People's Democratic Republic of Algeria

University Kasdi Merbah-Ouargla

Faculty of New Technologies of Information and Communication

Department of Electronic and Telecommunication

FINAL STUDY DISSERTATION

In the aim obtaining of MASTER Degree - ACADEMIC

Domain: Sciences and Technology

Option: Telecommunication

Specialty: Systems of communications

Presented by:

Mokadem Amina

Topic

Efficient person identification by Finger-Knuckle-Print based on Discrete Cosine Transform Network

Was Publicly Debated in: June 2018 in front of The Examining Committee Composed From:

M.N.DHAHRAOUI	MAA	President	UKM Ouargla
Dr. D. SAMAI	MCB	Supervisor	UKM Ouargla
M.K.BEN SID	Doctorant	Co-Supervisor	UKM Ouargla
Dr.M. CHAA	MCB	Examiner	UKM Ouargla

Academic year: **2017/2018**

ABSTRACT

Abstract

One of the current trends in human identification is the development of new emerging methods. Due to increased security concerns and the development of counterfeiting techniques. This development depends on the unique parts of the human body that can be identified and used as a means of identifying a person. Including fingerprints, iris, lips, etc. Most of the systems and methods are slow or require expensive technical equipment, for this, we suggest a new approach for personal authentication using Finger-Knuckle Print through with a novel texture descriptor, Discrete Cosine Transform Network (DCTNet) and support vector machine (SVM) classifier. Finger-knuckle-print is one of the emerging biometric traits.Recently it has been found FKP is highly rich in textures and can be used to uniquely identify a person. The study also takes the unimodal and multi-modal biometric systems results along with their methods of information fusion in score level, which does not require special equipment and can be used in systems where fast detection is needed. Our methods significantly out performs stateof the art methods.

Keywords
Biometric, FKP, DCTNet, SVM, unimodal, multimodal.

DEDICATION

DEDICATION

To my uncle Mokadem Mabrouk

I dedicate this humble work to the memory of my uncle, I constantly pray to the good god, that he may grant you his mercy and welcome you into his vast paradise.

To my daddy Mr.Mokadem miloud and my mother Ms Benyattou houria and my siblings Ahmed Karima Salah Fadila

I am indebted to all of you for your love, support and encouragement through everything.
I could not have done it without you.
Thank you.

ACKNOWLEDGMENTS

ACKNOWLEDGMENTS

First, thank God for giving me the courage and patience to reach this humble work. I would like to thank my supervisor **Mr.Djamal Samai** for spending part of their time in In order to judge my work and the co-supervisor **Mr.Khaled Bensid** for his supervision, follow-up and advice throughout this period.

I would like to thank all who have supported me, I would like to express my great gratitude to my family and friends for their support during these years.

Table of Contents

TABLE OF CONTENTS

LIST OF TABLE

LIST OF TABLES

TABLE **Page**

LIST OF FIGURE

LIST OF FIGURE

List of Figures

Figure **Page**

ACRONYMS

Acronyms

CMC	Cumulative Math Characteristic
DCT	Discrete Cosine Transform
DCTNet	Discrete Cosine Transform Network
DNA	Deoxyribo Nucleic Acid
DWT	Discrete Wavelet Transform
EER	Equal Error Rate
FAR	False Accept Rate
FKP	Finger knuckle Print
FMR	False match rate
FNMR	False non-match rate
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate
KLT	Karhunen Loeve Transform
LF	Left Finger
LIF	Left Index Finger
LMF	Left Middle Finger
PCA	Principal Component Analysis
PCANet	Principal Component Analysis Network
RF	Right Finger
RIF	Right Index Finger
RMF	Left Middle Finger

ROC Receiver Operating Characteristic
ROR Rank-One Recognition

RPR Rank of Perfect Rate

SVM Support Vector Machine

INTRODUCTION

Introduction

Biometrics is considered as a promising solution among traditional methods based on "what we own" (such as a key) or "what we know" (such as a password). It is based on "what we are" and "how we behave". Few people know that biometrics have been used for ages for identification or signature purposes. In 1928 for example[38], fingerprints were used for women clerical employees of the Los Angeles police department.Retinal [39, 40] and signature verification [41, 42] systems came in the 1980s, followed by face [43-44] systems. Iris recognition [45,46] systemswere developed in the 1990s.

There are a huge number of applications for biometric technology and more are being invented constantly. Biometric authentication can be used to provide better-than-password security to online accounts or personal hardware (like phones, tablets or PCs), in healthcare that help doctors and clinicians keep better patient health records.

Since biometric characteristics are distinctive, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification. As a newly emerging technique, biometric recognition systems are being increasingly used by government, business and forensic applications. Nature has made human beings with different characteristics, which may vary from one person to another; this property is used by biometric technology to distinctly identify a person.

Biometrics is the technical term for body measurements and calculations. Some biometric measurements are easy to see and others are not. Those that are on the surface such as facial, iris, fingerprint can be measured from a high-resolution image with an algorithm that compares physical details. There are also what are sometimes called Invisible Biometrics, essentially any type of unique biological quality that is not measured visually, usually because they rely on biological processes rather than outward appearance. Voiceprint biometrics, for instance, which rely on the unique sound of a human's voice, measure a trait that combines the uniqueness of your lungs, larynx and other vocal organs. In every case biometrics, allow for a high level of efficiency and assurance when it comes to every transaction dealing with identity and credentialing.

Most biometric systems deployed in real-world applications are unimodal, they rely on the evidence of a single source of information for authentication (e.g., single ftngerprint or Iris). Unimodal biometric systems often face signiftcant limitations due to sensitivity to noise, data quality, non-universality, and other factors. Limitations of unimodal biometric systems can be overcome by using multimodal biometric systems. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a veriftcation/identiftcation system.

To facilitate the using of physiological methods can be further sub-divided into different subcategories according to their respective position in human body such as hand region attributes, facial region attributes, ocular and periocular region attributes, behavioral attributes, and medico-chemical attributes [2]. A hand has a lot of biometric traits such as ftngerprint, palm print, ftnger/palm vein, ftnger knuckle, and hand geometry. Among such traits, a ftnger knuckle is a relatively new biometric trait in contrast with famous biometric traits such as face, ftngerprint, and iris [1].
In this work, one of these systems was chosen for study, which uses the Finger Knuckle Print (FKP) trait. This trait has been selected according to many great features; accepted by people, simple, easy to use, permanent, stable throughout life, unique to each and another. Finally, the combination of ftngers (ten ftngers with both hands) can be used to create a strong and precise biological system. Our experience is based on deep learning DCTNet for feature extraction and Support Vector Machine (SVM) classiftcation methods. This study aims at achieving the unimodal and multimodal biometric systems based on multi-sample ftnger knuckle print images and from feature extraction.

Increase the performance, the value of safe and trust to security systems based on biometric technologies is the goal of multi-sample images and for DCTNet is to view different representation of several levels to give together upper-level characteristics can efftciently represent the discriminating characteristics of the FKP images.
The main organization of this work are summarized as follows:

Chapter one includes an introduction to the biometric concept, operating modes of the biometric system. This chapter is ftnalized with an overview of the main areas of application of biometrics and their contribution to the global market.
Chapter two focuses on the use of the multi-biometric system, its various structures. In addition to explaining the fusion levels of its various operations (fusion rules).

Chapter three contain some explanation of Feature extraction, deep learning technique "DCTNet" and ”SVM” classifter.

Chapter four presents the results and discussion of the identiftcation system by the FKP modalities. In unimodal system case based on four ftngers (left index ftnger, left middle ftnger, right index ftnger and right middle ftnger), and fusion of the two samples (left ftngers and right ftngers) and of three samples (left index ftnger, left middle and right middle ftnger) forming a multimodal system case.

CHAPTER ONE

CHAPTER 1

INTRODUCTION TO BIOMETRICS

1.1 Introduction

Highly reliable and accessible personal authentication and identification techniques become an inevitable demand for human societies, with the increasing attention on security vulnerabilities and transactional fraudulent in industries and societies. Biometrics has emerged to meet this need and even has developed in the science combining biology technology and information technology to utilize physiological or behavioral characteristics in the human body to deal with identification of individuals. It is implemented to two main aspects applications, identity verification and identity recognition.

1.2 Definition of biometrics

The word biometrics comes from two Greek words and means life measure (”bio” means life and ”metric” means to measure). The definition of biometrics is a branch of biology that uses measurement and statistical analysis to understand humans or animals.

1. When fingerprints and retinal patterns are measured, this is an example of biometrics.

2. When human reproductive patterns are studied by looking at statistics on population growth, this is an example of biometrics.

That branch of biology, which deals with its data statistically, and by mathematical analysis. The scientific measurement and analysis of biological data, as in identifying individuals or in forensics. In the field of authentication, biometrics refers to the measurement of physiological and behavioral characteristics used to identify computer users. Physiological characteristics commonly include the face, fingerprints, and DNA. Behavioral characteristics commonly include the user's digital signature, his or her voice, and walk. Though many methods are involved in biometrics.

1.3 Biometric modalities

It is essential to be familiar with the characteristics of biometric systems in order to better understand how to think objectively about each type and make rational decisions about purchasing and using the technology. Ideally, the biometric characteristics used should satisfy the following properties:

. ***Robustness:*** Over time, the characteristic should not change (Permanence), and thus have low intra-class variability.

. ***Distinctiveness:*** Over the population, a great variation of the characteristic should exist (Uniqueness), and thus have large inter-class variability.

. ***Availability:*** Ideally, the whole population should possess the characteristic (Universality).

. ***Accessibility:*** The characteristic should be easy to acquire (Collectability).

Given the multitude of characteristics that is coupled to a human being, we need some way of classifying the different biometric identifiers, also called the biometric ***modalities.*** A first step is to group them as either behavioral or physiological.

Behavioral identifiers are measurable traits that are acquired over time. The traits can then be used for authentication of a person's identity by using pattern recognition techniques. Behavioral identifiers include for example signature recognition, voice recognition and keystroke dynamics. Physiological identifiers are something you are rather than something you do or know. There are many types of physiological identifiers, including fingerprint, handprint, iris and retina, face, DNA, ECG and many more, as shown in (Figure 1.1).

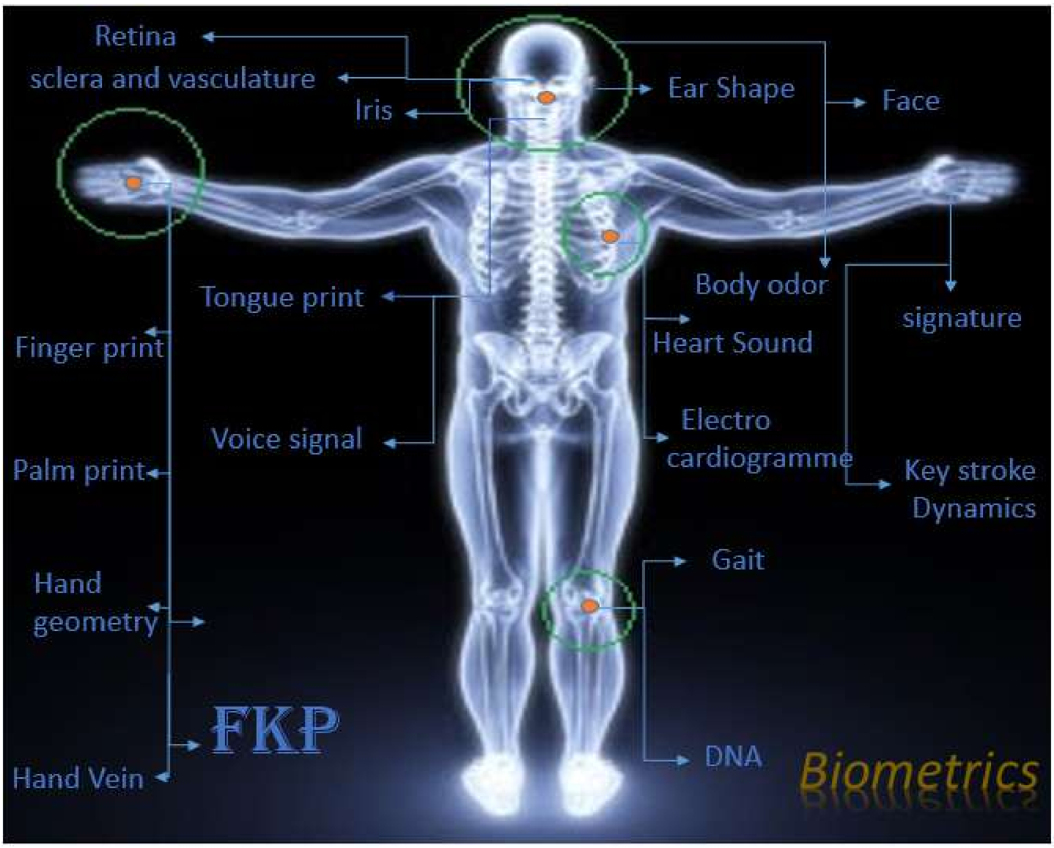

Figure 1.1: Different physiological and/or behavioral biometric characteristics.

1.4 Physiological traits

1.4.1 Finger print recognitions

Ever since latent fingerprints (latents or marks) were first introduced as evidence to convict a suspect in Argentina in 1893 [3], Fingerprint recognition, being the major biometric identifier in use, the ridges on the skin of our fingertips form unique patterns shown in our fingerprints (Figure 1.2).

Figure 1.2: fingerprint.

1.4.1.1 Facial recognition

Facial recognition contains taking many images or pictures of the face and extracting the unique facial features as well as distances from or between the nose, ears, mouth, eyes and cheeks (Figure 1.3) [4].

Figure 1.3: Facial recognition.

1.4.1.2 Iris recognition

The Iris recognition system is a rising field of information technology that uses human iris to identify them. By calculating the iris feature it is possible to identify each individual in a population (Figure 1.4)[5].

Figure 1.4: Iris recognition.

1.4.1.3 Palm print recognition

Palm print recognition is a biometric technology, which recognizes a person based on his/her palm print pattern. Palm print serves as a reliable human identifier because the print patterns are not duplicated in other people, even in monozygotic twins (Figure 1.5)[6].

Figure 1.5: Palm recognition.

1.4.1.4 Vein recognition

Finger-vein authentication is one of the newer biometric modalities. It captures images of the unique vein patterns inside the finger by passing near-infrared light through it and recording the effect via a sensor (Figure 1.6)[6].

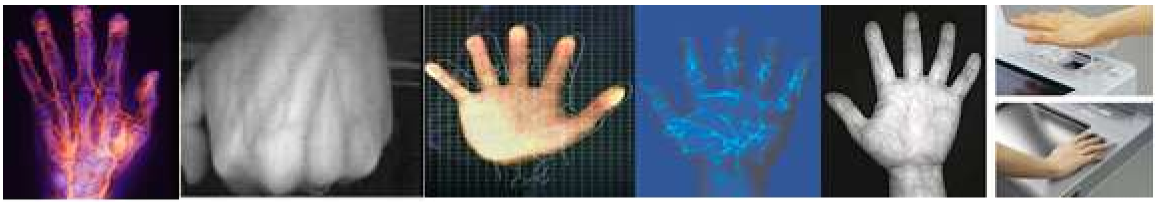

Figure 1.6: Vein recognition.

1.4.1.5 Ear shape recognition

Ear recognition may be done using a digital image, a thermo-graphic image or an ear print. An ear print can be taken by pressing the ear against the flat paper (Figure 1.7)[7].

Figure 1.7: Ear Shape.

1.4.1.6 Retina recognition

Retinal-scan modality makes use of the retina, which is the surface on the back of the eye that processes light entering through the pupil. The principle behind this modality is that the blood vessels in the retina provide a unique pattern, which may be used as a tamper-proof personal identifier(Figure 1.8)[7].

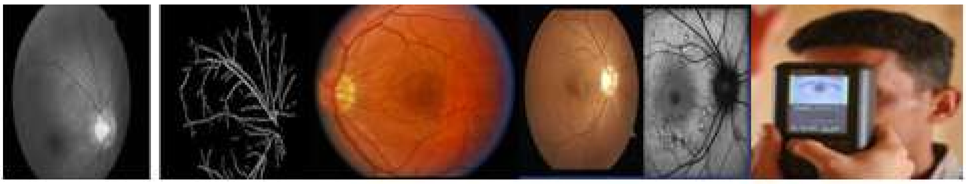

Figure 1.8: Retina recognition.

1.4.1.7 DNA recognition

Deoxyribonucleic acid (DNA) is the structure that defines who we are physically and intellectually, unless an individual is an identical twin, it is not likely that any other person will have the same exact set of genes [Philipkoski, K., 2004]. DNA can be collected from any number of sources: blood, hair, fingernails, mouth swabs, blood stains, saliva, straws, and any number of other sources that has been attached to the body at some time. DNA matching has become a popular use in criminal trials (Figure 1.9).

Figure 1.9: DNA recognition.

1.4.1.8 FKP recognition

Finger-Knuckle-Print (FKP) is one of the emerging biometric traits. The region of interest is the area where the maximum information is centered, for a finger knuckle it is the area surrounding the knuckle region (Figure 1.10).

Figure 1.10: FKP recognition.

1.4.1.9 Tongue print recognition

The tongue is a unique organ in that it can be stuck out of mouth for inspection, and yet it is otherwise well protected in the mouth and is difficult to forge. The tongue also presents both geometric shape information and physiological texture information which are potentially useful in identity verification applications (Figure 1.11).

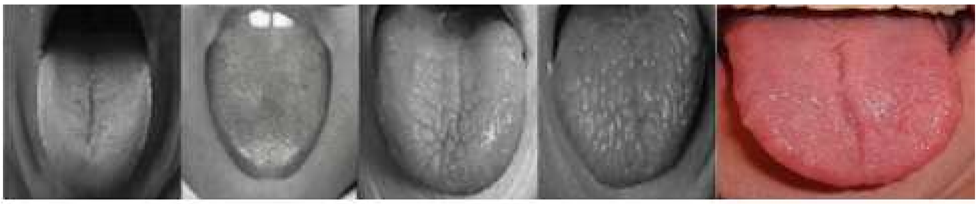

Figure 1.11: Tongue print recognition.

1.5 Behavioral

1.5.1 Gait recognition

Human gait recognition works from the observation that an individual walking style is unique and can be used for human identification. So as to recognize individual's walking characteristics, gait recognition includes visual cue extraction as well as classification (Figure 1.12)[8].

Figure 1.12: Gait recognition.

1.5.1.1 Voice recognition

Voice recognition is the process of automatically recognizing who is speaking on the basis of individual information included in speech waves (Figure 1.13)[8].

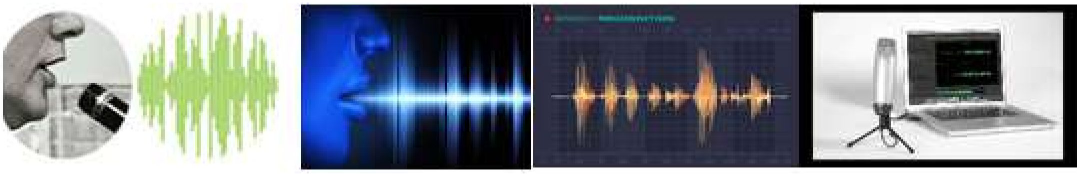

Figure 1.13: Voice recognition.

1.5.1.2 Signature recognition

Each person has a unique style of handwriting, and no two signatures of different persons are identical. However, the variations of a typical signature also depend upon the physical and emotional state of a person (Figure 1.14)[8].

Figure 1.14: Signature recognition.

1.5.1.3 Keystrokes recognition

Keystroke Dynamics is one of the famous biometric technologies, which identifies the authenticity of a user when the user is working via a keyboard. The authentication process is done by observing the variation in the typing pattern of the user. A comprehensive study of the existing keystroke dynamics methods, metrics, and different approaches are presented (Figure 1.15)[9].

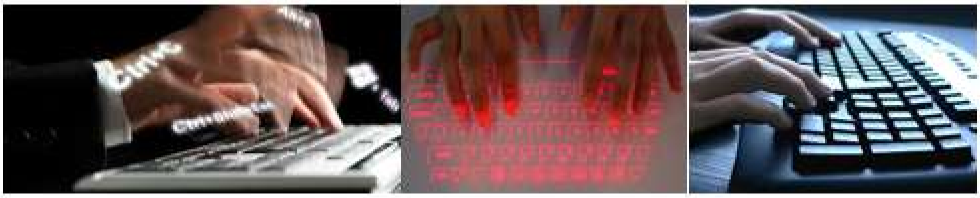

Figure 1.15: Keystorks recognition.

1.5.1.4 Electrocardiogram recognition

The human heartbeat can be used for identity recognition. Existing solutions for biometric recognition from electrocardiogram (ECG) signals are based on temporal and amplitude distances between detected fiducially points (Figure 1.16).

Figure 1.16: Electrocardigram recognition.

1.6 Biometrics market

There is no absolute best biometric technique, all depending on the exact nature of the application and the reasons for its implementation. However, we can analyze their distribution from the point of view of use, and compare them in their own contexts according to their performance criteria. A report on the biometrics market is published by the International Biometry Group (IBG) regularly. This study is a comprehensive analysis of the sales, growth trends and industrial developments of the current and future biometrics market. Reading this report is essential for institutions that deploy biometric technology, biometric business investors or biometric solutions developers.

The most common biometric identifiers used in biometric authentication systems today are fingerprint, face, voice vein and signature. Fingerprints continue to be the leading biometric technology in terms of market share, nearly 65% of total revenue (Fig 1.17).

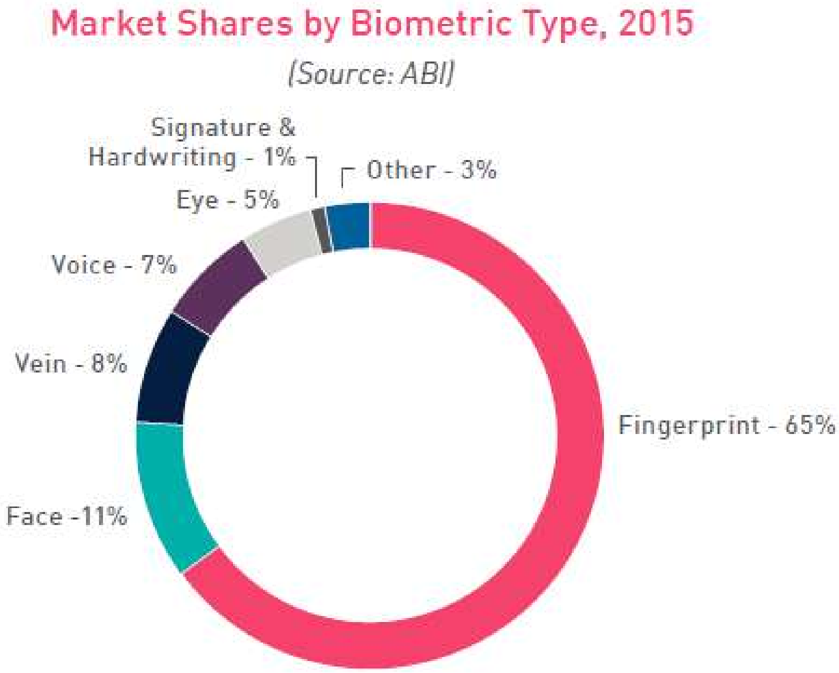

Figure 1.17: Biometrics market share by system type .based on revenue (Source: ABI Research 2016).

1.7 Biometric system

Although the various biometric technologies vary in what and how they scan, the principle of operation is very similar (see Figure.1.18). It consists predefined steps as well as we must know some basic terms related to a biometric system as enrollment, biometric data, presentation, template, feature extraction, matching, Decision.

1.7.1 Enrollment or Registration

The process, by which a user's biometric data is initially obtain, processed and stored in the form of a template for ongoing use in a biometric system. It is called enrollment or registration process. This template will be used for further process as authentication.

1.7.2 Biometric Data

The data presented by the user during registration is called unprocessed image data, which is also referred as raw biometric data or biometric sample. Raw biometric data cannot be used to perform biometric matches so it is used to generate biometric template with the help of feature extraction process.

1.7.3 Presentation

The process by which user presents his/her biometric data to the acquisition devices, the hardware which is used to collect data. For example, placing a finger on a plate at finger reader device.

1.7.4 Template

A mathematical representation of raw biometric data, which is obtained after applying a number of feature extraction algorithms. A template size can vary in size from a few bytes for hand geometry to several thousand bytes for facial recognition. The template created at the time of registration is called stored template and at the time of authentication is called a live template.

1.7.5 Feature Extraction

The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction takes place during enrollment and verification, any time a template is created.

1.7.6 Matching:

A process where the stored template is matched with the live template at the time of verification and we obtained a score, on the basis of this score we conclude that a user is authenticated human or not [10].

1.7.7 Decision-making:

The user's identity is either established or a claimed identity is accepted or rejected. This is done based on the results of the matching modules.
A biometric system can operate either in verification or identification mode. Biometric

verification is not the same as biometric identification, and it is important to understand what the difference is between verifying someone and ascertaining their identity.

In **Verification mode**, the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be, (I am who say I am?)[11].

In **Identification mode**, the system performs a one-to-many comparison against a biometric database in the attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person where the system establishes whether the person is who she (implicitly or explicitly) denies to be, (who am I?)[11].

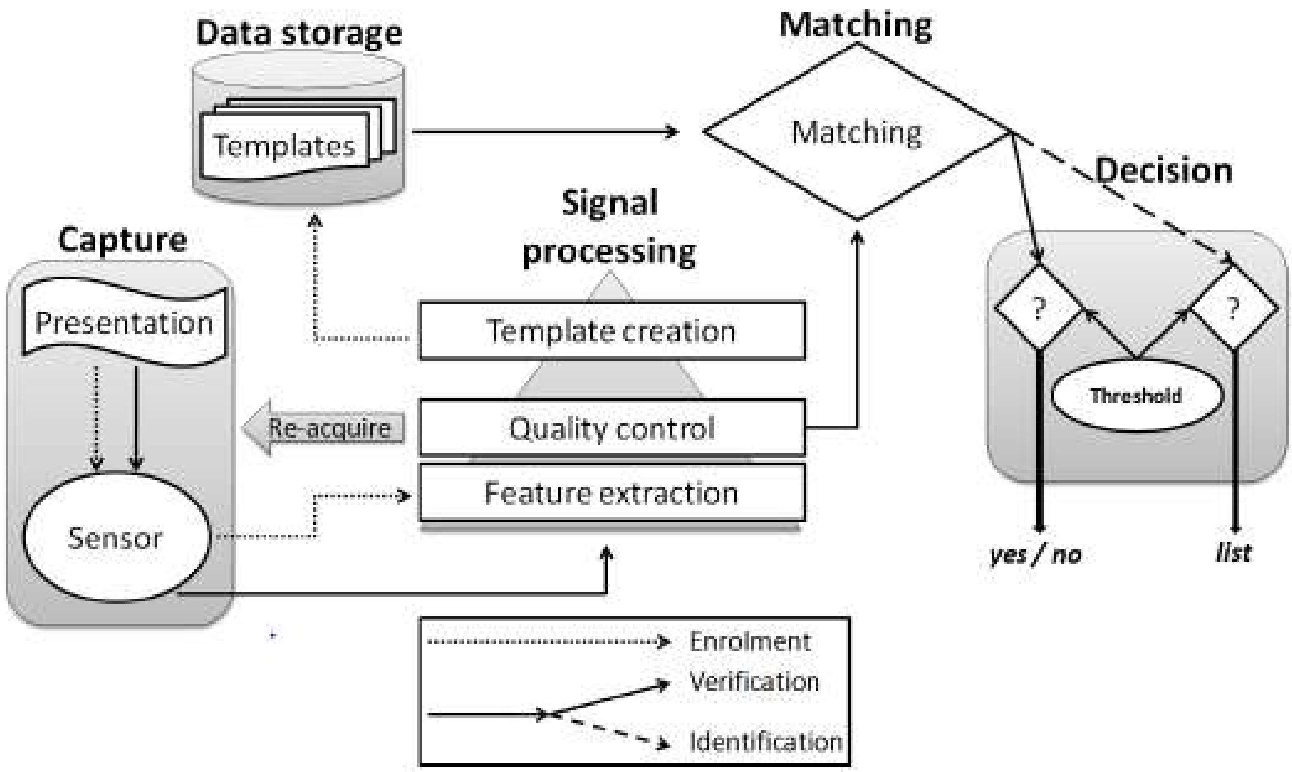

Figure 1.18: Architecture of a biometric system (Source [12]).

1.8 Biometric Performance Measures

A. False acceptance rate (FAR) or false match rate (FMR): The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

$$FAR(\%) = \frac{TotalFalseAcceptance}{TotalFalseAttempts} \tag{1.1}$$

B. False reject rate (FRR) or False non-match rate (FNMR): The probability that the system incorrectly declares the failure of the match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.

$$FRR(\%) = \frac{TotalFalseRejections}{TotalTrueAttempts} \tag{1.2}$$

C. Receiver (or relative) operating characteristic (ROC): In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems, the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes.

D. Equal error rate (EER): The rates at which both accept and reject errors are equal. **ROC** or **DET** plotting is used because how **FAR** and **FRR** can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value (Figure.1.19). The lower the EER, the more accurate the system is considered to be.

$$FAR = FRR \tag{1.3}$$

E. Genuine Acceptance Rate (GAR): It is the rate of clients who are accepted by the system. This rate is important because it represents the suction of the biometric system.

$$GAR(\%) = 1 - FRR \tag{1.4}$$

F. Cumulative match characteristic curve (CMC): In the case of a system used in identification mode, The **CMC** curve (Figure.1.20) gives the percentage of people recognized according to a variable called rank. It is said that a system recognizes rank one when it chooses the nearest image as a result of recognition. It is said that a system recognizes at rank two, when it chooses, from two images, the one that corresponds best to the input image, etc. CMC curve is just another way of displaying the performance of a biometric system and can be also calculated from the **FAR** and the **FRR**.

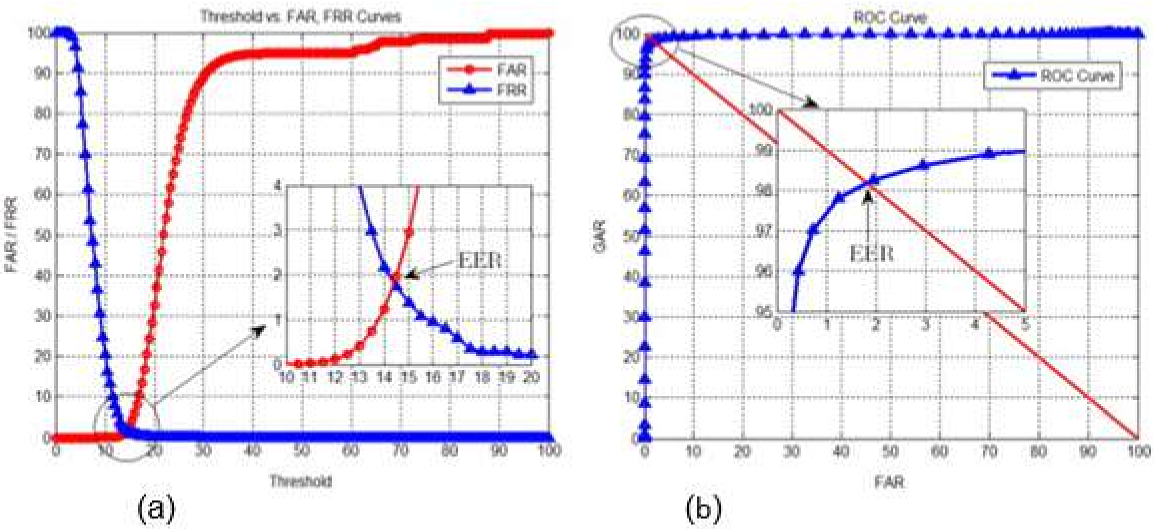

Figure 1.19: (a) Variation of FRRs and FARs depending on the threshold.(b)Roc curve depending of changement of FAR and GAR.

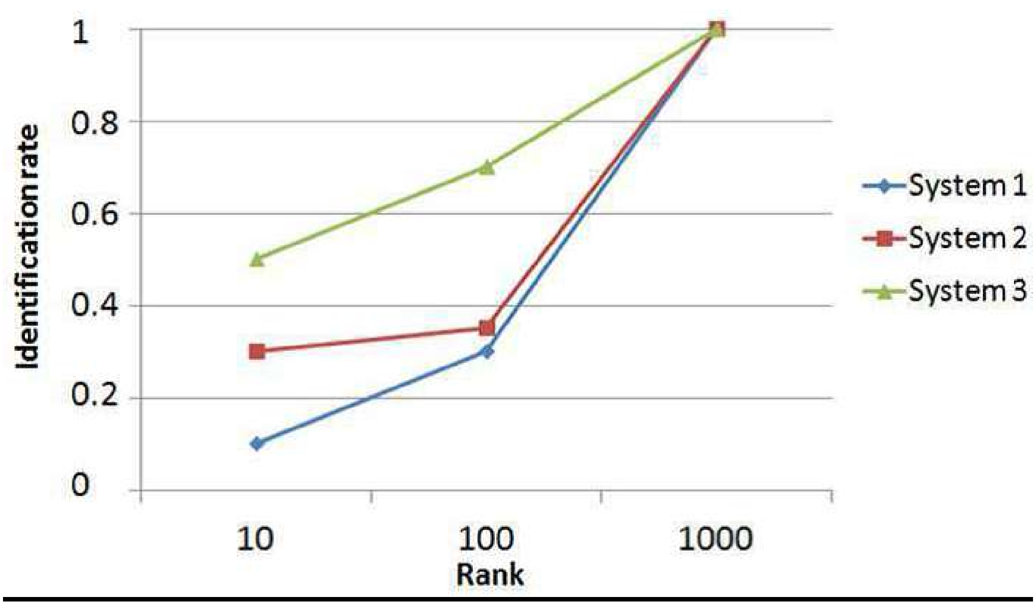

Figure 1.20: Examples of CMC curves of three biometric systems.

1.9 Biometric application

Most biometric applications fall into one of nine general categories [13]:

* Increase security - Provide a convenient and low-cost additional tier of security.

* Reduce fraud by employing hard-to-forge technologies and materials. For e.g. Minimise the opportunity for ID fraud, buddy punching.

* Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes for e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.

* Reduce password administration costs.

* Replace hard-to-remember passwords, which may be shared or observed.

* Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.

* Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN! Offer significant cost savings or increasing ROI in areas such as Los Prevention or Time and Attendance.

* Unequivocally link an individual to a transaction or event.

* Financial services (e.g., ATMs and kiosks).

* Immigration and border control (e.g., points of entry, precleared frequent travelers, passport and visa issuance, asylum cases).

* Social services (e.g., fraud prevention in entitlement programs).

* Health care (e.g., security measure for privacy of medical records).

* Physical access control (e.g., institutional, government, and residential).

* Time and attendance (e.g., replacement of time punch card).

* Computer security (e.g., personal computer access, network access, Internet use, e-commerce, e-mail, encryption).

* Telecommunications (e.g., mobile phones, call center technology, phone cards, televised shopping). Law enforcement (e.g., criminal investigation, national ID, driver's license, correctional institutions/prisons, Home confinement, smart gun).

1.10 Conclusion

Through this chapter, we have introduced the concept of a biometric system, its architecture and its different applications, the main modules of biometric systems and how to measure their performance. In the following chapter, the thesis proposes multimodal biometric systems as a solution to the problem of unimodal limitation.

CHAPTER TWO

CHAPTER 2

MULTI-MODAL BIOMETRICS

2.1 Introduction

The increasing demand of enhanced security systems has led to an unprecedented interest in biometric-based person authentication system. A biometric system is a Pattern Recognition system, which acquires required data, extract the feature set from it, and compare it with the template set stored in the database. Most biometric systems deployed in real-world applications are unimodal. Using unimodal biometric systems has to contend with a variety of problems, what if the biometric source becomes unreliable due to sensor or software malfunction, poor quality of specific biometric trait of the user, or deliberate manipulation?. These problems have been addressed by using multibiometric systems, which expected to be more reliable due to the presence of multiple, independent pieces of evidence. The process of consolidating the information or evidence presented by multiple biometric sources is known as information fusion, which is the main focus of this chapter.

2.2 Unimodal biometrics limitations

The unimodal biometric verification systems are more reliable than classical authentication systems. Unimodal biometric systems perform person recognition based on a single source of biometric information [14]. Such systems are often affected by the following limitations and problems:

The lack of universality of some characteristics (for instance, in the case of fingerprints, approximately 4% of people cannot enlist because of weak fingerprints, and this percent increases at 7% in the case of the iris);

Noisy signals captured from the sensors due to the incorrect usage by the clients and due to the environmental conditions (humidity, dirt, dust etc.).

The lack of the safety of the used sensors.

The limitation of the discrimination of biometric systems due to a high in-class and low inter-class variability.

The recognition performances of the systems are upper limited at a certain level.

Unacceptable error rates for the unimodal biometric systems.

The lack of permanence and variability in time of the biometric characteristics.

The fraud possibility through voluntarily or involuntarily cloning (of) a biometric characteristic.

2.3 Multimodal Biometric System

This system can be defined as one that combines the outcome obtained from more than one biometric feature for the purpose of identification. Unlike a unimodal biometric system that may result in non-universality, a multimodal system uses multiple biometric modalities that can result in highly accurate and secure biometric identification system [15,16].

2.4 Advantages of multibiometric systems

Biometric systems can be designed to recognize a person based on information acquired from multiple biometric sources. Such systems, known as multibiometric systems can be expected to be more accurate due to the presence of multiple pieces of evidence. Multi-biometric systems offer several advantages over traditional unibiometric systems listed below:

1. Multibiometric systems can offer substantial improvement in the matching accuracy of a biometric system depending upon the information being combined and the fusion methodology adopted.

2. Multibiometric systems address the issue of non-universality or insufficient population coverage.

3. It becomes increasingly difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual.

4. Multibiometric systems effectively address the problem of noisy data.

5. Multibiometric systems help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient.

6. A multibiometric system may be viewed as a fault tolerant system, which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation.

2.5 Multimodal Categories

Multi-biometric systems have two basic categories:
Synchronous and asynchronous. In synchronous, two or more biometrics combined within a single authorization process. On the other hand, asynchronous system uses two biometric technologies in sequence (one after the other) [39]. Multimodal biometric systems can operate in three different modes [40]:

2.5.1 Serial Mode (cascade mode)

Each modality is examined before the next modality is investigated. The overall recognition duration can be decreased, as the total number of possible identities - before using the next modality could be reduced (Figure 2.1).

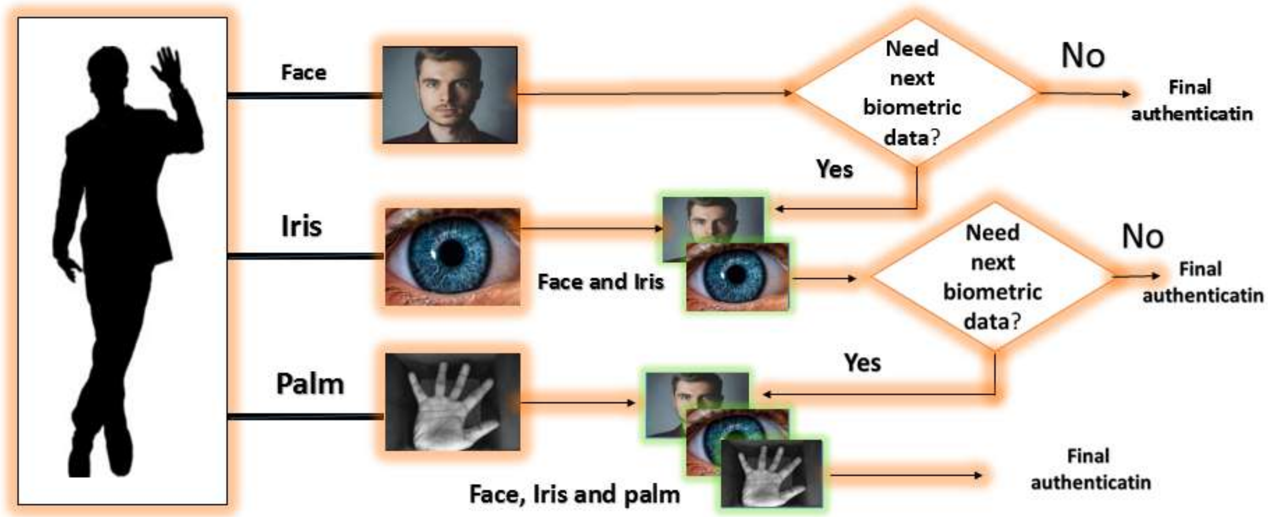

Figure 2.1: Serial Mode.

2.5.2 Parallel Mode

Sensed/captured data from multiple modalities are used in concurrent way to perform recognition. Then the results are combined to make final decision (Figure 2.2).

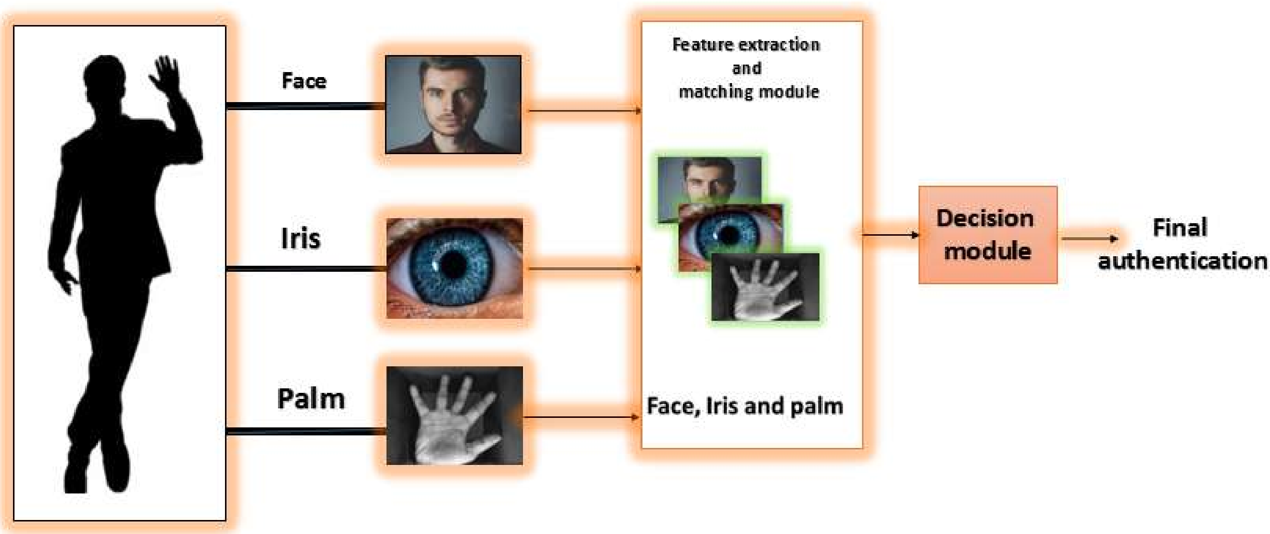

Figure 2.2: Parallel Mode.

2.5.3 Hierarchical Mode

Individual classifiers are combined in a hierarchy -tree like- structure. This mode is preferred when a large number of classifiers are expected.

2.6 Fusion scenarios

The application scenario plays an important role in making the design decisions, which influence the performance of the system. System using multiple biometric traits can be classified into six categories [17]:

2.6.1 Multi-sensor systems

Multiple sensors are used to capture the images of a single biometric trait of the user. For example, complementary information corresponding to fingerprints can be acquired using different types of sensors (like optical and capacitive sensors). Information obtained using these different sensors are then integrated using the sensor level fusion technique (Figure 2.3).

Figure 2.3: Multi-sensor.

2.6.2 Multi-algorithm systems

Multiple matching algorithms are applied to a single biometric trait. To get the final decision, any of the matching fusion technique (feature level, score level, rank level etc.) can be applied on the obtained results using different matching algorithms. These systems are more economical as no extra device is required to capture the data, but are also more complex because of the application of different algorithms (Figure 2.4).

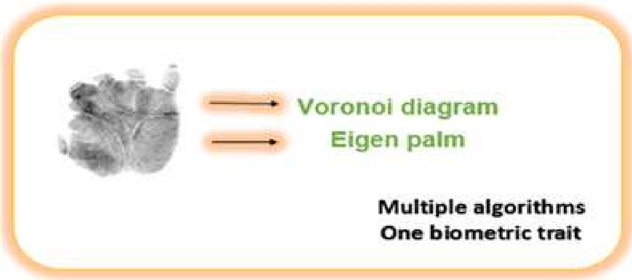

Figure 2.4: Multi-algorithm.

2.6.3 Multi-instance systems

Multiple instances of a single biometric trait are captured. For example, images of the left and right irises can be used for iris recognition. If a single sensor is used to acquire these images in a sequential manner, the system can be made really cost effective (Figure 2.5).

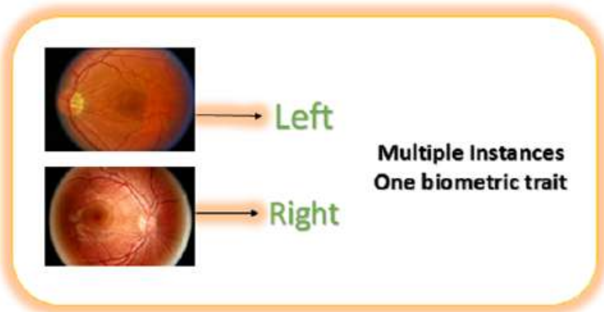

Figure 2.5: Multi-instance.

2.6.4 Multi-sample systems

Multiple samples of a same biometric trait are captured. For example, along with the frontal face, the left and right profiles are also captured (Figure 2.6).

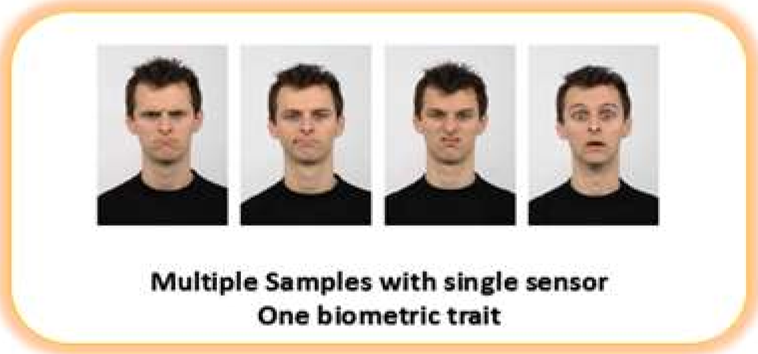

Figure 2.6: Multi-sample.

2.6.5 Multi-modal systems

More than one biometric trait is used for user identification. For example, the information obtained using face and voice features can be integrated to establish the identity of the user. To obtain better results, physically uncorrelated traits (like face and fingerprints) must be integrated. This can be more costly because it requires multiple sensors to capture different traits, but the improvement in performance is substantial (Figure 2.7).

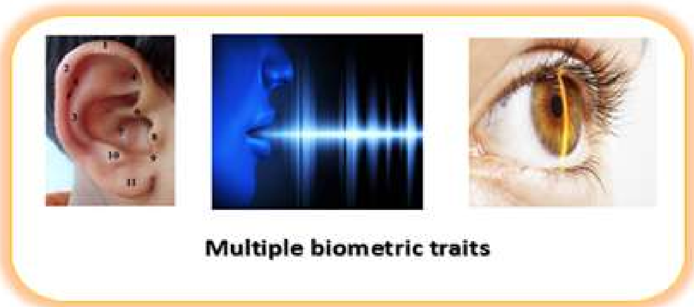

Figure 2.7: Multi-modal.

2.6.6 Hybrid systems

It is a system, which integrates more than one of the above mentioned multi-biometric systems. For example, two face recognition algorithms can be combined with two fingerprint recognition algorithms. Such a system will be multi-modal and multi-algorithmic system. If multiple sensors are used to obtain these images, then it will be multi-sensory and if multiple instance of the finger are used, it will be multi-instance system also.

2.7 Level of Fusion In Multimodal Biometric

When we employ the data from any of the modules discussed before, sensor, feature, matching and decision making module; they can be fused in more than one biometric system and called “fusion”. The different levels of fusion are therefore sensor, feature, matching score and decision level fusion [18,19].

2.7.1 Sensor level fusion

Sensor level fusion (Figure 2.8) entails the consolidation of evidence presented by multiple sources of raw data before they are subjected to feature extraction. Sensor level fusion can benefit multi-sample systems, which capture multiple snapshots of the same biometrics.

2.7.2 Feature Level Fusion

Feature level fusion (Figure 2.8), consolidating the feature sets obtained from multiple biometric algorithms into a single feature set, after normalization, transformation and reduction schemes.

a) Feature normalization: The goal of feature normalization is to modify the location (mean) and the scale (variance) of the feature value via a transform function in order to map them into a common domain. (e.g. Min-max normalization, Median normalization) [20].

b) Feature Selection or Transformation: Algorithm use to reduce the dimensionality of the feature set. (e.g. Sequential forward selection, Sequential backward selection, PCA).

2.7.3 Score Level Fusion

In score level fusion (Figure 2.8), the match scores output by multiple biometric matchers are combined to generate a new match score (a scalar). When match scores output by different biometric matchers are consolidated in order to arrive at a final recognition decision, fusion is said to be done at the match score level. (e.g. similarity score, distance score).

2.7.4 Decision Level Fusion

In a multibiometric system, fusion is carried out at the abstract or decision level (figure 2.8) when only final decisions are available [21], this is the only available fusion strategy (e.g. AND, OR, Majority Voting, Weighted Majority Voting, Bayesian Decision Fusion).

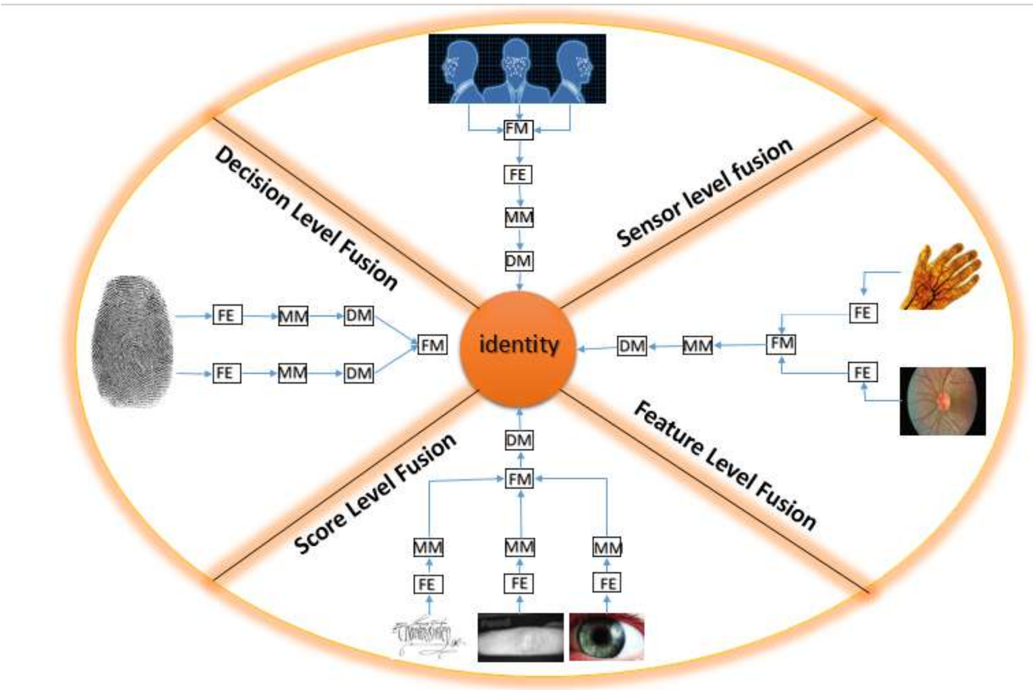

Figure 2.8: Level of fusion in multibiometric Which: FE (feature extraction) MM (matching module) FM (fusion module) DM (decision module).

2.8 Scores Normalization

The scores obtained from different matchers may have different ranges, (e.g., [0,100], [-1, 1], etc.), and may be of different types (similarity vs. distance). Therefore, it is important to normalize the scores from different matchers to a common domain, say [0, 1], before combining them using a fusion rule.

The normalization techniques may be linear or non-linear based on the function used to normalize the scores. Examples of linear normalization techniques include min-max normalization that is used to normalize the scores to a [0, 1] range, and decimal scaling to normalize scores to the same order of magnitude.
Non-linear score normalization techniques use normalization functions with tunable parameters, e.g., double sigmoid and tanh functions. These techniques are discussed in detail below.

2.8.1 Min-max normalization

Is used to normalize the scores to a [0,1] range. The minimum and maximum bounds on the possible scores may be known a priori or may be estimated from the data. Given the original score S_k, the normalized score $S_k^{'}$ is given by

$$S_k^{'} = \frac{S_k - \min(S)}{\max(S) - \min(S)} \tag{2.1}$$

Min-max normalization is not robust and is sensitive to outliers, especially when the bounds on the scores are estimated from data.

2.8.2 Decimal scaling

Is useful when the scores from different matchers are different by orders of magnitude. The normalized score $S_k^{'}$ is calculated as

$$S_k^{'} = \frac{S_k}{10^n} \tag{2.2}$$

Where $n = \log 10[max(S)]$. Decimal scaling is not robust and is sensitive to outliers.

2.8.3 Z-score normalization

Is the most commonly used normalization technique and is useful when the scores have a Gaussian distribution.The normalized score $S_k^{'}$ may be computed as

$$S_k^{'} = \frac{S_k - \mu}{\sigma} \tag{2.3}$$

Where μ and σ are the mean and standard deviation of the distribution of S, either known or estimated from the data.
The Z-score normalization is sensitive to outliers, but comparatively lesser than the earlier two methods. Note that Z-score normalization may not be optimal if the actual underlying score distribution is not Gaussian [22].

2.8.4 Median and median absolute deviation (MAD)

Has been proposed as an alternative to Z-score normalization. In this method, the normalized score . In this method, the normalized score$S_k^{'}$ is computed as

$$S_k^{'} = \frac{S_k - median(S)}{MAD} \tag{2.4}$$

Where $MAD = median(|S_k - median(s)|)$.

This method of normalization is not sensitive to outliers but performs worse than Z-score normalization when the underlying distribution is not Gaussian.
Both the Z-score and the median and MAD normalization schemes do not return normalized scores in a pre-determined bounded interval.
Non-linear normalization techniques that use tunable parameters have also been proposed. These include double sigmoid [23] and tanh [24] normalization.

2.8.5 The double sigmoid function

Has three tunable parameters t , r_1 and r_2, where r_1 and r_2 denote the region around operating point t where normalization is approximately linear. The normalized score $S_k^{'}$ is computed as follows

$$S_k^{'} = \begin{cases} \frac{1}{1+exp\left(-2(S_k - \frac{t}{r_1})\right)^{'}} & s_k < t \\ \frac{1}{1+exp\left(-2(S_k - \frac{t}{r_2})\right)^{'}} & \text{othewise} \end{cases} \tag{2.5}$$

This normalization is especially useful in amplifying the difference in the region of overlap between genuine and impostor scores $(t - r_1, t + r_2)$.

2.8.6 Tanh normalization

Is robust and is insensitive to outliers. The normalized scores may be computed as

$$S_k^{'} = \frac{1}{2}\left(\tanh\left(\alpha\left(\frac{s_k - \mu_H}{\sigma_H}\right)\right) + 1\right) \tag{2.6}$$

2.9 Fusion methods

Once the scores from different matchers have been transformed to a common domain, they are fused together using a fusion rule, such as one of the following [25]. These fusion rules work best when the scores obtained from different matchers are independent.

2.9.1 The weighted sum rule

Finds the weighted arithmetic [26] mean of the normalized matching scores obtained from different classifiers.

$$score^{(j)} = \sum_i W_i^{(j)} S_i^{(j)} \tag{2.7}$$

Where $score^{(j)}$ is the final score after fusion for the jth subject and $W_i^{(j)}$ and $S_i^{(j)}$ are the weights and normalized scores respectively for the ith matcher and the jth subject. The weights corresponding to different matchers may be subject specific, Note that the weighted average is subject to the condition $\Sigma W_i^{(j)} \overset{\text{def}}{=} 1 \forall ji$

2.9.2 The weighted product rule

Finds the weighted geometric [27] mean of the normalized matching scores.

$$score^{(j)} = \left(\prod_i W_i^{(j)} S_i^{(j)}\right)^{\frac{1}{\Sigma W_i^{(j)}}} \tag{2.8}$$

2.9.3 The median rule

Is a robust alternative for the sum rule, because the arithmetic mean is sensitive to outliers.

$$score^{(j)} = median(S_i^{(j)}) \tag{2.9}$$

2.9.4 The max rule

Chooses the normalized score from the matcher that presents the greatest degree of confidence.

$$score^{(j)} = \max(S_i^{(j)}) \tag{2.10}$$

2.9.5 The min rule

Chooses the normalized score from the matcher that presents the least degree of confidence.

$$score^{(j)} = \min(S_i^{(j)}) \tag{2.11}$$

2.10 Conclusion

Multimodal biometric systems have better accuracy and reliability due to the use of multiple biometric traits to authenticate a claimed identity or perform identification. For this, we exposed the advantage of a multimodal biometric, the different forms of the multi-modality, the different scenarios and fusion levels. All that after some unimodal biometrics limitations.

CHAPTER THREE

CHAPTER THREE

CHAPTER 3

FEATURE EXTRACTION

3.1 Introduction

The image is a set of different information, so that each image has specific characteristics that create a difference between each image about other, this feature used in the recognition system, because it is special property and stable with time.

3.2 Feature Extraction

An image defined in the ”real world”is considered to be a function of two real variables, for example, a(x, y) with a as the amplitude (e.g. brightness) of the image at the real coordinate position (x, y). An image may be considered to contain sub-images sometimes referred to as regions-of-interest, ROIs, or simply regions.
A feature is defined as an ”interesting” part of an image, and is used as a starting point in main primitives for subsequent algorithms .Over the last decades, image feature detectors and descriptors have become popular tools in the computer vision community and they are being applied widely in a large number of applications ,e.g. Image representation [28], object recognition and matching [29,30].

The various features classified and currently employed are:

a) General features: Independent features such as color, texture, and shape according to the abstraction level, they can be further divided into:

- **Pixel-level features:** Features calculated at each pixel, e.g. color, location.
- **Local features:** Features calculated over the results of subdivision of the image band of an image segmentation or edge detection (Thawar Arif, et al., 2009).
- **Global features:** Features calculated over the entire image or just regular sub-area of an image.

b) Domain-specific features : Application of dependent features such as human faces, fingerprints and conceptual ones.

However, the choice of feature extraction method is based on three essential categories, namely the line, the appearance and the texture. The majority of work shows that the most distinctive information, it is in the texture analysis, for that we chose a deep learning DCTNet algorithm and SVM classifier.

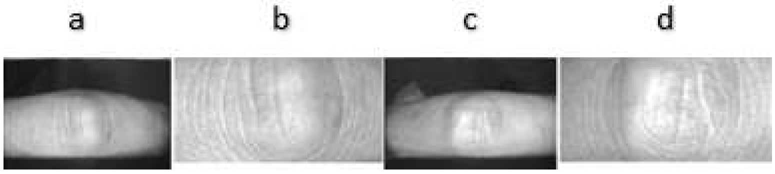

Figure 3.1: (a) and (c) are two FKP images; (b) and (d) are the ROI images of (a) and (c).

3.3 DCTNet Deep Learning

Recently, deep convolutional network shows its success in various image classification tasks has drawn significant attention. Many researchers have focused on deep learning because of its ability for automatically learning good representations of the underlying distribution of the data and learn abstract representation of the data build up in multiple stages.in order to learn good features, the networks usually have multi-layer and many hidden units which lead to extremely high training time costs.

DCT has been successfully used in computational intelligence as both a function approximation method [31] and a network compression method [32].In this study, we develop a biometric system for FKP recognition. The system is based on using the two-dimensional $(2-D)$ Discrete Cosine Transform (DCT) to obtain distinctive features from an FKP image. The choice of 2D DCT basis as filter bank is inspired by the Karhunen Loeve Transform (KLT) in transform coding literature, which is also known as Principal Component Analysis (PCA) in multivariate statistics community.

DCTNet [33] is an alternative to PCANet, which employs Discrete Cosine Transform (DCT) as filter banks instead of PCA. As well known, PCANet is data-dependence hence inflexible. In DCTNet, on the other hand, the filter banks created by DCT achieve a data-independent network, increasing the performance of the network. In order to decrease the computational complexity of the learning stages of the network, 2D DCT is also employed. Besides the low computational complexity, 2D DCT filter banks are independent from data, therefore, generating a learning-free framework. The main idea of the approach is instead of learning the set of filters at each layer of deep networks, Inspired by the scattering transform and PCANet, DCTNet was proposed in [33, 34, 35]. DCTNet uses a prefix cosine function as filter; this is an approximation of the eigenfunction used in PCANet. It performs multilayer short time Discrete Cosine Transform (DCT).
Classification of the FKP image is then achieved by applying a standard linear SVM classifier to the coefficients (features) extracted from the DCT (frequency) matrix. This shows that the modified DCTNet is a simple flexible and effective feature extractor for FKP image processing.
DCTNet structure is an extra layer at the histogram output for histogram normalization as shown in (Figure 3.2.)

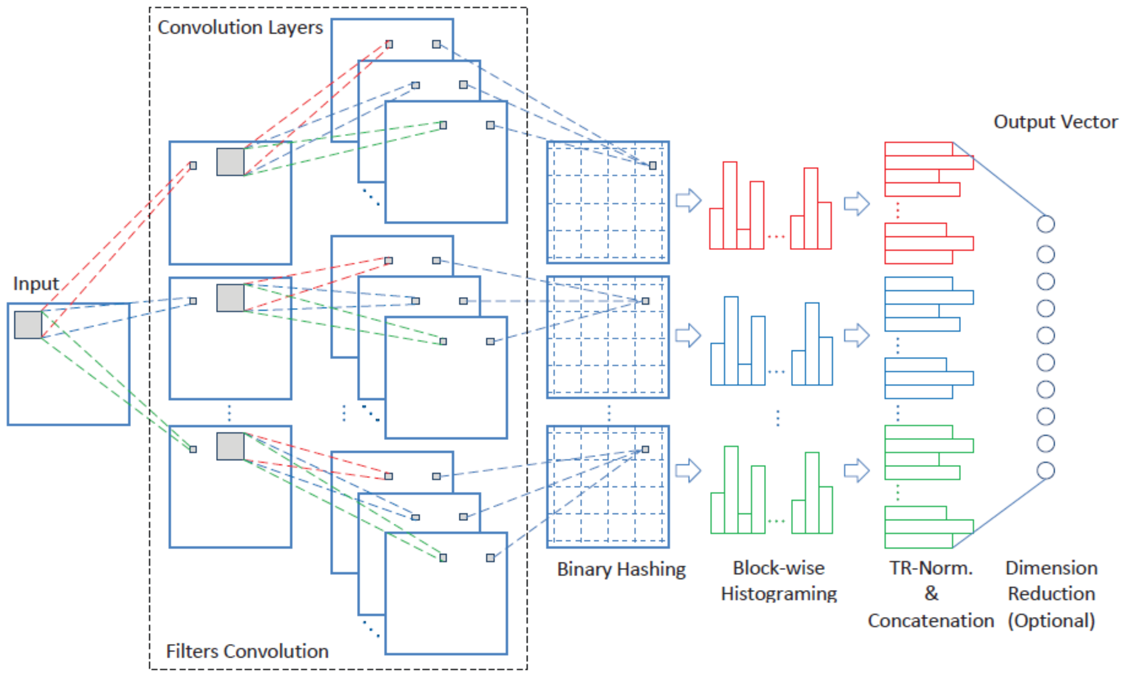

Figure 3.2: The block diagram of the proposed DCTNet Source [33] .

The following are the main elements of the DCT Net structure:

A. Convolution Layer: The output of input image Id of size nm with D channels given by

$$O_d^p = \left\{ I_d * W_l^p \right\}_p^{p_l} \tag{3.1}$$

Where $(*)$ denotes the discrete convolution and the size of output O_d^p is same as I_d and $W_l^p \in \Re^{k*k}, p = 1,2,...,p_l$ is 2D-DCT bases from p_l filters at layer l.

B. Binarization and Block-wise Histograming:

The outputs of convolution layer of DCTNet give real values. In this step, the output obtained in the last layer is turned into binary format with the comparison of responses with threshold to zero (value 1 for positive response, zero otherwise) denoted by BIN .

$$BIN(O_d^p) = \begin{cases} 1 \longrightarrow O_d^p \geq 0 \\ 0 \longrightarrow othewise \end{cases} \tag{3.2}$$

C. Histogram Tied Rank Normalization (TR Normalization):

Each of these binary images is divided into B non-overlapping blocks. The characteristics of these images are obtained by concatenating all the histograms of each block B such as

$$H = \left\{ O_b^d \right\}_{b=1,d=1}^{B,D} \tag{3.3}$$

Where $b = 1,2,...,B$, $d = 1,2,...,D$ The combination of binary hashing and block-wise histograms should be able to extract discriminating characteristics.

3.4 Support Vector Machine Classification

Support vector machines (SVM) is a form of supervised machine learning model. By learning from provided examples -the training data- the model finds a function that couples input data to the correct output. The output for novel data can then be predicted by applying the retrieved function. SVM is often used for classification problems for which the correct output is the class the data belongs to. The model works by creating a

hyperplane that separates data points from one class from those from the other class, with a margin as high as possible. The margin is the maximal width of the slab parallel to the hyperplane that has no interior data points.
The support vectors, which give the model its name are the data points closest to the hyperplane and therefore determine the margin.

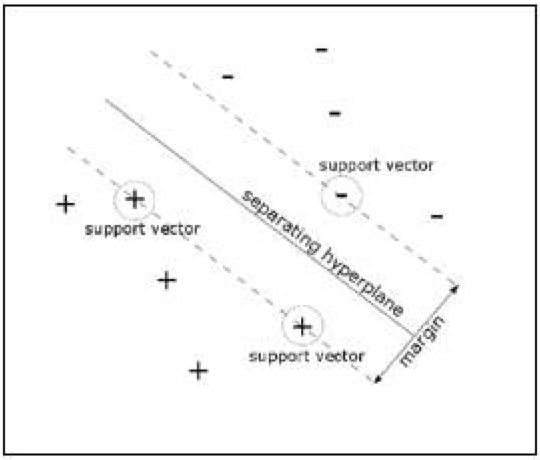

Figure 3.3: Illustration of the hyperplane separating data points from two classes shown as + and -. The support vectors and the margin are marked.

1. Multiclass SVM

A support vector machine is a technique of discrimination, it is a supervised learning method for classification and regression. It consists in separating two or more sets of points by a hyperplane. Depending on circumstances and configuration points. The original idea of SVM is based on using kernel core functions that allow optimal separation of the points of the plan in different categories. The method uses a set of training data. Which enables a hyperplane separating the best points. In this paper, we use the multi class SVM [36].

2. Normalization method

Score normalization is needed to transform these scores into a common domain, prior to combining them. Thus, a Min-Max normalization scheme was employed. To transform the scores computed into similarity scores in the same range. Thus,

$$\tilde{D} = \frac{D - min(D)}{max(D) - min(D)} \tag{3.4}$$

Where $\tilde{D}$ represent the normalized vector. However, these scores are compared, and the lowest score is selected. For perfect matching, the matching score is zero.

Consider the problem of separating the set of training vectors belong to two separate classes, $(x1, y1)...(xl, yl)$,where $xi \in R^n$,$yi \in -1, +1$ with a hyperplan $wx + b = 0$. The set of vectors is said to be optimally separated by the hyperplane if it is separated without error and the margin is maximal.A canonical hyperplane has the constraint for parameter $w, b : min_{xi} yi(w.xi + b) = 1$.
A separating hyperplane in canonical form must satisfy the following constraints ,

$$y_i[(w.x_i) + b] \geq 1, i = 1, ...l \tag{3.5}$$

The distance of a point x from the hyperplane is,

$$d(w, b, x) = \frac{|w.x + b|}{\|w\|} \tag{3.6}$$

The margin is $\frac{2}{\|w\|}$ according to its definition. Hence the hyperplane that optimally separates the data is the one that minimizes

$$\Phi(w) = \frac{1}{2}\|w\|^2 \tag{3.7}$$

The solution to the optimization problem of (3.7) under the constraints of (3.5) is given by the saddle point of the Lagrange functional,

$$L(w, b, \alpha) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{l} \alpha_i \{y_i[(w.x_i) + b] - 1\} \tag{3.8}$$

ROI extraction technique

The prime objective of any **ROI** extraction technique is to segment same region of interest consistently from all images. The central knuckle point can be used to segment any finger-knuckle-print consistently. Since finger-knuckle-print is aligned horizontally, one can now easily extract the central region of interest from any finger-knuckle-print that contains rich and discriminative texture using this point. The proposed ROI extraction algorithm performs in three steps; detection of knuckle area, central knuckle-line and central knuckle-point [47].

3.5 Conclusion

In this section, we gave an overview of a new deep learning method, which based by descriptor of the texture, it is Discrete Cosine Transform Network (DCTNet) and SVM classifier.

CHAPTER FOUR

CHAPTER 4

Experimental results and discussions

4.1 Introduction

One new biometric trait that has attracted researchers in the recent years is the Finger Knuckle Print (FKP). The FKP refers to the inherent skin patterns that are formed at the joints in the finger back surface. Recently it has been found that the finger knuckle print is highly rich in textures and can be used to uniquely identify a person. Hand based biometrics have the advantage of higher user acceptability and this new trait has an added advantage of not getting easily damaged, it is permanent and stable. However, the hand contains many fingers, so many of the works show that FKP can be used to identify people for strong and precise identification, if we use the combination or incorporate the information taken from each finger. In this chapter, we applied DCTNet and SVM classifier to our database in the unimodal case (Left Index Finger (LIF), Left Middle Finger (LMF), Right Index Finger (RIF), Right Middle Finger (RMF)) and in the multimodal case such as (LIF+LMF, RIF+RMF...) by fusion at the score level and compared the results to present the best.

4.2 Experimental database

Finger-Knuckle-Print is one of the emerging biometric traits. The region of interest is the area where the maximum information is centered, an outer surface of a finger has three knuckles: a distal interphalangeal (DIP) joint, a proximal interphalangeal (PIP) joint, and a metacarpophalangeal (MCP) joint as shown in (Figure 4.1). Kumar et al.[37] categorized three finger joints into major and minor finger knuckles, where a DIP joint is a first minor finger knuckle, a PIP joint is a major finger knuckle, and an MCP joint is a second minor finger knuckle. It is easy to capture such patterns on a finger knuckle by a camera. In this work, we used the finger knuckles of a PIP joint.

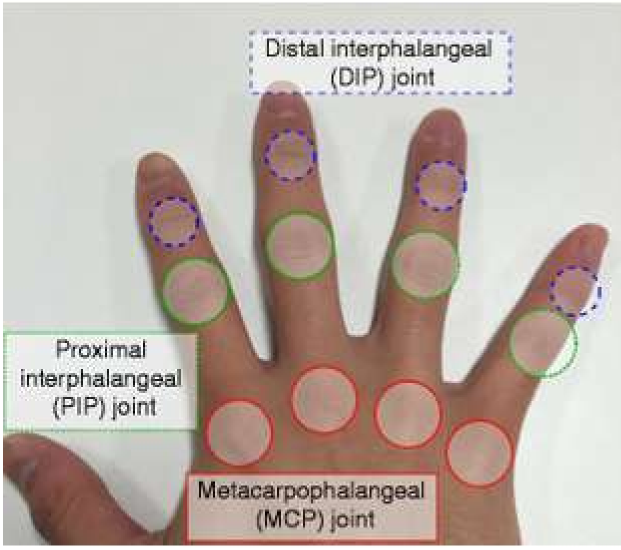

Figure 4.1: A taxonomy of finger knuckle joints: Blue-colored circles indicate distal interphalangeal (DIP) joints, green-colored circles indicate proximal interphalangeal (PIP) joints, and red-colored circles indicate metacarpophalangeal (MCP) joints.

The database of this experiment is separating to two principal parts: the first part is *Training images* (the first, fifth and ninth image) of each person to serve enrollment phase, the second part is *Tests Images* (The remaining nine images) of each individual have helped us achieving different tests. We experimented our approach on Hong Kong polytechnic university (PolyU) Finger-Knuckle-Print Database [38]. The database has 7920 images obtained from 165 persons. This database including 125 males and 40 females. Among them, 143 subjects are 20-30 years old and the others are 30-50 years old. These images are collected in two separate sessions. In each session, the subject was asked to provide 6 images for each of LIF, LMF, RIF and RMF. Therefore, 48 images from 4 fingers were collected from each subject.

4.3 Experimental protocol

In order to achieve the best and ideal results by this study using the new DCTNet algorithm, we put this experimentation plan into practice:

First step: we choose the best parameter of DCTNet feature extraction algorithm after we study the influence of the DCTNet parameter in the identification rate of our biometric system. Moreover, this is the important step.

Second step: DCTNet algorithm is among the best current texture descriptors. For this, we used it to extracting the features of finger knuckle print. To see which one is the best finger that gives powerful results, we conducted several experiments.

Third step: a single feature sometimes fails to be exact enough to identification. So for increased the performance of the identification system, we have merged the different finger knuckle print samples. This achieves much greater accuracy than single-feature systems.

4.4 Proposed system

Biometric system identification is based on two phases, an enrollment phase and an identification phase. It consists of pre-processing process, matching process, normalization and decision process. In this experiment we proposed two biometric systems (unimodal and multimodal) based on multi-sample finger knuckle print images, for the purpose of increasing the performance of the biometric system and enhancing security and confidence in security biometric systems. From feature extraction we use the deep learning DCTNet which the characteristics of an FKP image are effectively and clearly demonstrated by DCTNet, where a different representation can be displayed for several levels to give high-level properties and using support vector machine (SVM) for classification, we propose to fuse different samples of FKP features. It is composed of two biometric subsystems. Each subsystem exploits different biometric techniques that are (LIF, LMF, RIF, RMF) modalities. The schematic diagram of the proposed system using FKP images is in below figure (Figure 4.2).

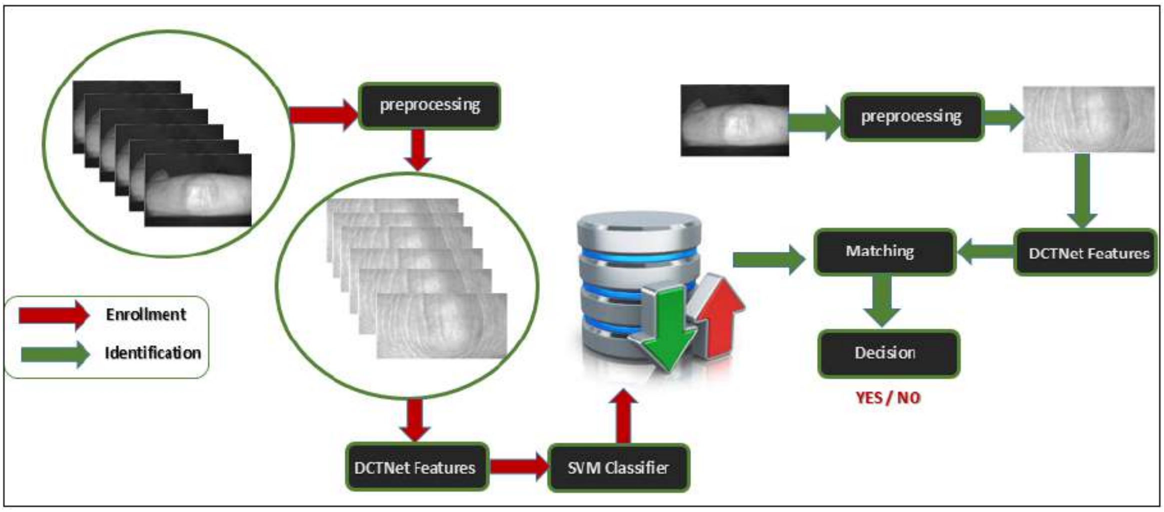

Figure 4.2: Multimodal finger knuckle print identification system

4.5 Experimental results

4.5.1 DCTNet parameter adaptation

Feature based approach DCTNet method is employed for FKP identification. This method can capture the information from the texture in an image and provide a very high robustness, which is efficiency describes the image characteristics. DCTNet has important parameter (the number of layers, number of filters in each layer, filter size and block wise histogram size). Improvement the performance is the main objective of this study for that, we select the optimal parameter for DCTNet.

1. the number of layer: After applying the various experiences and probabilities of the DCTNet algorithm, which relates to the breakthrough texture, to reach satisfactory and practical results in fact, we find that one layer is not enough to extract information. On the other hand, the use of 3 or 4 layers leads to the need to use special equipment is often expensive and it makes a calculation problem. Moreover, it deforms the image and take longer. Unlike when the phase number is equal to two, we get good results for the specifications of the current text descriptors (Figure 4.3 and Figure.4.4).

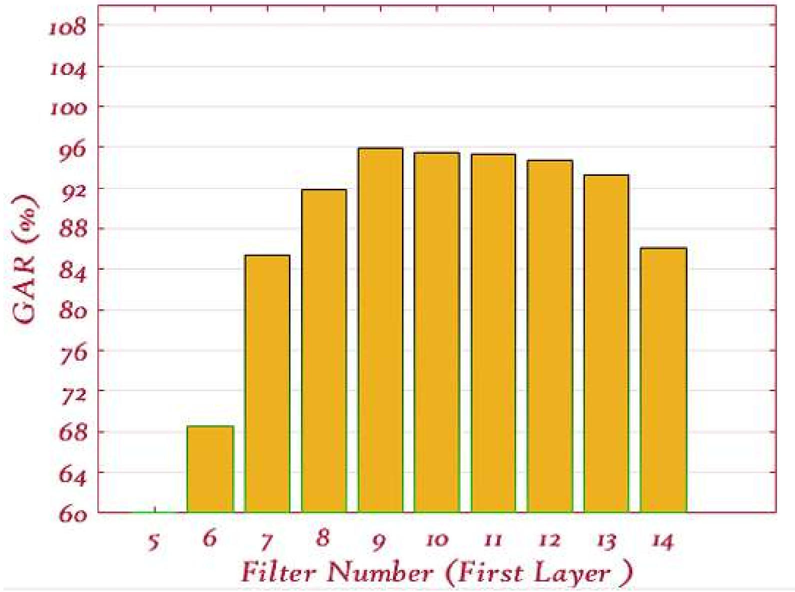

Figure 4.3: DCTNet parameter adaptation a) GAR against Filter number in first layer

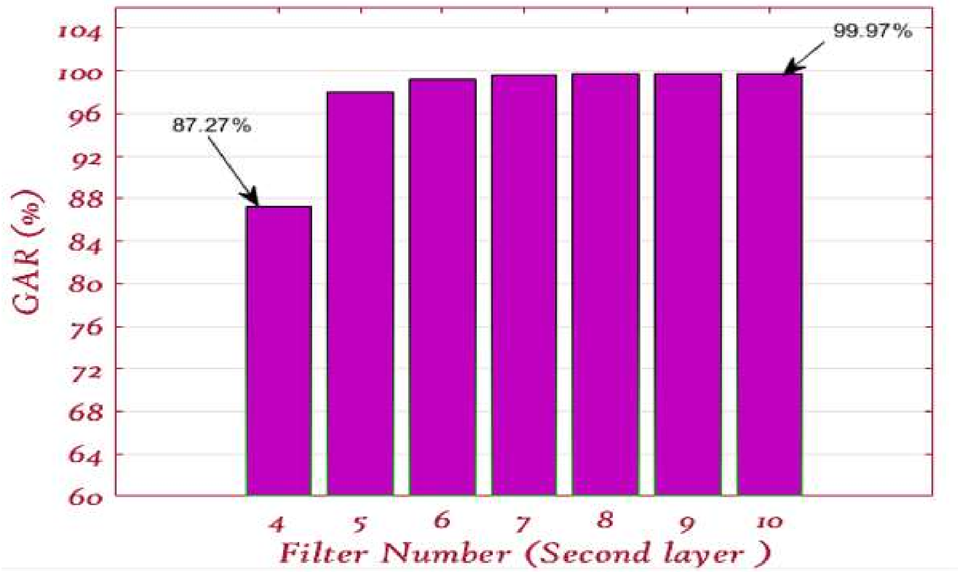

Figure 4.4: DCTNet parameter adaptation b) GAR against Filter number in second layer

2. number of filter in each layer : We conclude from this stage, the influence of filters number is great in the biometric system performance, because the filters number is essential for the DCTNet algorithm.

We note the accuracy of the identification becomes very high in the number of filters 9 to 14, it gives the best result GAR = 95.42% when the number of filter equal 10. After that, we fixed the number of filters in first layer in 10 and we change the number of filters in second layer. We note that all filters give better results when they give the identification rate higher than 99.50%, but the perfect given by number of filter equal 11.

Note: We found the best result in case [14-10] with GAR=99.93%, ERR=0%, and [15-10] with GAR=100%, ERR=0%. But that take more time and we use more filters on our database. For that, we choose the number of layer equal to two and the number of filters in each layer is [10 - 11], it gives the result GAR = 99.86% and we will make this result better in next step.

3. filter size and block wise histogram size : Now, we will see the impact of the filter size and the block wise histogram size in the identification rate of identification system.
We note as a general remark the filter size must be an odd number, the best results given when the filter size less than [9 - 9] but from the filter size larger to [9 - 9] we see a decline in the identification rate less than 98.10%. In this case, the perfect result given when the filter size equal [5 - 5] it gives GAR =99.52% (Figure 4.4,Figure 4.5).
We note as a general remark the block wise histogram size must be pair number, all the values give a best result > 99.52% and the perfect is 99.86% from the block wise histogram size equal [10 - 10].
Our results have been taken with using WPCA for dimension reduction, which we choose the size of the vector equals to 300. That gives a good results such as the size of the vector equals 400 or 500, but it takes more time and equipment than we have. So our choose was 300 because it is fast by contribution the other and we achieved a better result. In addition, we use SVM classifier because it is a technical classification (similarity), based on using kernel core functions that allow optimal separation of the points of the plan.

At the end, and after the comparison of the previous results, we conclude the best parameters of DCTNet Algorithm are:

The number of layers = 2.
The number of filters in the layers = [10 11].
The filter size = [5 5] .

The block-Wise histogram size = [10 10].

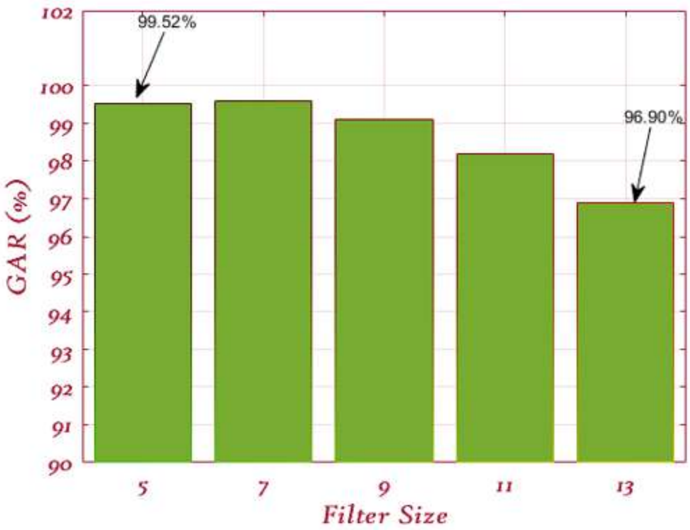

FIGURE 4.5. DCTNet parameter adaptation a) GAR against Filter size.

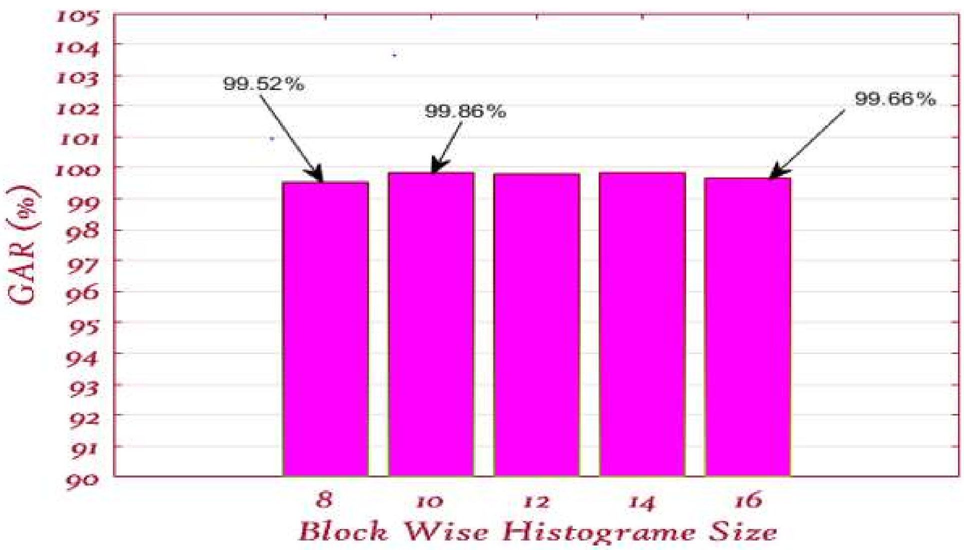

FIGURE 4.6. DCTNet parameter adaptation b) GAR against block wise histogram size.

4.5.2 Unimodal identification system results

Open set: Using DCTNet extraction for different fingers. Experimental results indicate that RIF performance is better than LIF, LMF, and RMF in terms of EER. This is illustrated in (Table 4.1) and(Figure 4.8 and Figure 4.7) for the performance of the unimodal system given EER = 0, 00% and T0 = 0, 8310. In the general case, the rest of the fingers give the best result when EER gives less than 0, 0673%.

Closed set: The perfect is RIF, because it gives the ideal value 100% than other fingers (LIF, LMF, RMF), they give the same best result when they give the identification rate 99:86%. These results are shown in the CMC curve (the identification rate against the rank) of closed set identification system (Figure 4.6). From the RPR, RIF and LIF and LMF give best results when it gives 1, 3, 14 respectively and RMF gives a very far value estimated at 104.

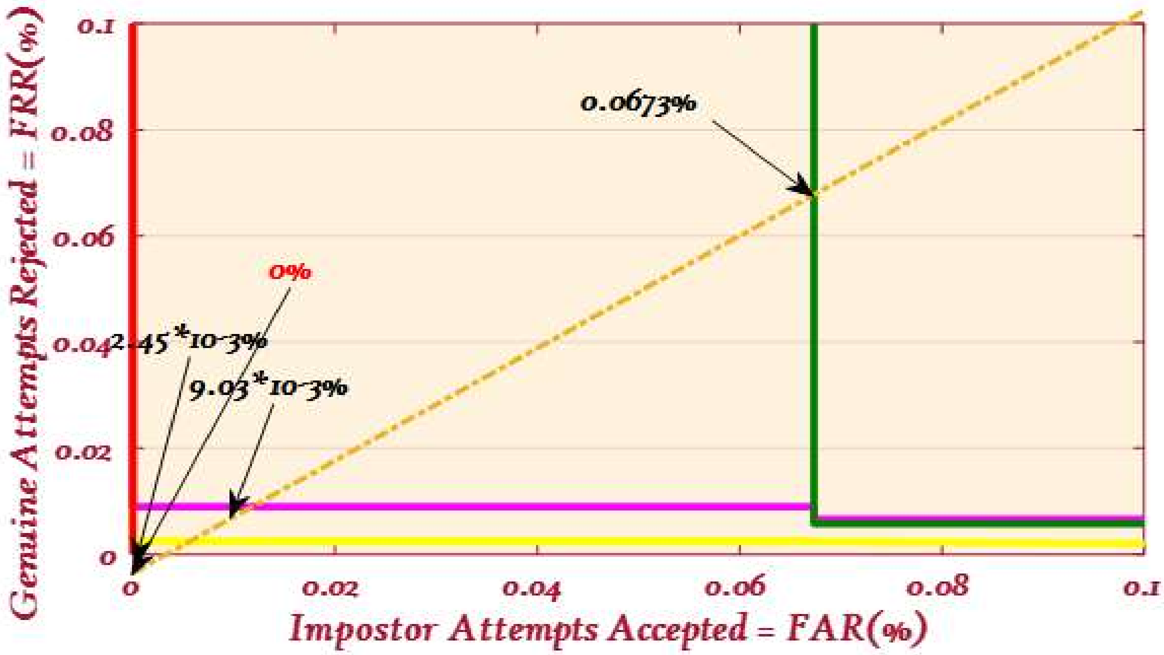

FIGURE 4.7. Unimodal system results curves 1) ROC curves.

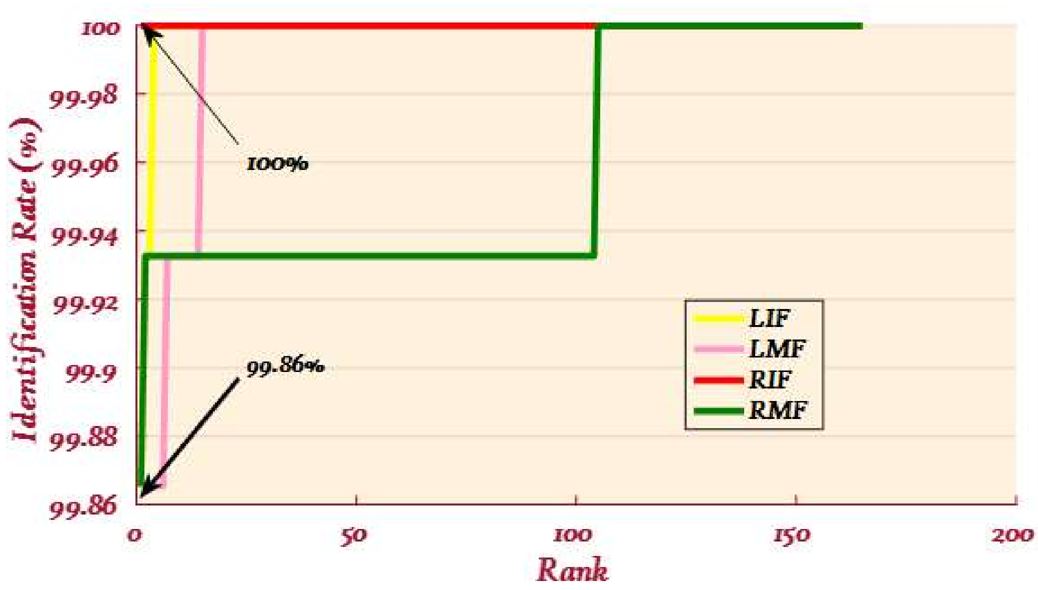

FIGURE 4.8. Unimodal system results curves 2) CMC curves.

The_performance of unimodal system					
Poly U Data Base	Types	DCTNet Features			
		Open set		Closed set	
		ERR	Th	ROR	RPR
165 Persons	LIF	$2.46 * 10^{-3}$%	0.8851	99.86%	03
	LMF	$9.03 * 10^{-3}$%	0.7444	99.86%	14
	RIF	0%	0.8310	100%	01
	RMF	0.0673%	0.6712	99.86%	104

Table 4.1: The performance of unimodal system using DCTNet extraction.

4.5.3 Multimodal identification system results

The purpose of multimodality is to improve the level of security of the system such that the identification rate of the merged biometric terms is greater than the maximum of the identification rates of the modalities taken separately. So, using the different modalities (four modalities: four fingers for FKP) we realize a system at the end based on the fusion between the two fingers.

In our work, the fusion at the score level is used because it is the most common approach used, it given the best results and it is simple for merged scores generated by different subsystems. (Table 4.2) and (Figure 4.8 and Figure 4.9) show the performance of the multimodal identification system.

The results indicate in open set identification all the fusion methods give a better result EER equal 0.00%, and the same in closed set identification all fusion methods give a better identification rate 100% in first rank.

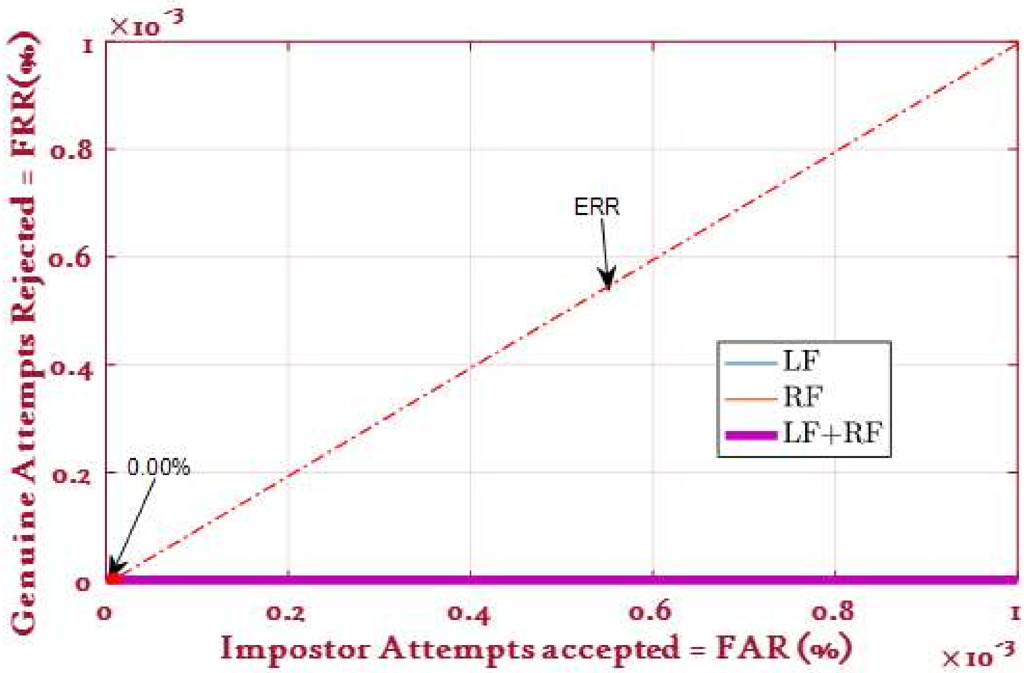

FIGURE 4.9. Multimodal system results a) ROC curves.

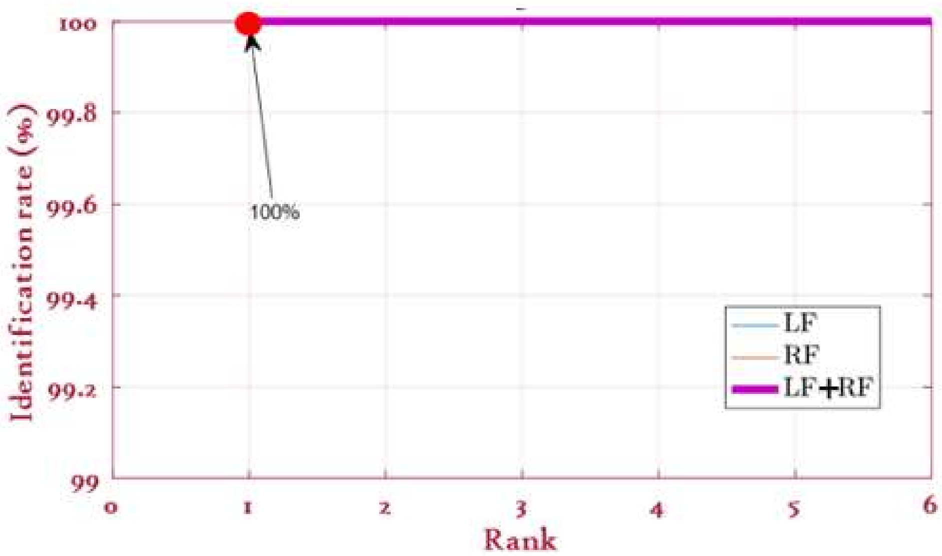

FIGURE 4.10. Multimodal system results b) CMC curves.

The performance of Multimodal system						
Poly U Data Base		DCTNet Features				
		Open set		Closed set		
	Fusion Types	ERR	Th	ROR	RPR	
165 Persons	LIF+LMF	0.00%	0.654	100%	01	
	RIF+RMF	0.00%	0.753	100%	01	
	RF+LF	0.00%	0.417	100%	01	

Table 4.2: The performance of multimodal system using DCTNet extraction.

By using different fusion rules on the performance of the multimodal system when our choose is LF (LIF, LMF) and with other case (RMF, LMF, LIF), the (Figure 4.10 and Figure 4.11) and (Table 4.3) or the (Figure4.12 and Figure 4.13) and (Table.4.4) show the performance of the multimodal identification system.

Where μ and σ are the mean and standard deviation of the distribution of S, either known or estimated from the data.
The Z-score normalization is sensitive to outliers, but comparatively lesser than the earlier two methods. Note that Z-score normalization may not be optimal if the actual underlying score distribution is not Gaussian [22].

2.8.4 Median and median absolute deviation (MAD)

Has been proposed as an alternative to Z-score normalization. In this method, the normalized score . In this method, the normalized score$S_k^{'}$ is computed as

$$S_k^{'} = \frac{S_k - median(S)}{MAD} \tag{2.4}$$

Where $MAD = median(|S_k - median(s)|)$.

This method of normalization is not sensitive to outliers but performs worse than Z-score normalization when the underlying distribution is not Gaussian.
Both the Z-score and the median and MAD normalization schemes do not return normalized scores in a pre-determined bounded interval.
Non-linear normalization techniques that use tunable parameters have also been proposed. These include double sigmoid [23] and tanh [24] normalization.

2.8.5 The double sigmoid function

Has three tunable parameters t , r_1 and r_2, where r_1 and r_2 denote the region around operating point t where normalization is approximately linear. The normalized score $S_k^{'}$ is computed as follows

$$S_k^{'} = \begin{cases} \frac{1}{1+exp\left(-2(S_k - \frac{t}{r_1})\right)}, & s_k < t \\ \frac{1}{1+exp\left(-2(S_k - \frac{t}{r_2})\right)}, & \text{othewise} \end{cases} \tag{2.5}$$

This normalization is especially useful in amplifying the difference in the region of overlap between genuine and impostor scores $(t - r_1, t + r_2)$.

2.8.6 Tanh normalization

Is robust and is insensitive to outliers. The normalized scores may be computed as

$$S_k^{'} = \frac{1}{2}\left(\tanh\left(\alpha\left(\frac{s_k - \mu_H}{\sigma_H}\right)\right) + 1\right) \tag{2.6}$$

2.9 Fusion methods

Once the scores from different matchers have been transformed to a common domain, they are fused together using a fusion rule, such as one of the following [25]. These fusion rules work best when the scores obtained from different matchers are independent.

2.9.1 The weighted sum rule

Finds the weighted arithmetic [26] mean of the normalized matching scores obtained from different classifiers.

$$score^{(j)} = \sum_i W_i^{(j)} S_i^{(j)} \tag{2.7}$$

Where $score^{(j)}$ is the final score after fusion for the jth subject and $W_i^{(j)}$ and $S_i^{(j)}$ are the weights and normalized scores respectively for the ith matcher and the jth subject. The weights corresponding to different matchers may be subject specific, Note that the weighted average is subject to the condition $\Sigma W_i^{(j)} \stackrel{\text{def}}{=} 1 \forall ji$

2.9.2 The weighted product rule

Finds the weighted geometric [27] mean of the normalized matching scores.

$$score^{(j)} = \left(\prod_i W_i^{(j)} S_i^{(j)}\right)^{\frac{1}{\Sigma W_i^{(j)}}} \tag{2.8}$$

2.9.3 The median rule

Is a robust alternative for the sum rule, because the arithmetic mean is sensitive to outliers.

$$score^{(j)} = median(S_i^{(j)}) \tag{2.9}$$

2.9.4 The max rule

Chooses the normalized score from the matcher that presents the greatest degree of confidence.

$$score^{(j)} = \max(S_i^{(j)}) \tag{2.10}$$

2.9.5 The min rule

Chooses the normalized score from the matcher that presents the least degree of confidence.

$$score^{(j)} = \min(S_i^{(j)}) \tag{2.11}$$

2.10 Conclusion

Multimodal biometric systems have better accuracy and reliability due to the use of multiple biometric traits to authenticate a claimed identity or perform identification. For this, we exposed the advantage of a multimodal biometric, the different forms of the multi-modality, the different scenarios and fusion levels. All that after some unimodal biometrics limitations.

CHAPTER THREE

CHAPTER THREE

CHAPTER 3

Feature Extraction

3.1 Introduction

The image is a set of different information, so that each image has specific characteristics that create a difference between each image about other, this feature used in the recognition system, because it is special property and stable with time.

3.2 Feature Extraction

An image defined in the ”real world”is considered to be a function of two real variables, for example, a(x, y) with a as the amplitude (e.g. brightness) of the image at the real coordinate position (x, y). An image may be considered to contain sub-images sometimes referred to as regions-of-interest, ROIs, or simply regions.
A feature is defined as an ”interesting” part of an image, and is used as a starting point in main primitives for subsequent algorithms .Over the last decades, image feature detectors and descriptors have become popular tools in the computer vision community and they are being applied widely in a large number of applications ,e.g. Image representation [28], object recognition and matching [29,30].

The various features classified and currently employed are:

a) General features: Independent features such as color, texture, and shape according to the abstraction level, they can be further divided into:

- **Pixel-level features:** Features calculated at each pixel, e.g. color, location.
- **Local features:** Features calculated over the results of subdivision of the image band of an image segmentation or edge detection (Thawar Arif, et al., 2009).
- **Global features:** Features calculated over the entire image or just regular sub-area of an image.

b) Domain-specific features : Application of dependent features such as human faces, fingerprints and conceptual ones.

However, the choice of feature extraction method is based on three essential categories, namely the line, the appearance and the texture. The majority of work shows that the most distinctive information, it is in the texture analysis, for that we chose a deep learning DCTNet algorithm and SVM classifier.

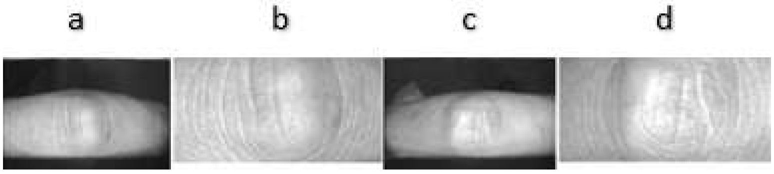

Figure 3.1: (a) and (c) are two FKP images; (b) and (d) are the ROI images of (a) and (c).

3.3 DCTNet Deep Learning

Recently, deep convolutional network shows its success in various image classification tasks has drawn significant attention. Many researchers have focused on deep learning because of its ability for automatically learning good representations of the underlying distribution of the data and learn abstract representation of the data build up in multiple stages.in order to learn good features, the networks usually have multi-layer and many hidden units which lead to extremely high training time costs.

DCT has been successfully used in computational intelligence as both a function approximation method [31] and a network compression method [32].In this study, we develop a biometric system for FKP recognition. The system is based on using the two-dimensional $(2-D)$ Discrete Cosine Transform (DCT) to obtain distinctive features from an FKP image. The choice of 2D DCT basis as filter bank is inspired by the Karhunen Loeve Transform (KLT) in transform coding literature, which is also known as Principal Component Analysis (PCA) in multivariate statistics community.

DCTNet [33] is an alternative to PCANet, which employs Discrete Cosine Transform (DCT) as filter banks instead of PCA. As well known, PCANet is data-dependence hence inflexible. In DCTNet, on the other hand, the filter banks created by DCT achieve a data-independent network, increasing the performance of the network. In order to decrease the computational complexity of the learning stages of the network, 2D DCT is also employed. Besides the low computational complexity, 2D DCT filter banks are independent from data, therefore, generating a learning-free framework. The main idea of the approach is instead of learning the set of filters at each layer of deep networks, Inspired by the scattering transform and PCANet, DCTNet was proposed in [33, 34, 35]. DCTNet uses a prefix cosine function as filter; this is an approximation of the eigenfunction used in PCANet. It performs multilayer short time Discrete Cosine Transform (DCT).
Classification of the FKP image is then achieved by applying a standard linear SVM classifier to the coefficients (features) extracted from the DCT (frequency) matrix. This shows that the modified DCTNet is a simple flexible and effective feature extractor for FKP image processing.
DCTNet structure is an extra layer at the histogram output for histogram normalization as shown in (Figure 3.2.)

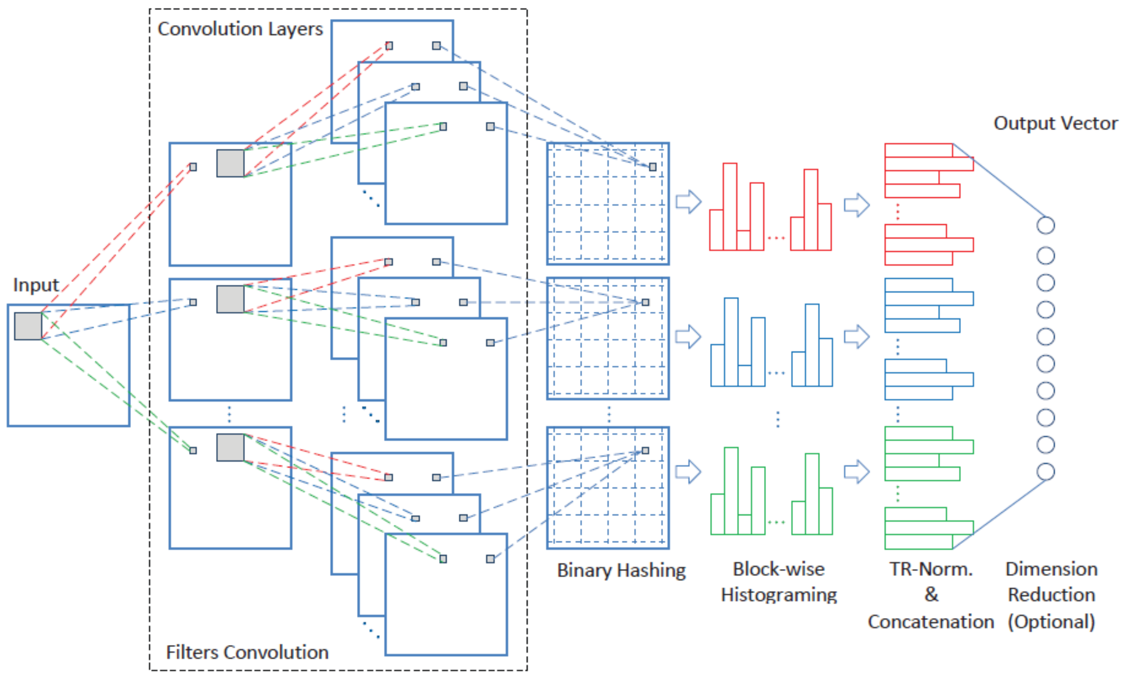

Figure 3.2: The block diagram of the proposed DCTNet Source [33] .

The following are the main elements of the DCT Net structure:

A. Convolution Layer: The output of input image Id of size nm with D channels given by

$$O_d^p = \left\{ I_d * W_l^p \right\}_p^{p_l} \tag{3.1}$$

Where $(*)$ denotes the discrete convolution and the size of output O_d^p is same as I_d and $W_l^p \in \Re^{k*k}$,$p = 1,2,...,p_l$ is 2D-DCT bases from p_l filters at layer l.

B. Binarization and Block-wise Histograming:

The outputs of convolution layer of DCTNet give real values. In this step, the output obtained in the last layer is turned into binary format with the comparison of responses with threshold to zero (value 1 for positive response, zero otherwise) denoted by BIN .

$$BIN(O_d^p) = \begin{cases} 1 \longrightarrow O_d^p \geq 0 \\ 0 \longrightarrow othewise \end{cases} \tag{3.2}$$

C. Histogram Tied Rank Normalization (TR Normalization):

Each of these binary images is divided into B non-overlapping blocks. The characteristics of these images are obtained by concatenating all the histograms of each block B such as

$$H = \left\{ O_b^d \right\}_{b=1,d=1}^{B,D} \tag{3.3}$$

Where $b = 1,2,...,B$, $d = 1,2,...,D$ The combination of binary hashing and block-wise histograms should be able to extract discriminating characteristics.

3.4 Support Vector Machine Classification

Support vector machines (SVM) is a form of supervised machine learning model. By learning from provided examples -the training data- the model finds a function that couples input data to the correct output. The output for novel data can then be predicted by applying the retrieved function. SVM is often used for classification problems for which the correct output is the class the data belongs to. The model works by creating a

hyperplane that separates data points from one class from those from the other class, with a margin as high as possible. The margin is the maximal width of the slab parallel to the hyperplane that has no interior data points.
The support vectors, which give the model its name are the data points closest to the hyperplane and therefore determine the margin.

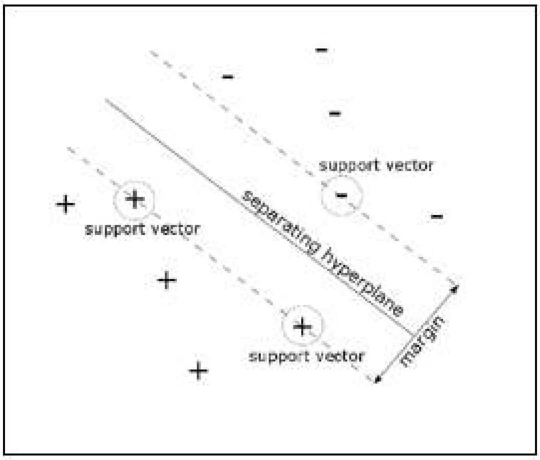

Figure 3.3: Illustration of the hyperplane separating data points from two classes shown as + and -. The support vectors and the margin are marked.

1. Multiclass SVM

A support vector machine is a technique of discrimination, it is a supervised learning method for classification and regression. It consists in separating two or more sets of points by a hyperplane. Depending on circumstances and configuration points. The original idea of SVM is based on using kernel core functions that allow optimal separation of the points of the plan in different categories. The method uses a set of training data. Which enables a hyperplane separating the best points. In this paper, we use the multi class SVM [36].

2. Normalization method

Score normalization is needed to transform these scores into a common domain, prior to combining them. Thus, a Min-Max normalization scheme was employed. To transform the scores computed into similarity scores in the same range. Thus,

$$\tilde{D} = \frac{D - min(D)}{max(D) - min(D)} \tag{3.4}$$

Where $\tilde{D}$ represent the normalized vector. However, these scores are compared, and the lowest score is selected. For perfect matching, the matching score is zero.

Consider the problem of separating the set of training vectors belong to two separate classes, $(x1, y1)...(xl, yl)$,where $xi \in R^n$,$yi \in -1, +1$ with a hyperplan $wx + b = 0$. The set of vectors is said to be optimally separated by the hyperplane if it is separated without error and the margin is maximal.A canonical hyperplane has the constraint for parameter $w, b : min_{xi} yi(w.xi + b) = 1$.
A separating hyperplane in canonical form must satisfy the following constraints ,

$$y_i[(w.x_i) + b] \geq 1, i = 1, ...l \tag{3.5}$$

The distance of a point x from the hyperplane is,

$$d(w, b, x) = \frac{|w.x + b|}{\|w\|} \tag{3.6}$$

The margin is $\frac{2}{\|w\|}$ according to its definition. Hence the hyperplane that optimally separates the data is the one that minimizes

$$\Phi(w) = \frac{1}{2}\|w\|^2 \tag{3.7}$$

The solution to the optimization problem of (3.7) under the constraints of (3.5) is given by the saddle point of the Lagrange functional,

$$L(w, b, \alpha) = \frac{1}{2}\|w\|^2 - \sum_{i=1}^{l} \alpha_i \{y_i[(w.x_i) + b] - 1\} \tag{3.8}$$

ROI extraction technique

The prime objective of any **ROI** extraction technique is to segment same region of interest consistently from all images. The central knuckle point can be used to segment any finger-knuckle-print consistently. Since finger-knuckle-print is aligned horizontally, one can now easily extract the central region of interest from any finger-knuckle-print that contains rich and discriminative texture using this point. The proposed ROI extraction algorithm performs in three steps; detection of knuckle area, central knuckle-line and central knuckle-point [47].

3.5 Conclusion

In this section, we gave an overview of a new deep learning method, which based by descriptor of the texture, it is Discrete Cosine Transform Network (DCTNet) and SVM classifier.

CHAPTER FOUR

Chapter 4

Experimental results and discussions

4.1 Introduction

One new biometric trait that has attracted researchers in the recent years is the Finger Knuckle Print (FKP). The FKP refers to the inherent skin patterns that are formed at the joints in the finger back surface. Recently it has been found that the finger knuckle print is highly rich in textures and can be used to uniquely identify a person. Hand based biometrics have the advantage of higher user acceptability and this new trait has an added advantage of not getting easily damaged, it is permanent and stable. However, the hand contains many fingers, so many of the works show that FKP can be used to identify people for strong and precise identification, if we use the combination or incorporate the information taken from each finger. In this chapter, we applied DCTNet and SVM classifier to our database in the unimodal case (Left Index Finger (LIF), Left Middle Finger (LMF), Right Index Finger (RIF), Right Middle Finger (RMF)) and in the multimodal case such as (LIF+LMF, RIF+RMF...) by fusion at the score level and compared the results to present the best.

4.2 Experimental database

Finger-Knuckle-Print is one of the emerging biometric traits. The region of interest is the area where the maximum information is centered, an outer surface of a finger has three knuckles: a distal interphalangeal (DIP) joint, a proximal interphalangeal (PIP) joint, and a metacarpophalangeal (MCP) joint as shown in (Figure 4.1). Kumar et al.[37] categorized three finger joints into major and minor finger knuckles, where a DIP joint is a first minor finger knuckle, a PIP joint is a major finger knuckle, and an MCP joint is a second minor finger knuckle. It is easy to capture such patterns on a finger knuckle by a camera. In this work, we used the finger knuckles of a PIP joint.

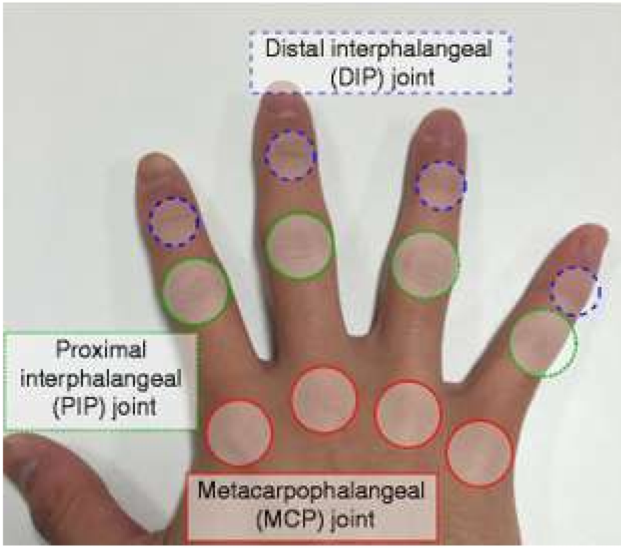

Figure 4.1: A taxonomy of finger knuckle joints: Blue-colored circles indicate distal interphalangeal (DIP) joints, green-colored circles indicate proximal interphalangeal (PIP) joints, and red-colored circles indicate metacarpophalangeal (MCP) joints.

The database of this experiment is separating to two principal parts: the first part is *Training images* (the first, fifth and ninth image) of each person to serve enrollment phase, the second part is *Tests Images* (The remaining nine images) of each individual have helped us achieving different tests. We experimented our approach on Hong Kong polytechnic university (PolyU) Finger-Knuckle-Print Database [38]. The database has 7920 images obtained from 165 persons. This database including 125 males and 40 females. Among them, 143 subjects are 20-30 years old and the others are 30-50 years old. These images are collected in two separate sessions. In each session, the subject was asked to provide 6 images for each of LIF, LMF, RIF and RMF. Therefore, 48 images from 4 fingers were collected from each subject.

4.3 Experimental protocol

In order to achieve the best and ideal results by this study using the new DCTNet algorithm, we put this experimentation plan into practice:

First step: we choose the best parameter of DCTNet feature extraction algorithm after we study the influence of the DCTNet parameter in the identification rate of our biometric system. Moreover, this is the important step.

Second step: DCTNet algorithm is among the best current texture descriptors. For this, we used it to extracting the features of finger knuckle print. To see which one is the best finger that gives powerful results, we conducted several experiments.

Third step: a single feature sometimes fails to be exact enough to identification. So for increased the performance of the identification system, we have merged the different finger knuckle print samples. This achieves much greater accuracy than single-feature systems.

4.4 Proposed system

Biometric system identification is based on two phases, an enrollment phase and an identification phase. It consists of pre-processing process, matching process, normalization and decision process. In this experiment we proposed two biometric systems (unimodal and multimodal) based on multi-sample finger knuckle print images, for the purpose of increasing the performance of the biometric system and enhancing security and confidence in security biometric systems. From feature extraction we use the deep learning DCTNet which the characteristics of an FKP image are effectively and clearly demonstrated by DCTNet, where a different representation can be displayed for several levels to give high-level properties and using support vector machine (SVM) for classification, we propose to fuse different samples of FKP features. It is composed of two biometric subsystems. Each subsystem exploits different biometric techniques that are (LIF, LMF, RIF, RMF) modalities. The schematic diagram of the proposed system using FKP images is in below figure (Figure 4.2).

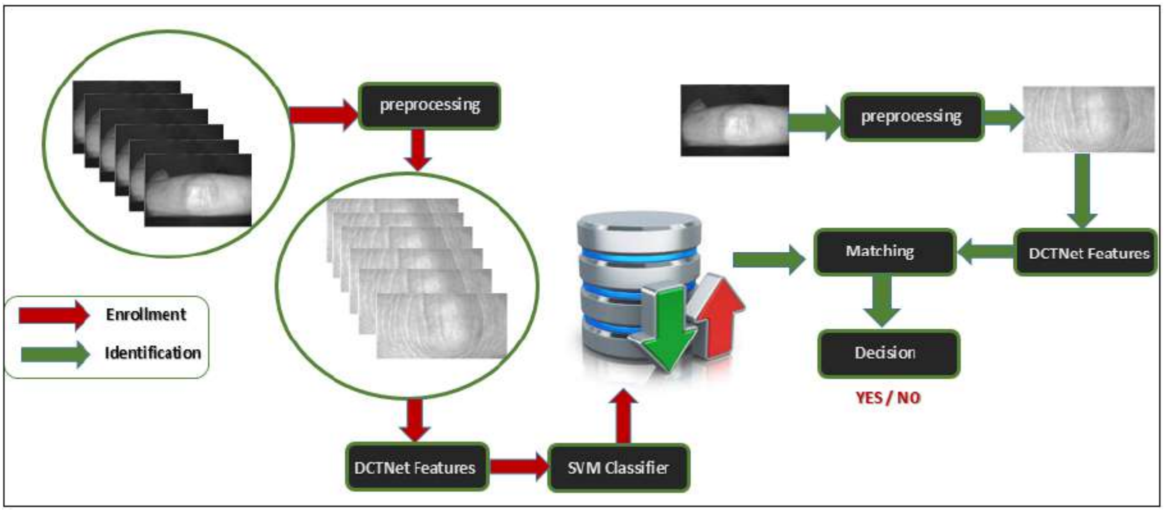

Figure 4.2: Multimodal finger knuckle print identification system

4.5 Experimental results

4.5.1 DCTNet parameter adaptation

Feature based approach DCTNet method is employed for FKP identification. This method can capture the information from the texture in an image and provide a very high robustness, which is efficiency describes the image characteristics. DCTNet has important parameter (the number of layers, number of filters in each layer, filter size and block wise histogram size). Improvement the performance is the main objective of this study for that, we select the optimal parameter for DCTNet.

1. the number of layer: After applying the various experiences and probabilities of the DCTNet algorithm, which relates to the breakthrough texture, to reach satisfactory and practical results in fact, we find that one layer is not enough to extract information. On the other hand, the use of 3 or 4 layers leads to the need to use special equipment is often expensive and it makes a calculation problem. Moreover, it deforms the image and take longer. Unlike when the phase number is equal to two, we get good results for the specifications of the current text descriptors (Figure 4.3 and Figure.4.4).

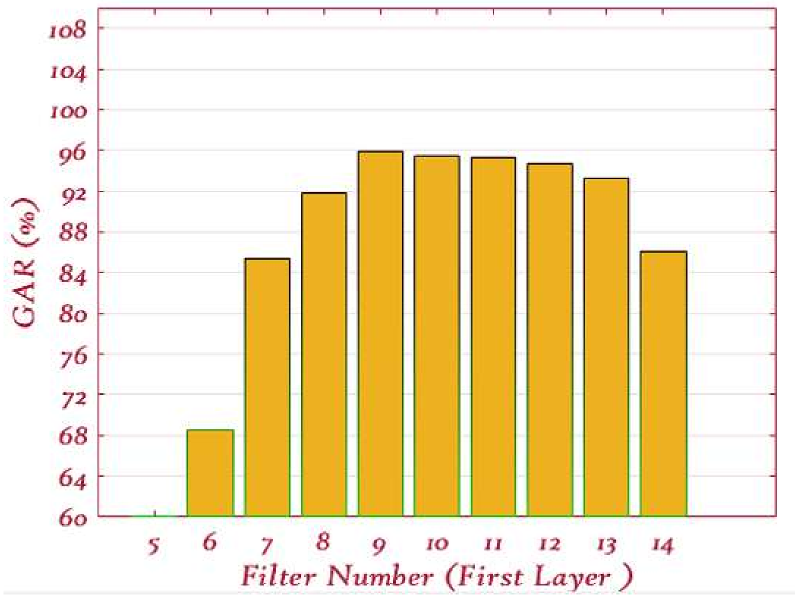

Figure 4.3: DCTNet parameter adaptation a) GAR against Filter number in first layer

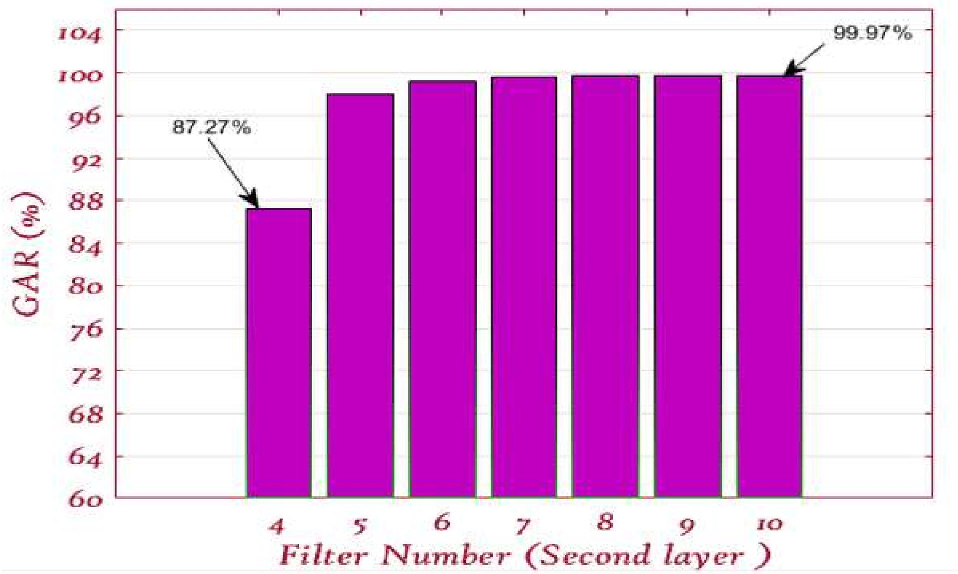

Figure 4.4: DCTNet parameter adaptation b) GAR against Filter number in second layer

2. number of filter in each layer : We conclude from this stage, the influence of filters number is great in the biometric system performance, because the filters number is essential for the DCTNet algorithm.

We note the accuracy of the identification becomes very high in the number of filters 9 to 14, it gives the best result GAR = 95.42% when the number of filter equal 10. After that, we fixed the number of filters in first layer in 10 and we change the number of filters in second layer. We note that all filters give better results when they give the identification rate higher than 99.50%, but the perfect given by number of filter equal 11.

Note: We found the best result in case [14-10] with GAR=99.93%, ERR=0%, and [15-10] with GAR=100%, ERR=0%. But that take more time and we use more filters on our database. For that, we choose the number of layer equal to two and the number of filters in each layer is [10 - 11], it gives the result GAR = 99.86% and we will make this result better in next step.

3. filter size and block wise histogram size : Now, we will see the impact of the filter size and the block wise histogram size in the identification rate of identification system.
We note as a general remark the filter size must be an odd number, the best results given when the filter size less than [9 - 9] but from the filter size larger to [9 - 9] we see a decline in the identification rate less than 98.10%. In this case, the perfect result given when the filter size equal [5 - 5] it gives GAR =99.52% (Figure 4.4,Figure 4.5).
We note as a general remark the block wise histogram size must be pair number, all the values give a best result > 99.52% and the perfect is 99.86% from the block wise histogram size equal [10 - 10].
Our results have been taken with using WPCA for dimension reduction, which we choose the size of the vector equals to 300. That gives a good results such as the size of the vector equals 400 or 500, but it takes more time and equipment than we have. So our choose was 300 because it is fast by contribution the other and we achieved a better result. In addition, we use SVM classifier because it is a technical classification (similarity), based on using kernel core functions that allow optimal separation of the points of the plan.

At the end, and after the comparison of the previous results, we conclude the best parameters of DCTNet Algorithm are:

The number of layers = 2.
The number of filters in the layers = [10 11].
The filter size = [5 5] .

The block-Wise histogram size = [10 10].

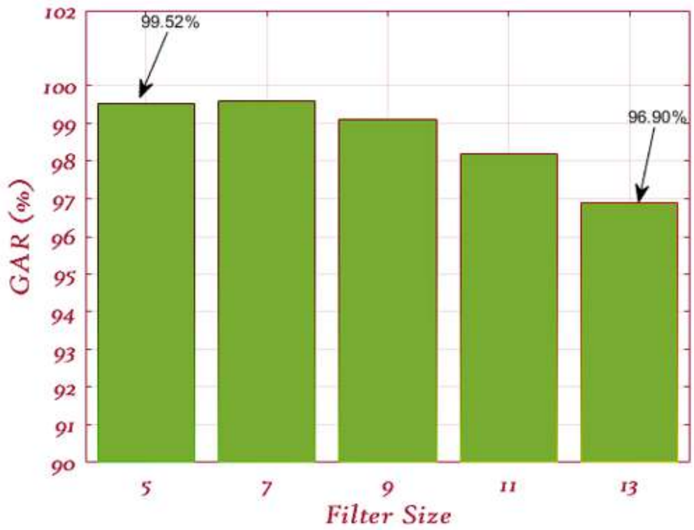

FIGURE 4.5. DCTNet parameter adaptation a) GAR against Filter size.

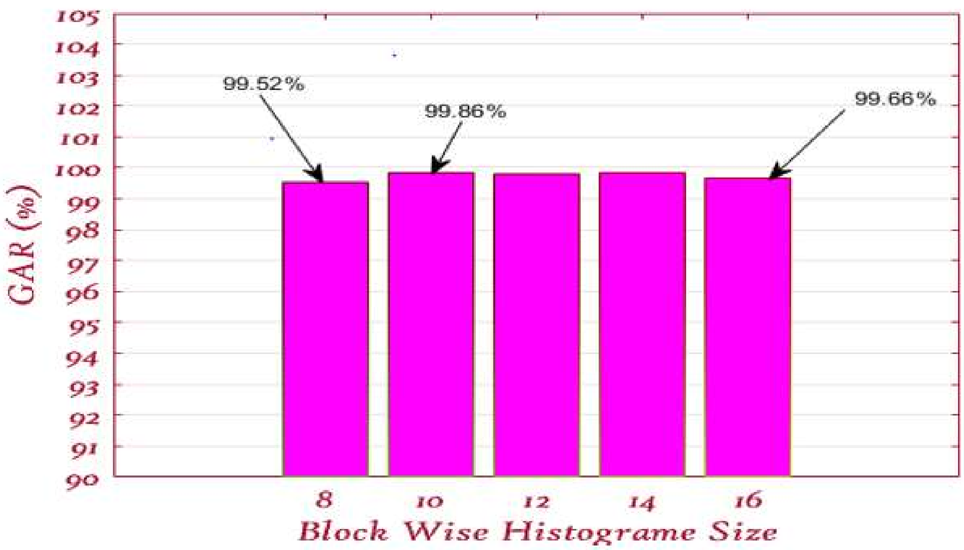

FIGURE 4.6. DCTNet parameter adaptation b) GAR against block wise histogram size.

4.5.2 Unimodal identification system results

Open set: Using DCTNet extraction for different fingers. Experimental results indicate that RIF performance is better than LIF, LMF, and RMF in terms of EER. This is illustrated in (Table 4.1) and(Figure 4.8 and Figure 4.7) for the performance of the unimodal system given EER = 0, 00% and T0 = 0, 8310. In the general case, the rest of the fingers give the best result when EER gives less than 0, 0673%.

Closed set: The perfect is RIF, because it gives the ideal value 100% than other fingers (LIF, LMF, RMF), they give the same best result when they give the identification rate 99:86%. These results are shown in the CMC curve (the identification rate against the rank) of closed set identification system (Figure 4.6). From the RPR, RIF and LIF and LMF give best results when it gives 1, 3, 14 respectively and RMF gives a very far value estimated at 104.

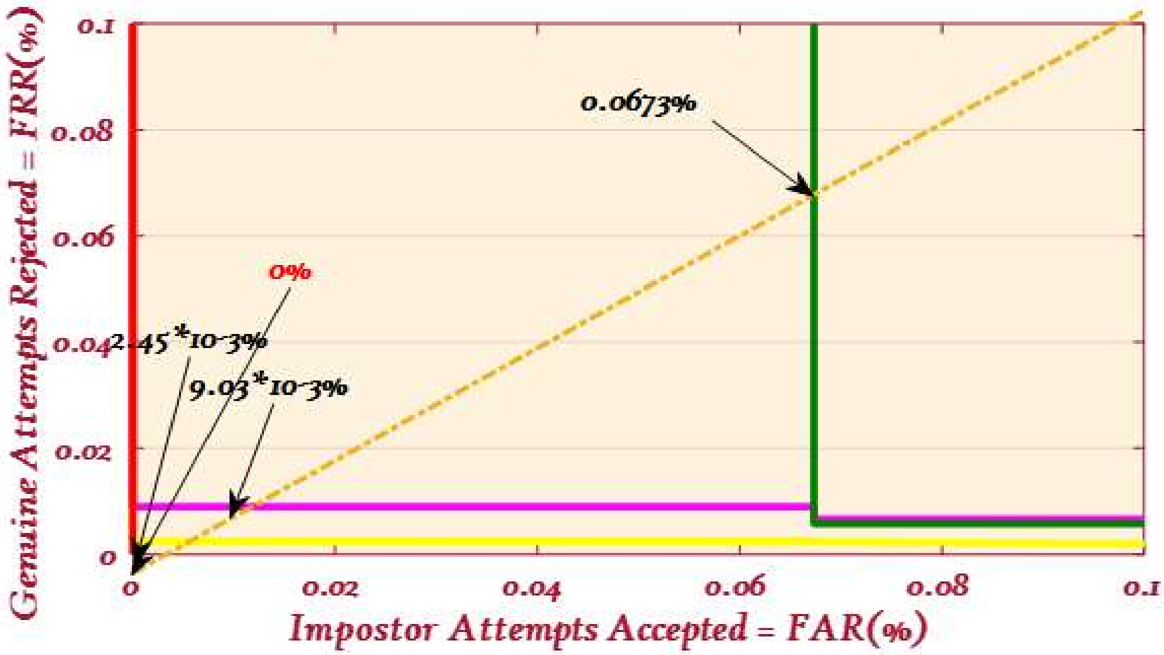

FIGURE 4.7. Unimodal system results curves 1) ROC curves.

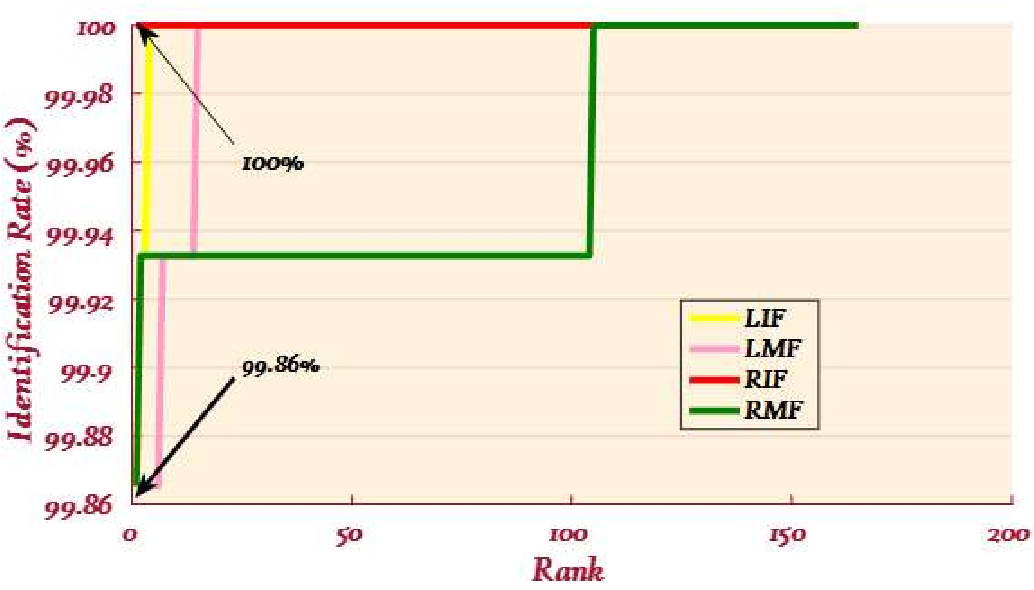

FIGURE 4.8. Unimodal system results curves 2) CMC curves.

The_performance of unimodal system					
Poly U Data Base	Types	DCTNet Features			
		Open set		Closed set	
		ERR	Th	ROR	RPR
165 Persons	LIF	$2.46 * 10^{-3}\%$	0.8851	99.86%	03
	LMF	$9.03 * 10^{-3}\%$	0.7444	99.86%	14
	RIF	0%	0.8310	100%	01
	RMF	0.0673%	0.6712	99.86%	104

Table 4.1: The performance of unimodal system using DCTNet extraction.

4.5.3 Multimodal identification system results

The purpose of multimodality is to improve the level of security of the system such that the identification rate of the merged biometric terms is greater than the maximum of the identification rates of the modalities taken separately. So, using the different modalities (four modalities: four fingers for FKP) we realize a system at the end based on the fusion between the two fingers.

In our work, the fusion at the score level is used because it is the most common approach used, it given the best results and it is simple for merged scores generated by different subsystems. (Table 4.2) and (Figure 4.8 and Figure 4.9) show the performance of the multimodal identification system.

The results indicate in open set identification all the fusion methods give a better result EER equal 0.00%, and the same in closed set identification all fusion methods give a better identification rate 100% in first rank.

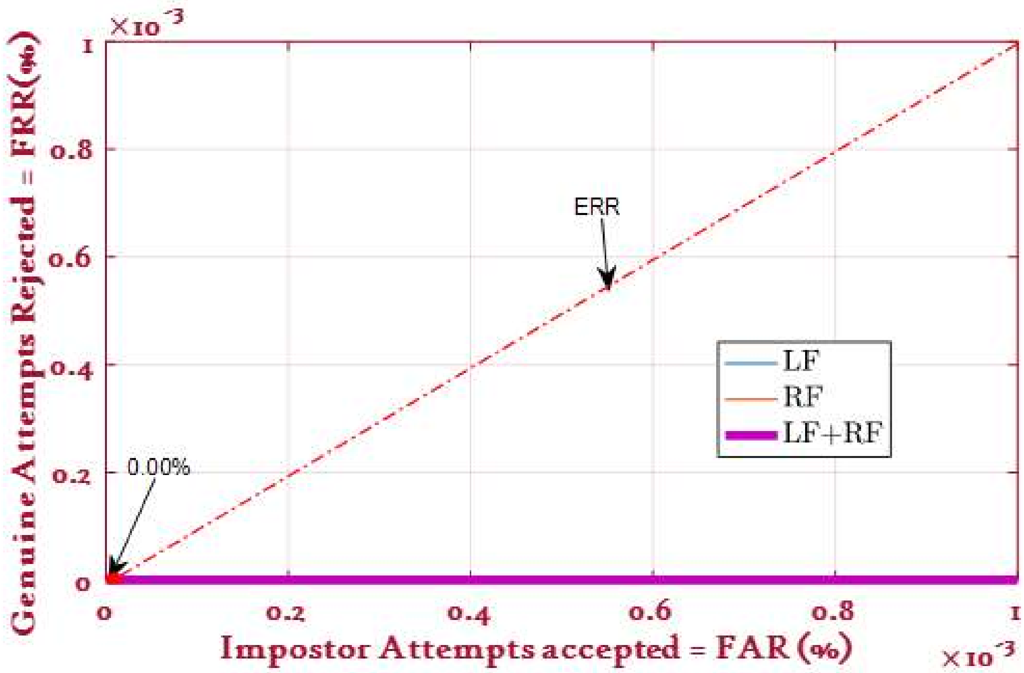

FIGURE 4.9. Multimodal system results a) ROC curves.

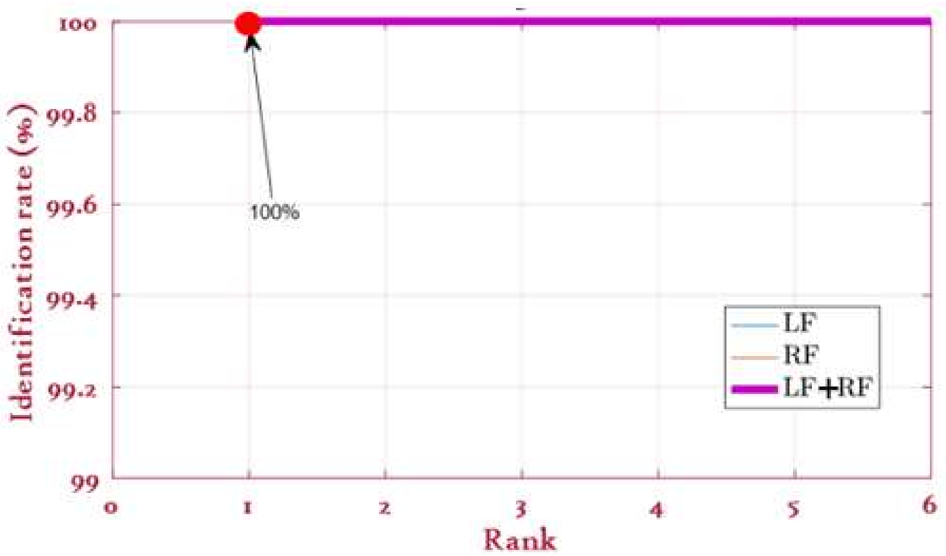

FIGURE 4.10. Multimodal system results b) CMC curves.

The performance of Multimodal system						
Poly U Data Base		DCTNet Features				
		Open set		Closed set		
	Fusion Types	ERR	Th	ROR	RPR	
165 Persons	LIF+LMF	0.00%	0.654	100%	01	
	RIF+RMF	0.00%	0.753	100%	01	
	RF+LF	0.00%	0.417	100%	01	

Table 4.2: The performance of multimodal system using DCTNet extraction.

By using different fusion rules on the performance of the multimodal system when our choose is LF (LIF, LMF) and with other case (RMF, LMF, LIF), the (Figure 4.10 and Figure 4.11) and (Table 4.3) or the (Figure4.12 and Figure 4.13) and (Table.4.4) show the performance of the multimodal identification system.

For all the rules in this study, the open set showed the best result where EER=0.00%, and in the closed set gives each of the Sum, Mul ,Weighted Product,Weighted Sum and Min the ideal result ROR=100% and RPR=1, except Max rule gives a lower result estimated by ROR=99.86% and RPR=02. Based on the above results, we note the accuracy of the multimodal system is better than the uni-modal system. The multimodal system have a (EER = 0.00%) and an (ROR = 100%) and an (RPR = 01), a perfect result. This ideal precision can be reduced to a large database. Because the sum rule sample to use and it gives a perfect result, it is the best compared to the other rules.

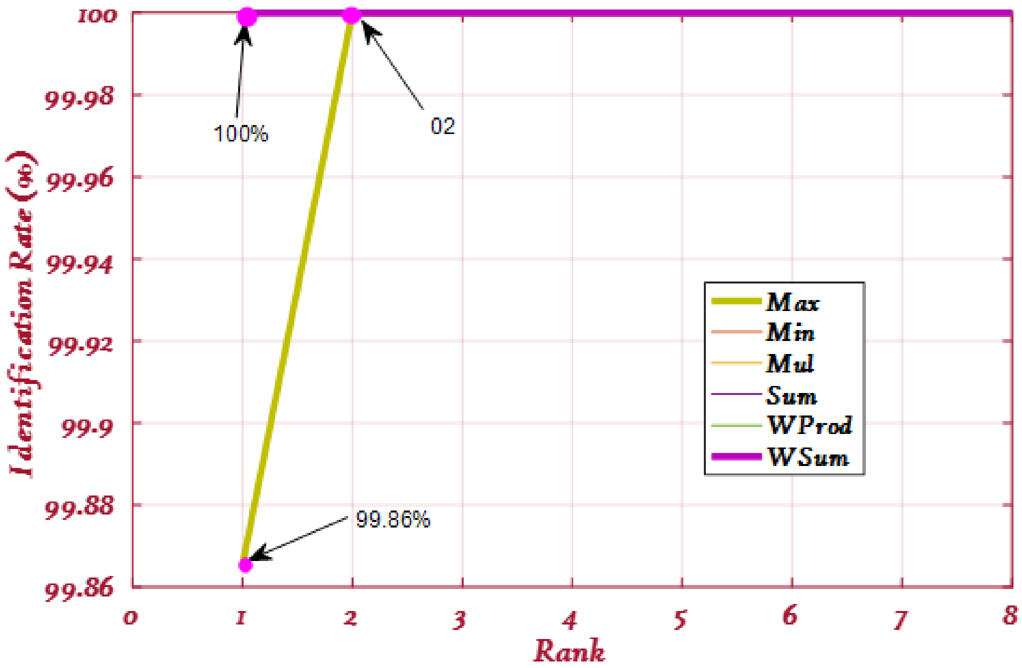

FIGURE 4.11. Multimodal system results a) CMC curves .in case two fingers (LMF,LIF)

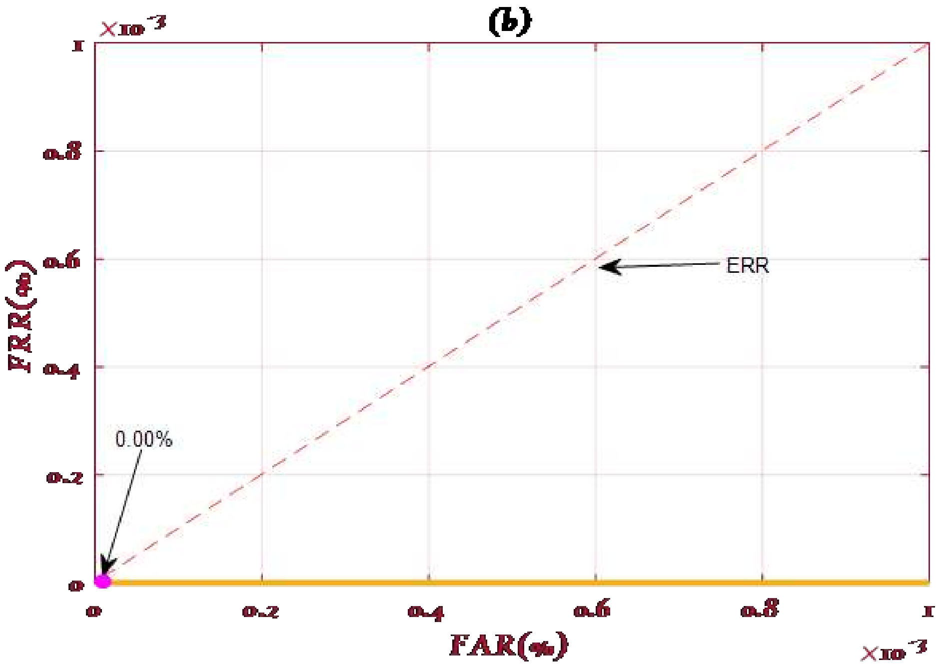

FIGURE 4.12. Multimodal system results b) ROC curves.in case two fingers (LMF,LIF)

Poly U Data Base	Fusion Rules	Open Set		Closed Set	
		DCTNet Features			
165 Persons		ERR	Th	ROR	RPR
	Sum	0.00%	0.654	100%	01
	Mul	0.00%	0.372	100%	01
	Min	0.00%	0.555	100%	01
	Max	0.00%	0.999	99.86%	02
	Weighted Product	0.00%	0.798	100%	01
	Weighted Sum	0.00%	0.915	100%	01

Table 4.3: The performance of multimodal system using DCTNet extraction.In case two finger (LMF,LIF)

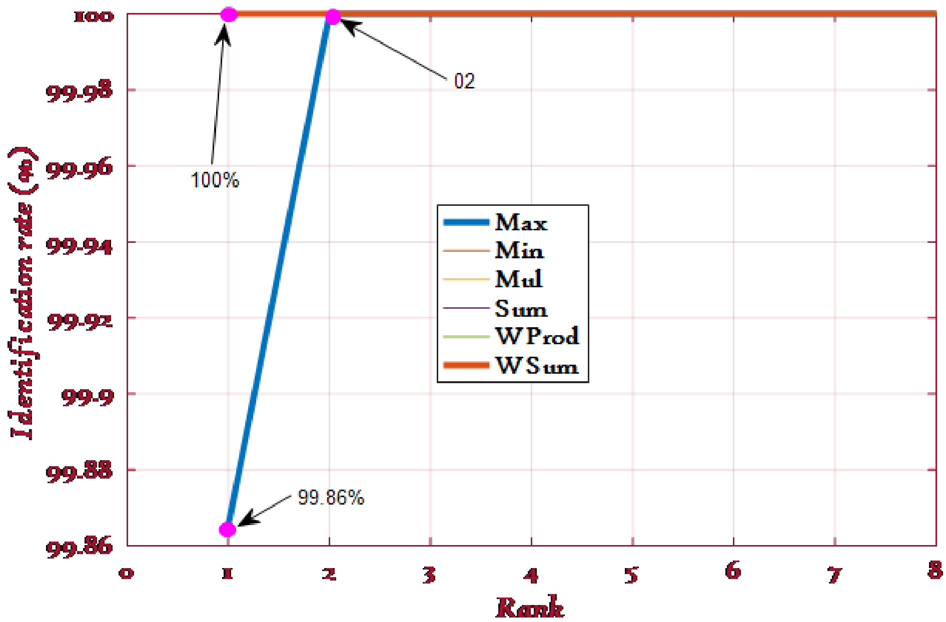

Figure 4.13: Multimodal system results a) CMC curves.In case three fingers (RMF, LMF, and LIF)

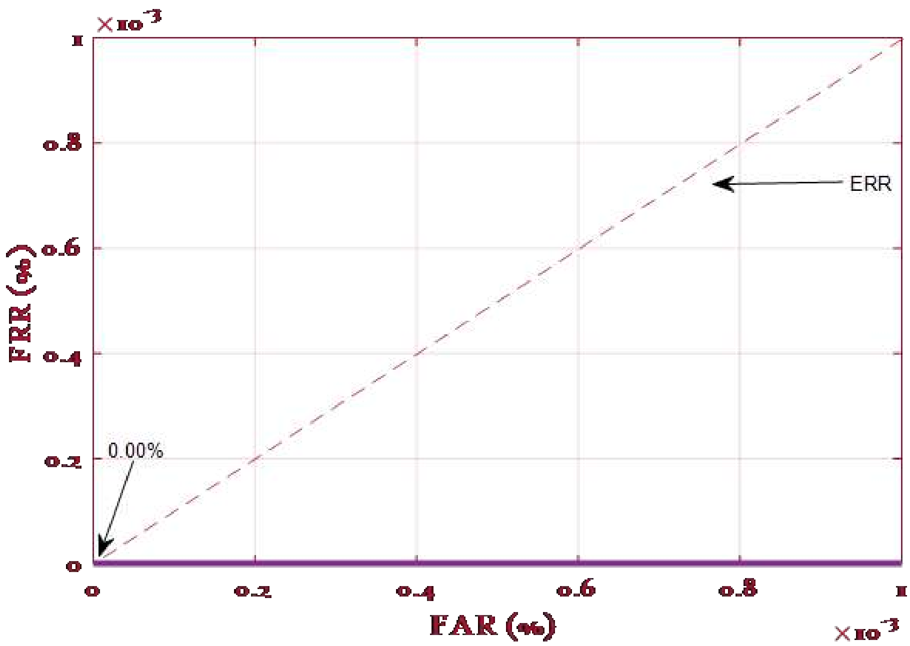

Figure 4.14: Multimodal system results b) ROC curves.In case three fingers (RMF, LMF, and LIF)

Poly U Data Base	Fusion Rules	Open Set		Closed Set	
		DCTNet Features			
165 Persons		ERR	Th	ROR	RPR
	Sum	0.00%	0.492	100%	01
	Mul	0.00%	0.108	100%	01
	Min	0.00%	0.462	100%	01
	Max	0.00%	0.999	99.86%	02
	Weighted Product	0.00%	0.108	100%	01
	Weighted Sum	0.00%	0.888	100%	01

Table 4.4: The performance of multimodal system using DCTNet extraction.In case three fingers (RMF, LMF, and LIF)

4.6 Conclusion

The biometric studies presented led to the development of a system for identifying people by FKP recognition. To do that, in this chapter we proposed several biometric systems. In addition to unimodal systems, we have explored some multimodal systems. These different systems are tested in order to improve the identification rate of the modalities in the two identification modes (open set and closed set) using feature extraction methods called DCTNet, we achieved a considerable improvement in the identification rate (100%).

CONCLUSION

Conclusion

In this highly interconnected world with increased concerns of identity fraud and national security, reliable and efficient identity management system has become very important. Biometric systems provide a greater degree of security and user convenience than the traditional authentication methods. Moreover, biometric systems also provide negative recognition and non-repudiation that traditional systems do not. Multibiometric systems, if properly designed, are able to increase the matching accuracy of a recognition system, increase population coverage and deter spoofing attacks.

The work presented in this dissertation is in the context of the automatic identification of people based on their biometric descriptors. We have used a new biometric modality, FKP, to realize our proposed biometric, unimodal and multimodal biometric systems. After introducing the general concepts of biometrics, we presented state of the art fusion methods of biometric modalities, using different techniques and levels of fusion. Our tests based on FKP data from the Polytechnic University of Hong Kong (PolyU) showed that our method could provide excellent result in terms of EER, recognition rate and global separation of impostor and customer distributions. We presented a novel approach for personal identification using two dimensional FKP image. A simple deep learning feature extraction DCTNet method is employed for knuckle identification. This method can capture the information from the texture in an image and provide a very high robustness that is efficiency describe the image characteristics. Improvement the performance is the main objective of this study. To achieve this we have applied and selected the best parameter of the DCTNet. All this results are obtained with using WPCA to reduce the dimension and SVM to classification.

In this work, in unimodal system the accuracy of given system is 100% for RIF and 99.86% for others (LIF, LMF and RMF).This means DCTNet works efficiently with RIF than others types. In multimodal system, the application of the combination of samples (LIF+LMF) and (RIF+RMF) also used to improve reached it gives the best process

EER=0.00% and ROR=100. In the end, the results are very interesting. In fact we got a great recognition rate of 100%, this rate is very interesting what makes our reliable system where it meets the objective that we set at the start.

EER=0.00% and ROR=100. In the end, the results are very interesting. In fact we got a great recognition rate of 100%, this rate is very interesting what makes our reliable system where it meets the objective that we set at the start.

Bibliography

Bibliography

[1] Jain AK, Flynn P, Ross AA "Handbook of biometrics". Springer, US, 2008.

[2] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer Science+Business Media, LLC 2011.

[3] Kai Cao and Anil K. Jain "Automated Latent Fingerprint Recognition ", in IEEE, April 2017.

[4] Ziaul Haque Choudhury "Biometrics Security Based On Face Recognition" B.S Abdu Rahman University, June 2013.

[5] Humayan Kabir Rana, Md Shafiul Azam and Mst Rashida Akhtar "Iris Recognition System Using PCA Based on DWT",SM Journal of Biometrics & Biostatistics.Aug, 2017.

[6] Michael Goh Kah Ong, Connie Tee and Andrew Teoh Beng Jin " TOUCH-LESS PALM PRINT BIOMETRIC SYSTEM ", International Conference on Computer Vision Theory and Applications, 2008.

[7] Dyala R. Ibrahim, Abdelfatah A. Tamimi, and Ayman M. Abdalla "Performance Analysis of Biometric Recognition Modalities", International Conference on Information Technology (ICIT), 2017.

[8] M. Pushpa Rani and G.Arumugam"An Efficient Gait Recognition System For Human Identification Using Modified ICA",International Journal of computer Science and Information Technology (IJCSIT),Vol 2,No 1,February,2010.

[9] Sandhya Avasthi, Tanushree Sanwal "Biometric Authentication Techniques: A Study on Keystroke Dynamics", International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016.

[10] Himanshu Srivastava" A Comparison Based Study on Biometrics for Human Recognition", Journal of Computer Engineering (IOSR-JCE), Volume15 Issue 1, (Sep. – Oct) 2013.

[11] Pankaj Sareen "Biometrics – Introduction, Characteristics, Basic technique, its Types and Various Performance Measures " Department of Computer Applications, Baddi University of Emerging Sciences & Technology, India, April 2014.

[12] Mohammed El-Abed, Christophe Charrier "Evaluation of Biometric Systems", New Trends and Developments in Biometrics, 13 May 2014.

[13] Dr.Rakesh Singh Jadon, Dr. Sarita Singh Bhadauria, Sushma Jaiswal " Biometric: case study", Journal of Global Research in Computer Science, Volume 2, No. 10, October 2011.

[14] Eugen LUPU, Petre G. POP,"MULTIMODAL BIOMETRIC SYSTEMS OVERVIEW", Technical University of Cluj-Napoca,Volume 49, Number 3, 2008.

[15] H. Jaafar and D. A. Ramli, "A Review of Multibiometric System with Fusion Strategies and Weighting Factor", Int. J. Comput. Sci.Eng. (IJCSE*)*, vol. 2, no. 4, pp. 158_165, Jul. 2013.

[16] C. Prathipa and L. Latha, ``A survey of biometric fusion and template security techniques," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 3, no.10, pp. 3511_3516, 2014.

[17] Mohamed Deriche, “Trends and Challenges in Mono and Multi Biometrics”, IEEE 2008.

[18] S. Singh, A. Gyaourova, G. Bebis, and I. Pavlidis, ``Infrared and visible image fusion for face recognition," in Proc. Defense Secur., vol. 5404.2004, pp. 585_596.

[19] M. F. Nadheen and S. Poornima, ``Feature level fusion in multimodal biometric authentication system," Int. J. Comput. Appl., vol. 69, no. 18, p. 36, 2013.

[20] Robert Snelick, Mike Indovina, James Yen, and Alan Mink, "Multimodal Biometrics: Issues in Design and Testing", ICMI’03, November 5-7, 2003, Vancouver, British Columbia, Canada. ACM 1-58113-621-8/03/0011.

[21] A.Ross, K.Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer-Verlag edition, 2006.

[22] A. K. Jain, K. Nandakumar and A. Ross, “Score normalization in multimodal biometric systems,” Pattern Recognition, vol. 38, no. 12, p. 2270–2285, 2005.

[23] R. Cappelli, D. Maio and D. Maltoni, "Combining Fingerprint Classifiers", in Proceedings of First International Workshop on Multiple Classifier Systems (MCS), Cagliari, Italy, 2000.

[24] F. R. Hampel, E. M. Ronchetti, P. J. Rousseeuw and W. A. Stahel, "Robust Statistics: The Approach Based on Influence Functions", Wiley, 1986.

[24] R. Brunelli and D. Falavigna, “Person identification using multiple cues,” Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 17, no. 10, pp.955-966, 1995.

[25] Yap, T., Jiang, X., Kot, A.C " Two-dimensional polar harmonic transforms for invariant image representation", IEEE Trans. Pattern Anal. Mach. Intell. 32(7), 1259–1270 (2010).

[26] Andreopoulos, A., Tsotsos, J " 50 years of object recognition: directions forward. Comput", Vis.Image Underst. 11**7**(8), 827–891 2013.

[27] Kim, B., Yoo, H., Sohn, K. "Exact order based feature descriptor for illumination robust image matching" Pattern Recogn. 46(12), 3268–3278, 2013.

[28] Angelika Olejczak, Janusz Korniak, and Bogdan M.Wilamowski." Discrete Cosine Transformation as Alternative to Other Methods of Computational Intelligence for Function Approximation". In Leszek Rutkowski, Marcin Korytkowski, Rafa Scherer, Ryszard Tadeusiewicz, Lotfi A. Zadeh, and Jacek M.Zurada, editors, Artificial Intelligence and Soft Computing, pages 143–153. Springer International Publishing, 2017.

[29] YunheWang, Chang Xu, Shan You, Dacheng Tao, and Chao Xu. CNNpack "Packing Convolutional Neural Networks in the Frequency Domain" In D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, editors, Advances in Neural Information Processing Systems 29, pages 253–261. Curran Associates, Inc., 2016.

[30] C. J. Ng and A. B. J. Teoh, \Dctnet "A simple learning- free approach for face recognition," in 2015 Asia-Paci_c Signal and Information Processing Association Annual Summit and Conference (APSIPA). IEEE, 2015, pp.761-768.

[31] Y. Xian, "Detection and classification of whale vocalizations", Ph.D. thesis, Duke University, 2016.

[32] Y. Xian, A. Thompson, X. Sun, D. Nowacek, and L. Nolte, "DCTNet and PCANet for acoustic signal feature extraction", arXiv preprint arXiv: 1404.3606, 2016.

[33] C.-C. Chang and C.-J. Lin. LIBSVM "A library for support vector machines" In: ACM Transactions on Intelligent Systems and Technology, Vol. 2, pp. 1-27,2011.

[34] Kumar A, XuZ "Can we use second minor finger Knuckle patterns to identify

humans?", Proc IEEE Co; put Soc Conf Comput, Vis Patterns Recognit Workshop: 106_112, 2014.

[35] PolyU Finger KnucklePrint Database. ttp://www.comp.polyu.edu.hk/ biometrics/FKP.htm, Hong Kong polytechnic university (PolyU).

[36] M. Deriche, "Trends and Challenges in Mono and Multi biometrics," presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, Sousse, 2008. pp. 1-9.

[37] G. Amirthalingam, "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues (IJCSI), vol. 10, no. 5, pp. 234-241, 2013.

[38] Mohamad El-Abed, Christophe Charrier, "Evaluation of Biometric Systems", New Trends and Developments in Biometrics, pp. 149 - 169,<10.5772/52084>. <hal-00990617>,2012.

[39] H. D. Crane and J. S. Ostrem, Automatic signature verification using a threeaxis force-sensitive pen. *IEEE Trans. on Systems, Man and Cybernetics,* **SMC-13**(3), 329–337, 1983.

[40] V. S. Nalwa, Automatic on-line signature verification. *Proc. IEEE,* **85**(2), 215–239, 1997.

[41] J.R. Samples and R.V.Hill,Use of infrared fundus reflection for an identification device.*Am. J. Ophthalmol.*, **98**(5), 636–640, 1984.

[42] R. H. Hill, Retina identification, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.

[43] L. D. Harmon, M. K. Khan, R. Lasch and P. F. Ramig, Machine recognition of human faces. *Pattern Recognition*, **31**(2), 97–110, 1981.

[44] J.D.Daugman,High confidence visual recognition of persons by a test of statistical independence, *IEEE Trans. Pattern Analysis andMachine Intelligence,* **15**(11), 1148–1161, 1993.

[45] R. P.Wildes, Iris recognition: an emerging biometric technology, *Proc. IEEE,* **85**(9), 1348–1364, 1997.

[46] A. Jain, R. Bolle and S. Pankati, Introduction to biometrics, in A. Jain, *et al.* (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.

[47] Aditya Nigam1 , Phalguni Gupta2, "Finger-Knuckle-Print ROI Extraction Using Curvature Gabor Filter for Human Authentication", 1School of Computer Science and Electrical Engineering, (IIT Mandi), Mandi, India, 2National Institute of Technical Teacher’s & Research (NITTTR), Salt Lake, Kolkata, India

Abstract

one of the current trends in human identification is the development of new emerging methods. Due to increased security concerns and the development of counterfeiting techniques. This development depends on the unique parts of the human body that can be identified and used as a means of identifying a person. Including fingerprints, iris, lips, etc.

Most of the systems and methods are slow or require expensive technical equipment, for this, we suggest a new approach for personal authentication using Finger-Knuckle Print through with a novel texture descriptor, Discrete Cosine Transform Network (DCTNet) and support vector machine (SVM) classifier. Finger-knuckle-print is one of the emerging biometric traits.Recently it has been found FKP is highly rich in textures and can be used to uniquely identify a person. The study also takes the unimodal and multi-modal biometric systems results along with their methods of information fusion in score level, which does not require special equipment and can be used in systems where fast detection is needed.

Keywords : Biometric, FKP, DCTNet, SVM, unimodal, multimodal.

الملخص

واحدة من الاتجاهات الحالية في تحديد الإنسان هو تطوير أساليب جديدة ناشئة. بسبب تزايد المخاوف الأمنية وتطوير تقنيات التزوير. يعتمد هذا التطور على الأجزاء الفريدة من الجسم البشري التي يمكن تحديدها واستخدامها كوسيلة لتحديد هوية الشخص. بما في ذلك بصمات الأصابع ، القزحية ، الشفاه ، إلخ.

معظم الأنظمة والأساليب بطيئة أو تتطلب معدات تقنية باهظة الثمن ، ولهذا الغرض ، نقترح نهجًا جديدًا للمصادقة الشخصية باستخدام بصمة مفصل الاصبع من خلال واصف نسيج جديد ، شبكة تحويل كوسين منفصلة. يعتبر مفصل الاصبع إحدى السمات البيومترية الناشئة. وقد وجد أن بصمة مقصل الاصبع غنية جدًا بالقوام ويمكن استخدامها لتمييز شخص ما بشكل فريد. كما تتناول الدراسة نتائج أنظمة القياس الحيوي أحادية الواسطة ومتعددة الوسائط إلى جانب أساليب دمج المعلومات في مستوى النقاط ، والتي لا تتطلب معدات خاصة ويمكن استخدامها في الأنظمة التي تحتاج إلى الكشف السريع.

الكلمات المفتاحية : البيومتري, مفاصل الإصبع ,التعلم العميق, أحادي الوسيطة ,متعدد الوسائط

Résume

L'une des tendances actuelles en matière d'identification humaine est le développement de nouvelles méthodes émergentes. En raison de problèmes de sécurité accrus et du développement de techniques de contrefaçon. Ce développement dépend des parties uniques du corps humain qui peuvent être identifiées et utilisées comme un moyen d'identifier d'une personne. Y compris les empreintes digitales, l'iris, les lèvres, etc.

La plupart des systèmes et des méthodes sont lents ou nécessitent un équipement technique coûteux. Pour cela, nous suggérons une nouvelle approche pour l'authentification personnelle à l'aide de Finger-Knuckle Print avec un nouveau descripteur de texture, un réseau discret de transformateur cosinus (DCTNet). L'empreinte digitale est l'un des caractères biométriques émergents. Récemment, on a découvert que FKP est très riche en textures et peut être utilisé pour identifier une personne de façon unique. L'étude prend également les résultats des systèmes biométriques unimodaux et multimodaux ainsi que leurs méthodes de fusion de l'information au niveau des scores, qui ne nécessitent pas d'équipement spécial et peuvent être utilisés dans des systèmes où une détection rapide est nécessaire.

Mots clés : biométrique, FKP, PCANet, monomodal, multimodal, SVM