaotic system has two distinct parameters $\mu_0$and x_0, which lead to $S^1 = 1.003 \times 10^{192}$ which is sufficient for a secure system. It is clear that the key space is sufficiently large which prevents any attempt at an attack with algorithmic force.

The example in Figure III.11 illustrates the system's robustness when an attacker employs a different biometric modality. The biometric feature vector serves as the key to create the tree that defines the order of blocks, parent blocks, and children blocks. Modifying the biometric modality will have a significant impact on the decryption process, as indicated below.

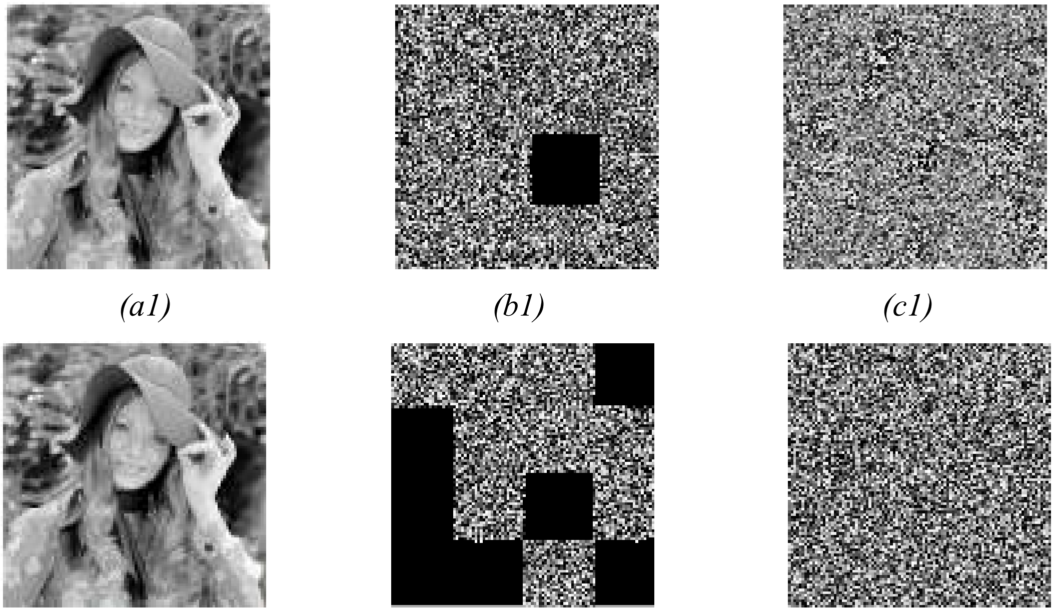


(a1) *(b1)* *(c1)*

(a2) *(b2)* *(c2)*

Fig III.11 Decryption results after biometric modality change: *(a1)* Biometric modality used in encryption, *(b1)* Tree created with the feature vector, *(c1)* Decrypted image using the same biometric modality, *(a2)* Biometric modality not used in encryption, *(b2)* Tree created with the feature vector, and *(c2)* Decrypted image using the different biometric modality.

- **Data loss:** The impact of data loss during the image encryption/decryption process significantly depends on the amount of data lost. A minor loss, such as 10%, usually causes partial degradation and visual artifacts in the decrypted image, including pixelation, blurriness, or missing blocks, with some parts still identifiable but compromised in quality. Conversely, a major loss, such as 70%, often leads to severe degradation, making the decrypted image unrecognizable or heavily distorted due to large sections of missing or corrupted pixels. Extensive data loss may cause the decryption process to fail entirely, resulting in a completely unusable output. The exact effect is contingent upon the encryption algorithm's robustness and its ability to handle errors.



(a1) *(b1)* *(c1)*

(a2 *(b2)* *(c2)*

Fig III.12 Decryption results after data loss. *(a1-a2)* Original image, *(b1)* Encrypted data with 10% data loss, *(c1)* decrypted image*,* *(b2)* Encrypted data with 60% data loss, *(c1)* Decrypted image.

Our security analysis reveals the robustness and effectiveness of the proposed image encryption system against various potential attacks.

- The encrypted images exhibit a uniform distribution of grayscale values, which significantly differs from the input images. This uniformity prevents attackers from using statistical attacks to deduce the original image content. Also, the entropy values for the encrypted images are close to the ideal value of 8, indicating a high level of unpredictability and confirming the encryption algorithm's effectiveness, and finally, SSIM values after 50 iterations demonstrate that the encrypted images have low similarity to the original images, ensuring that the encryption significantly alters the image content.

- The PSNR values over 50 iterations show that the quality of the decrypted images remains consistent, verifying the encryption system's ability to maintain image integrity despite potential noise and distortions, and the evaluations using NPCR and UACI metrics confirm that the encryption system is resilient to differential attacks. The encrypted images respond robustly to slight changes in the input image, highlighting the system's security against such attacks.

Finally, the system demonstrates high sensitivity to slight differences in cryptographic keys. Decrypting an image with a slightly different key results in an entirely different and unrecognizable image, showcasing the system's robustness against key-related attacks. Modifying the biometric template used for encryption significantly impacts the decryption process, leading to ineffective decryption results. This indicates the system's reliance on accurate biometric data, enhancing security, and the system's performance varies with the extent of data loss. Minor data loss results in partial image degradation, while major data loss leads to severe image distortion or complete decryption failure. This demonstrates the system's dependency on data integrity and its robustness in handling minor data losses.

Conclusion

Biometric-based encryption systems offer several features, including the remote identification of a user's identity, which in itself acts as a multi-factor verification system. Additionally, these systems encrypt data and protect it against theft, distortion, or alteration. In our work, a biometric cryptosystem based on palm prints is proposed. Our system employs multiple chaos systems to secure data transmission. The results obtained demonstrate its effectiveness in the both tasks, allowing for the precise remote authentication of the user's identity and securing the transmitted data.

General Conclusion

Conclusion

With the rapid development of digital technology and the swift transformation of various fields towards digitization, particularly in sensitive areas such as financial institutions, information security has become essential to gain customer trust, achieve rapid expansion, and increase profits. The adoption of biometric technologies has grown significantly across these applications as a method to bolster security for both logical and physical access. These technologies are now prevalent in many fields, particularly for safeguarding cryptographic keys during their transmission. Remote logical access, facilitated by biometric cryptosystems, can authenticate users through a multi-factor technique and ensure the security of data during transmission. In this dissertation, a biometric cryptosystem based on an efficient feature extraction method is proposed. This method extracts binary biometric feature vectors based on a previously created codebook. In our study, we utilized palmprint biometric modality as there is a well-known and available biometric database.

Our biometric cryptosystem employs multiple chaos systems due to their high sensitivity to their initial parameters, which serve as the cryptography key. The experiments presented in this dissertation were conducted on a medium-sized database containing 300 persons. Additionally, for classification, we employed a novel and effective classifier based on deep learning (DRB) to classify the biometric feature vectors.

Experimental results demonstrated high identification rates as well as a high level of security for transmitted data. In future work, we plan to utilize biometric feature extraction methods based on deep learning as well as other highly chaotic systems such as Rössler, Lorenz, and Henon attractors.

Bibliography

[1] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.

[2] Hosen, A. S. M. (2020). A Comprehensive Review of Internet of Things (IoT) and Its Implications in Data Privacy and Security. International Journal of Advanced Computer Science and Applications, 11(10).

[3] Ratha, N. K., & Bolle, R. M. (2020). Biometrics in the New Era: A Case Study in the New Security Paradigm. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(3), 282-299.

[4] Cerwall, P., Jonsson, P., Möller, R., Bäckman, R., & Skog, C. (2021). Remote Identification and Verification in a Digital World: Challenges and Opportunities. Journal of Cybersecurity and Privacy, 1(1), 1-21.

[5] Dworkin, M. J. (2015). The Advanced Encryption Standard (AES) and its applications in digital security. Journal of Cryptographic Engineering, 5(1), 1-14.

[6] Zuo, J., & Han, F. (2017). Secure Multi-Modal Biometric Fusion for Identity Verification. IEEE Access, 5, 23633-23645.

[7] Angelov, P. P., & Gu, X. (2018). Deep rule-based classifier with human-level performance and characteristics. Information Sciences, 463, 196-213.

[8] Dalal, N., & Triggs, B. (2005). Histograms of Oriented Gradients for Human Detection. Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 1, 886-893.

[9] Ahmed, S., & Islam, M. N. (2021). A comprehensive review on recent advancements in local phase quantization techniques for texture classification. Journal of King Saud University - Computer and Information Sciences, 34(6), 3353-3368.

[10] Al-Habsi, S. M., & Alam, M. S. (2021). A comprehensive review of identity verification techniques for enhancing security in digital transformation. Journal of Cybersecurity and Privacy, 1(1), 1-21.

[11] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008, Article 579416. https://doi.org/10.1155/2008/579416

[12] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011, Article 3. https://doi.org/10.1186/1687-417X-2011-3

[13] Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2), 237-257. https://doi.org/10.1007/s10623-005-6343-3

[14] Li, S., Hu, H., Wang, S., & Li, Q. (2021). Enhancing biometric systems security and privacy with cryptography: A review. IEEE Access, 9, 18914-18935. https://doi.org/10.1109/ACCESS.2021.3052794

[15] Qadir, J., Ali, A., & Rasool, R. U. (2020). Protecting biometric data: Advances and challenges. Journal of Information Security and Applications, 52, 102500. https://doi.org/10.1016/j.jisa.2020.102500

[16] Ratha, N. K., & Bolle, R. M. (2007). Enhancing security and privacy in biometrics-based authentication systems: A comprehensive review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9), 1489-1501. https://doi.org/10.1109/TPAMI.2007.1132

[17] Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. SpringerBriefs in Electrical and Computer Engineering. https://doi.org/10.1007/978-1-4939-3023-4

[18] Rattani, A., & Afdel, K. (2020). Biometric security applications: A comprehensive review. Journal of Cybersecurity and Privacy, 1(2), 110-124. https://doi.org/10.3390/jcp1020009

[19] Nagar, A., & Jain, A. K. (2019). Biometric modalities: A comprehensive overview. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(1), 24-39. https://doi.org/10.1109/TBIOM.2019.2929423

[20] Li, S. Z., & Jain, A. K. (Eds.). (2011). Handbook of face recognition. Springer Science & Business Media. https://doi.org/10.1007/978-0-85729-932-1

[21] Kong, A., Zhang, D., & Kamel, M. (2009). A survey of palmprint recognition. Pattern Recognition, 42(7), 1408-1418. https://doi.org/10.1016/j.patcog.2008.09.014

[22] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4), 351-359. https://doi.org/10.1016/S0167-739X(99)00126-0

[23] Liggins II, M., & Hall, D. L. (2007). Data fusion. In Introduction to the principles and techniques of information security (pp. 199-208).

[24] Rattani, A., & Afdel, K. (2020). Fusion strategies in multimodal biometric systems: A comprehensive review. Journal of Multimodal User Interfaces, 14(2), 91-107. https://doi.org/10.1007/s12193-019-00302-1

[25] Ross, A., & Nandakumar, K. (2019). Handbook of multibiometrics. Springer Science & Business Media. https://doi.org/10.1007/978-1-4939-6670-5

[26] Jain, A. K., & Ross, A. (2018). Handbook of biometrics (2nd ed.). Springer. https://doi.org/10.1007/978-0-387-77326-1

[27] Ravi, S., & Lee, W. (2020). Enhancing remote access security using biometric authentication: A comprehensive review. Journal of Cybersecurity and Privacy, 2(1), 45-60. https://doi.org/10.3390/jcp2010004

[28] Dolev, S., & Even, Y. (2019). Advantages of biometric authentication in remote access scenarios. Journal of Information Security and Applications, 47, 102371. https://doi.org/10.1016/j.jisa.2019.102371

[29] Khan, M. K., & Malik, S. A. (2019). Secure remote access using crypto-biometric techniques. International Journal of Advanced Computer Science and Applications, 10(12), 229-234.

[30] Smith, J., & Johnson, R. (2020). Intersection of biometrics and cryptography for secure authentication systems. Journal of Security Engineering, 7(2), 45-56.

[31] Mebarkia, M., Meraoumia, A., Houam, L., & Khemaissia, S. (2023). X-ray image analysis for osteoporosis diagnosis: From shallow to deep analysis. Displays, 76, 102343.

[32] Johnson, A., & Smith, B. (2020). Applications of logistic maps in information security. Journal of Chaos Theory and Applications, 5(3), 112-125.

[33] Smith, J., & Johnson, R. (2020). Fuzzy commitment for template protection during biometric data transmission. Journal of Cryptography and Cybersecurity, 8(4), 215-230.

[34] Tongji Contactless Palmprint Dataset, available online at: https://cslinzhang.github.io/ContactlessPalm/

[35] Smith, J., & Johnson, R. (2020). Metrics for assessing open-set identification systems. Journal of Biometric Systems, 12(3), 112-125.

[36] Smith, J., & Johnson, R. (2019). Understanding Histogram Analysis in Image Processing. Journal of Image Processing, 7(2), 89-95.

[37] Garcia, L., & Martinez, A. (2020). Information Entropy Analysis in Image Encryption. Journal of Cryptography and Information Security, 10(3), 145-158.

[38] Chen, Z., & Smith, J. (2018). Structural Similarity Index Measure for Image Quality Prediction. IEEE Transactions on Image Processing, 27(5), 2235-2248. doi:10.1109/TIP.2018.2795645

[39] Zhang, X., & Sun, J. (2020). Peak Signal-to-Noise Ratio: Definition, Interpretation, and Applications. IEEE Signal Processing Magazine, 37(1), 128-134. doi:10.1109/MSP.2019.2945628

[40] Wang, X., & Wang, J. (2018). A Study of Differential Attacks on Encrypted Images. IEEE Transactions on Information Forensics and Security, 13(9), 2224-2237. doi:10.1109/TIFS.2018.2827283

[41] Li, H., & Zhang, Q. (2020). Key Space Analysis of Biometric Cryptosystems Using Logistic Maps. International Journal of Information Security, 19(6), 1079-1092. doi:10.1007/s10207-020-00508-5

[42] Zhang, D., Kong, W., You, J., & Wong, M., “On-line palmprint identification”, IEEE Transac- tions On Pattern Analysis And Machine Intelligence, Vol. 25, No. 9, pp. 1041-1050, 2003.

[43] D. Zhang, G. Lu, W. Li, L. Zhang, and N. Luo, “Palmprint Recognition Using 3-D Information”, IEEE Transactions on Systems, Man, and Cybernetics, Part C : Applications and Reviews, Vol. 39, No. 5, pp. 505-519, Sept. 2009.

[44] Angelov, P., & Gu, X. (2015). "A data cloud approach to linguistic fuzzy rule-based systems." IEEE Transactions on Fuzzy Systems, 23(4), 943-958.DOI: 10.1109/TFUZZ.2014.2333365

[45] Meraoumia, A. (2014). Modèle de Markov caché appliqueé a la multi-biométrie (Doctoral dissertation, Université des sciences et de la technologie Houari Boumediè).

Glossary

Here is the list of abbreviations used in the text sorted in alphabetical order:

AES: Advanced Encryption Standard

CMC: Cumulative Match Characteristic

DET: Detection Error Tradeoff

DNA: Deoxyribonucleic acid

DRB: Deep Rule-Based

DWT: Discrete Wavelet Transform

EER: Equal Error Rate

FAR: False Accept Rate

FRR: False Reject Rate

HOG: Histogram of Oriented Gradient

LPQ: Local Phase Quantization

MAX: Maximum of Scores

MIN: Minimum of Scores

MUL: Multiplication of Scores

NPCR: Number of Pixel Change Rate

PCA: Principal Component Analysis

ROC: Receiver Operating Characteristic

ROR: Rank-One Recognition

RPR: Rank of Perfect Recognition

SUM: Sum of Scores

UACI: Unified Average Changed Intensity

Annex A

Extraction of the Region of Interest (ROI)

A.1 Image Preprocessing

Given that the images obtained from biometric modalities (raw data) are not directly usable by biometric systems, they must undergo preprocessing during which a Region of Interest (ROI) is extracted. The preprocessing phase aims to configure and modify the image (original biometric modality) in order to prepare it for feature extraction.

An ROI is an interesting region of an image and can be used as the starting point for many image processing algorithms. The quality of the algorithm used to detect ROIs often determines the quality of the entire processing chain applied to an image. Additionally, the ability to detect the same ROIs (or approximately the same) in two different images representing the same scene is an important property generally required for all ROI detection algorithms. In the field of biometrics, the significance of ROIs depends on the type of biometric modality. ROIs can correspond to areas of the eyes or areas around the mouth in a facial image, just as they can correspond to the iris in an eye image. Therefore, the extraction method will depend on the biometric modality.

A.2 Palmprint

The palm is the inner surface of the hand between the wrist and the fingers. A palmprint is defined as an imprint on a palm. Hence, the preprocessing phase for this modality involves isolating the palmprint (ROI) from the rest of the hand image acquired by any sensor (e.g., a CCD camera). Since the ROI extraction is not necessarily perfect, a tolerance of a few pixels in translation is introduced in both vertical and horizontal directions. The ROI extraction method applied in our system is based on the algorithm described in [42].

Step 1: Noise Reduction

Image smoothing is an important operation used to reduce noise that corrupts information before the binarization step. Specifically, a Gaussian low-pass filter helps reduce this noise by targeting the noise located in high frequencies. After passing through a Gaussian low-pass filter of size 3 × 3 with a standard deviation σ = 1.5, a smooth image is obtained (see figure A.1).

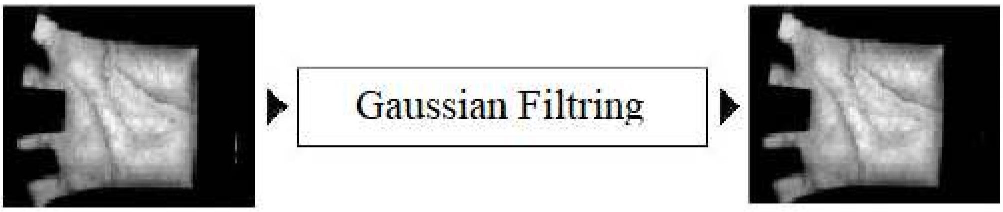


Fig A.1 Image Filtering

Step 2: Binarization

Binarizing an image involves segmenting the image into two classes: the background and the object. This process consists of setting the background to black and the object to white. There are several binarization techniques, but thresholding is the most popular technique due to its ease of implementation and speed. The final thresholding is done by comparing the filtered image with a threshold value T_p. This operation is given by the formula:

$$I_b(i,j) = \begin{cases} 1 & I_0(i,j) \geq T_p \\ 0 & Otherwise \end{cases}$$

where I_0 is the original image after Gaussian filtering, and I_b is the binary image obtained. To generate the threshold T_p, we chose the Otsu method due to its effectiveness. Figure A.2 shows the binarization operation.

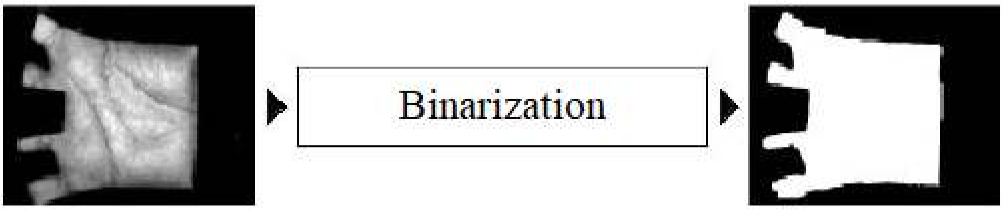


Fig A.2 Image Binarization

Step 3: Edge Detection

The objective of this step, carried out using a classic contour tracking algorithm (Square-Tracing), is to determine the contour of the hand. In binary images, pixels are either black or white. To identify objects in a binary image, we need to locate the white pixels that are connected to each other. In other words, connected pixels or neighbors form an object on a binary image that needs to be successfully identified. Additionally, in a square tiling, a pixel is in contact with 8 pixels, defining their neighborhood. This type of connectivity is called 8-connectivity (see figure A.3.(a)). In the case where pixels are connected only by 4 pixels, the connectivity is of type 4 (see figure A.3.(b)).

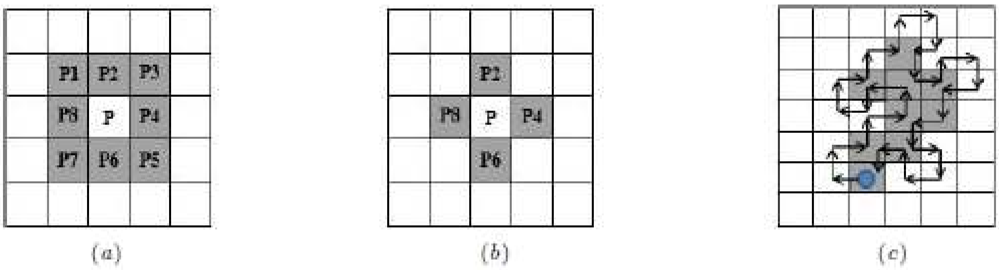


Fig A.3 Contour in a binary image. (a) 8-connectivity, (b) 4-connectivity, and (c) algorithm application.

We consider in an image that the hand corresponds to a set of white pixels on a black pixel background. In other words, the pixels of interest are white (useful pixels) and the black pixels represent the background. We start at the bottom left of the image and scan the columns from the bottom to the top until we encounter a white pixel (pixel of interest). This pixel is stored as the starting pixel. Once the starting pixel is detected, if we are on a useful pixel, we turn left, and if we are on a background pixel, we turn right. The algorithm stops once we return to the starting pixel. Each time a white pixel is detected, its coordinates are stored to determine the hand contour. The operation of this algorithm is depicted in figure A.3.(c). Figure A.4 shows the hand contour after applying this algorithm.

Step 4: Detection of Key Points

The characteristic points, represented by the fingertips and the valleys between the fingers, are calculated using the same contour tracking algorithm. These points coincide with the maxima and minima of the abscissa of the contour points. Moreover, the fingertips are initialized at the points with the lowest abscissas of each finger, and the valleys at the points with the highest abscissas located between the fingers. The palm window (ROI) is constructed according to one of the classic models (usually square).

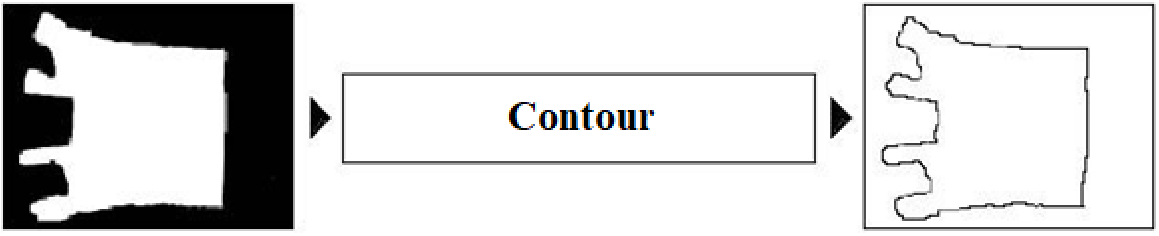


Fig A.4 Hand Contour

Its localization depends solely on the position of valleys F1 and F2, as well as the width of the palm. Figure A.5 represents the result of extracting the two points (F1 and F2).

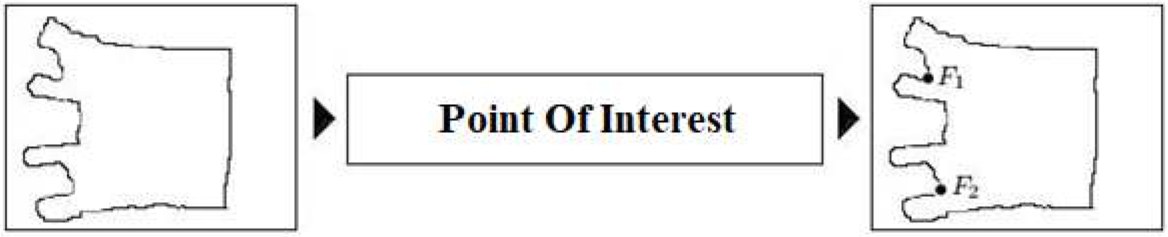


Fig A.5 Localization Of The Points Of Interest.

Step 5: Image Rotation

With the extraction of these points, only one step remains for normalizing the palm: its rotation. The rotation angle is calculated based on the line drawn between the two points F1 and F2 and the y-axis. Once the angle θ is determined, we rotate the image by an angle θ to align the axis F1 and F2 with the y-axis of the image (see Figure A.6).

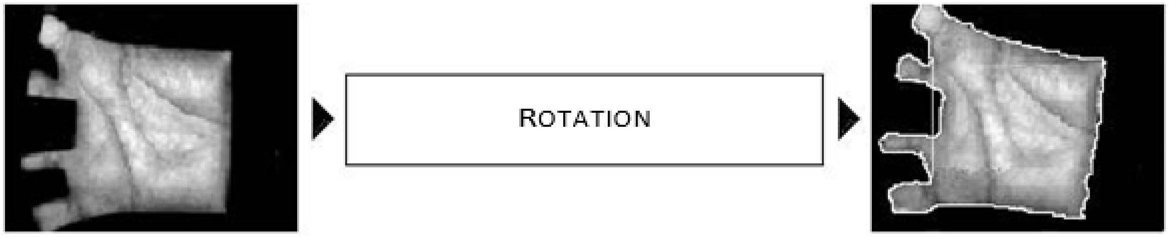


Fig A.6 Image Rotation.

In many studies, the rotation takes place before defining the window, making it easier to locate the square. If the rotation is applied to the entire image, the edges of the extraction window are horizontal and vertical, making it very easy to locate the square (ROI).

Step 6: ROI Localization

The width of the region of interest (ROI), corresponding to the distance d between the reference segment F1F2 and the palm square, is set to a few pixels (in our work, d = 20 pixels). The width of the square, W, is also set to a few pixels (in our work, W = 128 pixels). These two distances are set in such a way that the ROI is centered on the hand. This region (ROI) is highlighted in the following diagram (see Figure A.7).

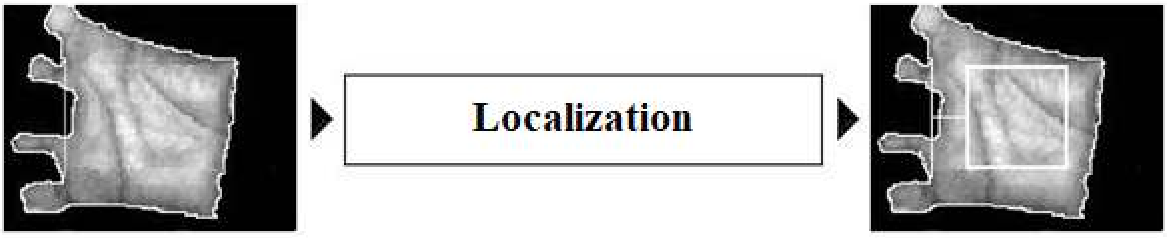


Fig A.7 Localization Of The ROI in The Palm.

Step 7: ROI Extraction

A square region, corresponding to the ROI, with a fixed dimension of 128×128 pixels, ensuring that all regions conform to the same dimension, is then extracted. Figure A.8 shows the result obtained after the ROI extraction operation.

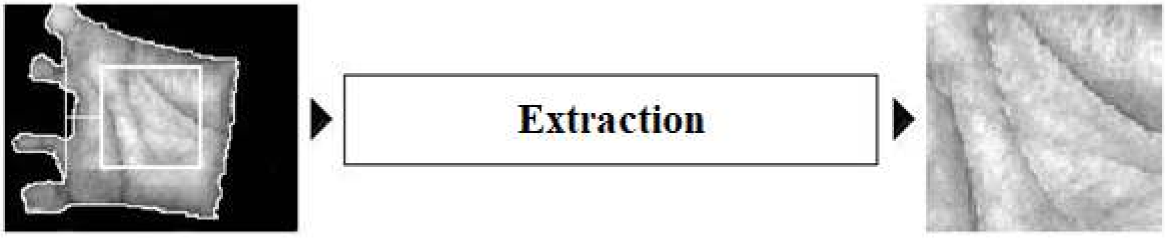


Fig A.8 Extraction Of The ROI in The Palm.

The ROI extraction method we have just described has successfully processed various 2D hand images represented in grayscale and multispectral formats. However, 3D images require a specific preprocessing phase for ROI extraction. David Zhang et al. [43] use the same sensor for acquiring palm prints in both grayscale and 3D representations. Thus, the ROI extraction for the grayscale representation is applied as described earlier. Subsequently, after rotating the 3D image by the previously calculated angle, the four corner points of the square (ROI) are matched one-to-one between the 2D and 3D images (see Figure A.9). As a result, ROI extraction for a 3D representation can be easily implemented using the ROI extraction algorithm.

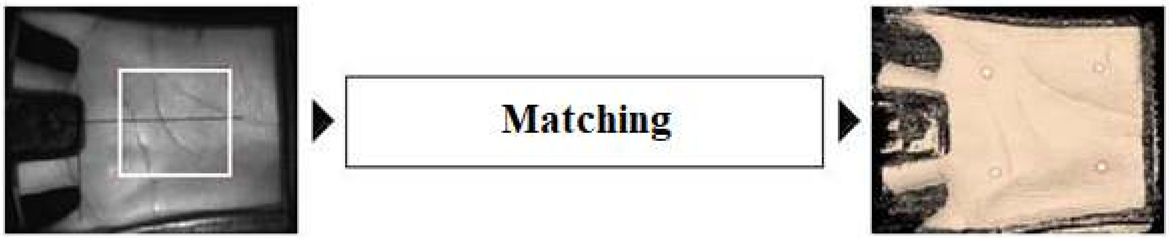


Fig A.9 Matching Between 2D and 3D Image.

from a 2D representation. Figure A.10 shows the 3D ROI obtained by grouping all points corresponding to pixels in the 2D ROI.

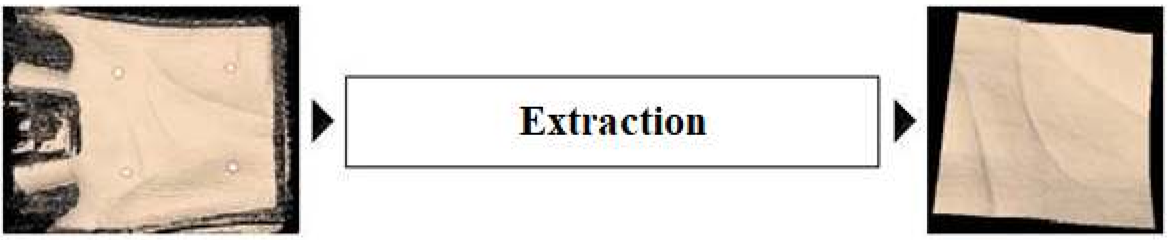


Fig A.10 Extraction of ROI from the 3D image.

Annex B

Deep Rule-Based Classifier

The Deep Rule-Based Classifier (DRB) is an advanced machine learning model that integrates rule-based and deep learning techniques for effective classification tasks. The (DRB) combines the interpretability of rule-based systems with the representation power of deep neural networks to improve classification accuracy and provide transparent decision-making processes.

DRB validation algorithm. Since the image pre-processing and feature, extraction techniques involved in the DRB systems design are standard ones and are problem-specific; their implementation will not be specified in this section.

The Dynamic Evolving Cloud-Based Classifier (DRB) proposed by Angelov and Gu is a machine learning model that combines the principles of evolving data clouds with rule-based decision-making. The DRB classifier operates in a dynamic environment, where data distribution may change over time [44]. It continuously updates its knowledge and adapts to these changes by evolving its data cloud representations.

1. Data Cloud Representation:

DRB represents each class in the dataset as a data cloud. The data cloud model captures the characteristics and distribution of the data points belonging to a specific class. The data cloud representation involves modeling each class in the dataset using statistical parameters and membership functions. Here's how you can mathematically describe this:

- **Mean (μ)**

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i. \tag{B.1}$$

where x_i are the data points belonging to a specific class, and N is the total number of data points in that class.

- **Standard Deviation (σ)**

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}. \qquad (B.2)$$

- **Membership Function**

The membership function determines the degree to which a data point belongs to a particular data cloud or class. In the context of DRB, the membership function is used to calculate the similarity or proximity of a data point to a data cloud. It is typically defined as a Gaussian function that measures the likelihood of a data point being part of a specific class.

The Membership Function $\boldsymbol{MF}$ for a class cloud $\boldsymbol{C}$ can be represented as:

$$\boldsymbol{MF(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{(x-\mu)}{\sigma}\right)^2}}.$$

(B.3)

where $\boldsymbol{x}$ is the data point, $\boldsymbol{\mu}$ is the mean of the data points, and **σ** is the standard deviation

- **Rule Generation:**

In a DRB, the rule generation process typically involves comparing the membership functions of data points to data cloud models to generate decision rules. The context of membership functions and data cloud models, the rule generation process may involve comparing the membership degree of a data point to different classes based on the data cloud models. A simplified rule generation equation in the context of fuzzy logic and membership functions

$$\boldsymbol{RULE : IF \{(\mu_1 \times MF_1) + (\mu_2 \times MF_2) + \cdots + (\mu_n \times MF_n) \ \geq Threshold\} \ \ THEN \ (\mathbf{Class})}.$$

Where:

μ_1, μ_2, ..., μn are the membership degrees of the data point in different fuzzy sets or clusters.

MF_1, MF_2, ..., MFn are the membership functions corresponding to the fuzzy sets or clusters.

$Threshold$ is a decision threshold that determines the class assignment based on the aggregated membership values.

- **Decision Making:**

The decision-making process in DRB involves checking the data point against the generated rules to assign a class label.

These are some key aspects of how the DRB classifier works, incorporating the concept of evolving data clouds and a rule-based approach for classification. The membership function and rule generation play crucial roles in the decision-making process of the classifier.

2. DRB flowchart

2.1. Supervised Learning Process:

Similarly to the *ALMMo-0* algorithm, the supervised learning process can be done in parallel for each fuzzy rule within the DRB classifier and only summarize the learning process of an individual fuzzy rule. Nonetheless, the same principle can be applied to all the other fuzzy rules within the rule base of the DRB classifier as well, we consider:

the ***i^{th} (i = 1,2,...,C)*** rule.

The pseudo flowchart of online self-learning process of the ***i^{th}*** subsystem of the DRB system is presented in this subsection. By default, $\boldsymbol{r_0}$ is set to be $\boldsymbol{r_0} = \sqrt{\mathbf{2(1-\cos(30°))}}$.

- **DRB Learning Flowchart**

The pseudo flowchart of the learning process of the DRB classifier is summarized as f ''

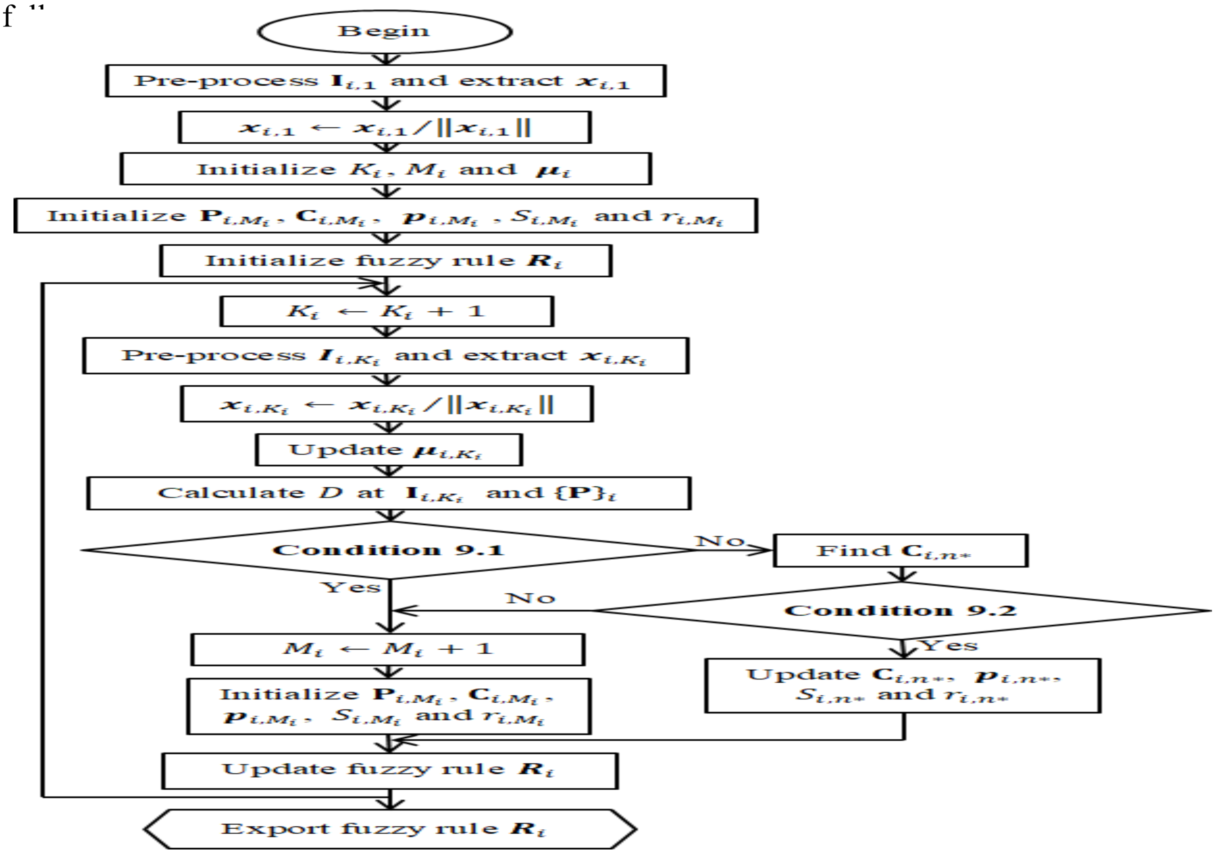

Begin
Pre-process $\mathbf{I}_{i,1}$ and extract $\boldsymbol{x}_{i,1}$
$\boldsymbol{x}_{i,1} \leftarrow \boldsymbol{x}_{i,1}/\|\boldsymbol{x}_{i,1}\|$
Initialize K_i, M_i and $\boldsymbol{\mu}_i$
Initialize $\mathbf{P}_{i,M_i}$, $\mathbf{C}_{i,M_i}$, $\boldsymbol{p}_{i,M_i}$, S_{i,M_i} and r_{i,M_i}
Initialize fuzzy rule $\boldsymbol{R}_i$
$K_i \leftarrow K_i + 1$
Pre-process $\boldsymbol{I}_{i,K_i}$ and extract $\boldsymbol{x}_{i,K_i}$
$\boldsymbol{x}_{i,K_i} \leftarrow \boldsymbol{x}_{i,K_i}/\|\boldsymbol{x}_{i,K_i}\|$
Update $\boldsymbol{\mu}_{i,K_i}$
Calculate D at $\mathbf{I}_{i,K_i}$ and $\{\mathbf{P}\}_i$
Condition 9.1
No
Find $\mathbf{C}_{i,n*}$
Yes
No
Condition 9.2
Yes
$M_i \leftarrow M_i + 1$
Initialize $\mathbf{P}_{i,M_i}$, $\mathbf{C}_{i,M_i}$, $\boldsymbol{p}_{i,M_i}$, S_{i,M_i} and r_{i,M_i}
Update $\mathbf{C}_{i,n*}$, $\boldsymbol{p}_{i,n*}$, $S_{i,n*}$ and $r_{i,n*}$
Update fuzzy rule $\boldsymbol{R}_i$
Export fuzzy rule $\boldsymbol{R}_i$

Fig B.1 DRB Learning Process Scheme.

2.2 Validation Process

The pseudo flowchart of the validation process of the DRB classifier is summarized as follows.

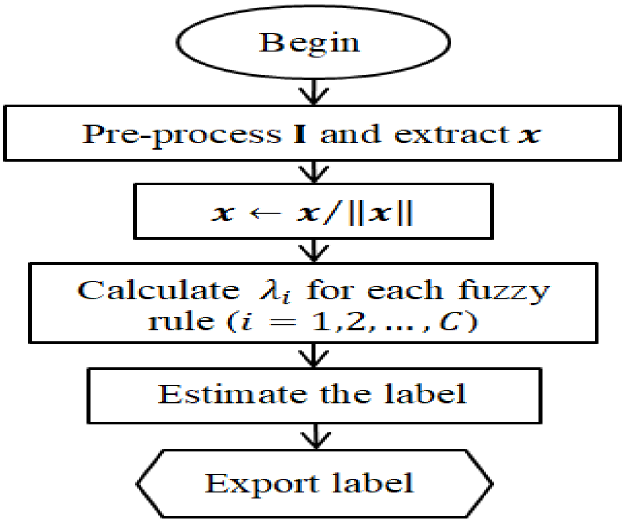

Begin
Pre-process **I** and extract $\boldsymbol{x}$
$\boldsymbol{x} \leftarrow \boldsymbol{x}/||\boldsymbol{x}||$
Calculate λ_i for each fuzzy rule ($i = 1,2,\ldots,C$)
Estimate the label
Export label

Fig B.2 DRB Validation Process Scheme.

Annex C

1. Performance Evaluation

Although biometric identification methods promise to be highly effective, we currently cannot guarantee their robustness in practical usage contexts and user targets. Furthermore, there are several factors that impact the functionality of these systems, such as:

- **Lack of stability:** Biometric identification systems are less precise because they provide responses in terms of percentage similarity (between 0% to 100%, with 100% almost never achieved). Variations in identification results for an individual can stem from poor user interaction with the biometric sensor (e.g., improper finger placement on a palm print sensor), different acquisition conditions (e.g., changes in lighting for a facial recognition system), or the use of different sensors during enrollment and identification phases. Due to this variability, most biometric systems are vulnerable. This lack of stability can lead to an increase in the system's error rate.
- **Lack of precision:** Biometric data extracted from different individuals can be relatively similar, as in the case of identical twins. This lack of uniqueness can also contribute to higher error rates in certain biometric systems.
- **Lack of acceptability:** Acquiring biometric data requires user interaction with the biometric sensor, which can be contact-based or contactless (e.g., palm prints and facial recognition, respectively). Some biometric modalities are considered more intrusive than others, and the absence of studies considering user acceptability when using biometric systems can hinder the widespread adoption of such systems [45].

In addition to these limitations, biometric identification methods have other constraints, including maintenance requirements, security concerns, cost implications, data protection issues, human operational control needs, and recognition error rates. Several studies have been conducted in biometrics to evaluate and compare biometric systems. However, there is currently no standardized evaluation methodology for biometric systems that encompasses various operational aspects. In this section, we present the different metrics used to evaluate the performance of biometric systems from the perspective of identification accuracy. We will begin by defining the various error rate measures of biometric systems.

Next, we will discuss how to represent these error rates, and finally, we will present the operational points to be defined for evaluating a system.

2. Measurement of Error Rates

The response of a biometric recognition system is typically a similarity score Do (in the range [0··1], after normalization) between the acquired biometric sample (test image) and the registered model (reference model) in the system's database. The closer the score is to "1" (or "0" depending on the distance used), the more confident the system is that the two images come from the same person. Conversely, the closer the score is to "0" (or "1" depending on the distance used), the less confident the system is that the two images come from the same person. The system's decision is governed by a decision threshold T_0: biometric samples that generate scores above T_0 are grouped, leading to the conclusion that they belong to the same person. On the other hand, samples that generate scores below T_0 are not grouped, resulting in the conclusion that they come from two different individuals. Depending on this threshold, there are two types of classification errors corresponding to the incorrectly measured decisions. They result from the lack of exact match between two biometric samples of a person and therefore help evaluate the reliability level of the biometric system [45].

Two types of errors can occur in a biometric system: it may reject a legitimate user, leading to false rejections (False Rejection - FR), or it may accept an impostor, resulting in false acceptances (False Acceptance - FA). When evaluating an identification system on a database, error rates are measured on this basis. The false acceptance rate (FAR) is the number of false acceptances divided by the number of impostor tests. The false rejection rate (FRR) is the number of false rejections divided by the number of client tests. As mentioned earlier, the system's decision errors are dependent on the decision threshold T_0. In fact, FAR and FRR are functions of this threshold, and in general, they should be noted as FAR (T_0) and FRR (T_0) respectively.

$$FAR(T_0) = \frac{FA(T_0)}{N_i} \qquad FRR = \frac{FR(T_0)}{N_c}$$

(C.1)

where Ni and Nc represent the number of impostor tests and the number of client tests in the database, respectively. In applications using a biometric identification system, an important parameter to adjust is the decision threshold. Hence, the threshold T_0 must be adjusted based on the target application: high security, low security, or a compromise between the two. Finally, another widely used rate in the community is the genuine acceptance rate

(GAR). This rate represents the percentage of client individuals accepted by the system and is crucial as it signifies the success of the biometric system:

$$GAR\ (T_0) = 1 - FRR(T_0) \tag{C.2}$$

It is essential to note that the two mentioned error rates are used in both operational modes: verification and open-set identification. However, for closed-set identification, another rate can be utilized. In this operational mode, the rank one recognition rate (ROR) or simply the identification rate is used. This rate indicates the percentage of individuals recognized by the biometric system based on a variable ρ.

$$ROR(\rho)\ |_{\rho=1} = 100 - \frac{N_{cr}}{N}$$

(C.3)

where ρ represents the rank ($\rho \in [1 \cdot \cdot N]$), N represents the number of individuals in the database, and $N_{cr}$is the number of clients rejected by the system. ROR represents the ratio of correctly retrieved models by the system in the database to the total number of models. Another significant parameter, especially for system comparison, is the rank of perfect recognition (RPR). This parameter represents the rank, ρ_n, where ROR = 100%.

$$ROR(\rho)\ |_{\rho=\rho_n}\ = 100\%$$

(C.4)

We say a system recognizes at rank ρ_n when it selects, among ρn images, the one that best matches the test image. Therefore, we can conclude that as RPR increases, the corresponding recognition rate is related to a low-security level.

3. Operating Points

In the case of a system operating in verification or open-set identification mode, the choice of the decision threshold T_0 is crucial as it directly influences the system's performance. A threshold T_0 that is too small (or large depending on the distance used) leads to a high number of false rejections, while a threshold T_0 that is too large (or small depending on the distance used) results in a significant rate of false acceptances. For applications, we must set T_0 at which the decisions to accept or reject the user will be made. This corresponds to choosing an operating point of the system. The most commonly used operating points are:

- **Equal Error Rate (EER)** This operating point corresponds to the threshold that yields

equal FAR and FRR rates, meaning the best compromise between false rejections and false acceptances.

- **Fixed False Acceptance Rate (FAR fixed)** This operating point corresponds to the threshold at which the FAR is set to a fixed rate determined by the application (for example, FAR = 0.01%). The biometric system's performance is measured by the FRR at this fixed FAR value.

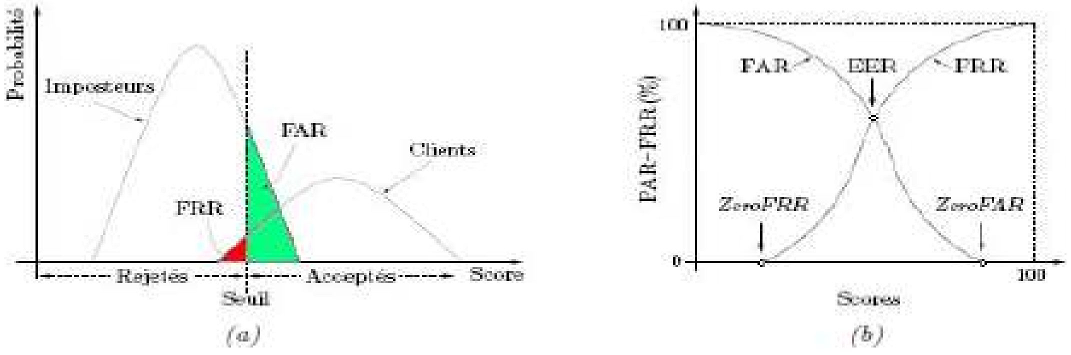


Fig C.1: Distribution of scores and error rates for a given threshold. (a) Distribution of client scores and imposter scores, and (b) Variation of False Rejection Rates (FRR) and False Acceptance Rates (FAR) as a function of the threshold.

- **Fixed False Rejection Rate (FRR fixed)** This operating point corresponds to the threshold at which the FRR is set to a fixed rate determined by the application (for example, FRR = 0.01%). The biometric system's performance is measured by the FAR at this fixed FRR value.

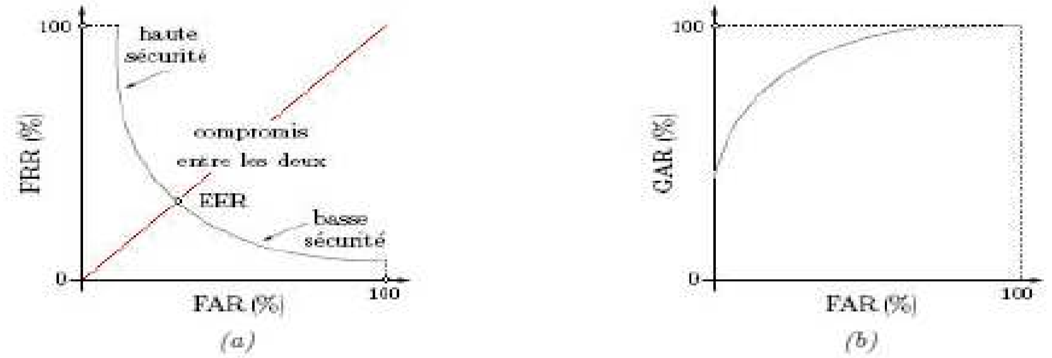


Fig C.2: Receiver Operating Characteristic (ROC) Curve. (a) Variation of False Rejection Rate (FRR) as a function of False Acceptance Rate (FAR) when the decision threshold varies, and (b) Variation of Genuine Accept Rate (GAR) as a function of FAR when the threshold varies.

4. Performance Curves

To visualize the performance of biometric systems as the threshold varies, we use performance curves. The most commonly used performance curves are:

- **Score Distribution Curve for Genuine and Impostor Scores**

To assess the accuracy of a biometric system, we need to calculate scores from biometric samples belonging to the same person and scores from biometric samples of different individuals. The distribution of scores from biometric samples belonging to the same person is called the genuine distribution, while the distribution of scores from biometric samples of different individuals is called the imposter distribution. Figure C.1.(a) illustrates the genuine and impostor score distributions. It is evident from this figure that if the threshold T_0 varies, the respective values of FAR and FRR change.

- **FAR and FRR Variation Curve as a Function of the Decision Threshold**

As we have seen before, the performance of a biometric system (verification or open-set identification) is generally evaluated based on FAR and FRR. It is noteworthy that these two rates are highly correlated, and if one increases, the other decreases.

The correlation between FAR and FRR is illustrated in Figure C.1.(b). This correlation is primarily due to the difficulty of separating the genuine and imposter distributions. On this figure, we can observe the error rates for each threshold value. Additionally, the threshold of the Equal Error Rate (EER) point, which is where FAR and FRR are equal, is the intersection of the two curves.

- **FRR Variation Curve as a Function of FAR when the Threshold Varies**

Since both FAR and FRR error rates depend on the same decision threshold, we can also represent the variation of FRR as a function of FAR when the threshold varies. This curve is called the Receiver Operating Characteristic (ROC) curve. This curve graphically represents the performance of a verification or open-set identification system for different values of To. The threshold of the EER point, where FAR and FRR are equal, is the intersection of the curve with the first bisector for ROC curves represented in Figure C.2.(a). By observing Figure C.2.(a), we can identify two other significant points: ZeroFRR, where no false rejections occur, and ZeroFAR, where no false acceptances occur.

- **Cumulative Score Curve**

In closed-set identification mode, the Rank-One Recognition (ROR) is the most commonly used measure, but it is not always sufficient. In the case of an error, it can be beneficial to know if the correct choice is among the ρ_n top responses. We then plot the Cumulative Match Characteristics (CMC) curve, which represents the probability that the correct choice is among the top responses, as illustrated in Figure C.3. On this figure, we can read the value of ROR, which corresponds to $\rho = 1$, and the value of RPR, which corresponds to ROR = 100%.

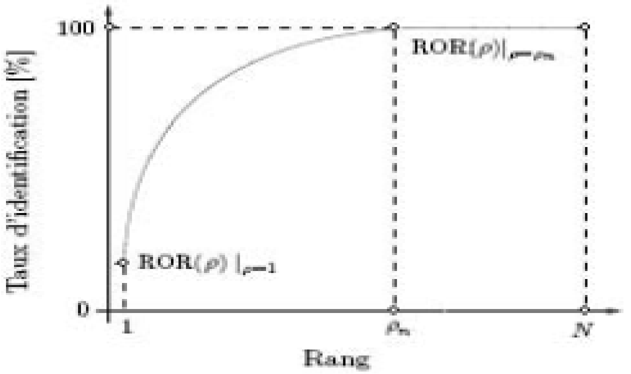


Fig C.3 : Cumulative Score Curve (CMC)