PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA UNIVERSITY

EL-OUEDFACULTY OF TECHNOLOGIES

DEPARTMENT OF ELECTRICAL ENGINEERING

FINAL STUDY DISSERTATION

In the aim obtaining of MASTER Degree - ACADEMIC Domain:

Sciences and TechnologyOption: Telecommunication

Specialty: Systems of communications

THEME

Finger knuckle print recognition based on features selection methods

Presented by:
Bachi Slimane
Mekhadmi Rofaida
Mezzar Abdelkarim

Was Publicly Debated in: June 2021 in front of The Examining Committee Composed from:

President	**Dr. A . Khelil**	**MCA**	**El-Oued University**
Examiner	**Dr. R . Touhami**	**MAA**	**El-Oued University**
Supervisor	**Dr. A .Tidjani**	**MCB**	**El-Oued University**
Co-Supervisor	**Dr. K .BEN SID**	**Doctorant**	**Ouergla University**

Academic year: 2019/2020

ABSTRACT

ABSTRACT

Biometrics is the automated recognition of individuals based on their physiological and behavioral characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways .

One of the directi 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,

Finger knuckle print is considered as one of the emerging hand biometric traits due to its potentiality toward the identification of individuals. for this we are interested in studying a new approach for personal authentication using Finger-Knuckle Print through with a novel texture descriptor, AlexNet , GoogleNet and Support vector machine (SVM) , k-Nearest-Neighbor (KNN), Radial Basis Function (RBF).

Keywords

Biometric, FKP, AlexNet, GoogleNet , SVM , KNN , RBF unimodal, multimodal.

DEDICATION

DEDICATION

Rofaida

To my niece "E .Radoua " I dedicate this humble work to her memory , I constantly pray to the good god , that he may grant you his mercy .

Slimane

To my best friend "A.mustapha" I dedicate this humble

Work and I constantly pray to the god , to bless him.

Abdelkarim

To my best friend "B.yacine " I dedicate this humble

Work and I constantly pray to the god ,

I constantly pray to the god , to bless him

To our fathers and our mothers, and all of our family and our dear friends. We are indebted to all of you for your love, support and encouragement. We could not finish without saying thank you for everything.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

Acronyms

Acronyms

DNA Deoxyribo Nucleic Acid

PIN Personal Identification Number

IoT Internet of Things

DART Dallas Area Rapid Transit

ID Identification cards

LED Light-emitting diode

CCD Charge coupled device

IE Convex Direction Coding

ICD Convex direction code map

DL Deep learning

NN Neural networks

DBM Deep Boltzmann Machine

DBN Deep Belief Networks

CONV Convolutional Layer

ReLU Rectified Linear Unit Layer

POOL Pooling Layer

FC Fully Connected Layer

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

Acronyms

LIF Left Index Finger

LMF Left Middle Finger

PCA Principal Component Analysis

RF Right Finger

RIF Right Index Finger

RMF Left Middle Finger

ROC Receiver Operating Characteristic

ROR Rank-One Recognition

RPR Rank of Perfect Rate

CMC Cumulative Math Characteristic

DCT Discrete Cosine Transform

CNN Conventional neural network

SVM Support Vector Machine

KNN K-Nearest-Neighbor

RBF Radial Basis Function

General introduction

General introduction

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.

The fingerprint is very popular in the biometric system and is used in access control and for attendance system. Some of the issues in using fingerprint are: 1) easily spoofed by the attackers, 2) if the skin is wet or dry, then, it is difficult for sensors to detect, and 3) for most of the individuals working in agricultural lands the fingerprint features such as minutiae, ridges and valleys are not clear. Finger knuckle print is been used as one of biometrics in during the last ten years. Finger Knuckle print (FKP) is the skin pattern of the back surface of the hand, which is highly rich in texture, unique in characteristics, contactless and less expensive. The back surface of the hand has three joints called phalangeal joints. The region which joins the finger and hand is known as Metacarpophalageal joint. The mid joint of the finger is called Proximal Inter-Phalangeal joint (PIP) or major Knuckle and the hinge joint in the tip is called as Distal Interphalangeal Joint (DIP) or minor knuckle. The skin pattern of interphalangeal joints creates the dermal patterns consisting of lines, wrinkles, contours etc. Patterns of finger dorsum surface are highly unique in nature and are used in a biometric system for identification and authentication [45-46-47] .

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 four types of fingers, Left Index Fingers (LIF), Left Middle Fingers (LMF), Right Index Fingers (RIF) and Right Middle Fingers (RMF) can be used to create a strong and precise biological system. Our experience is based on deep learning GoogleNet and AlexNet for feature extraction and with different classifier methods (SVM, KNN, RBF) .

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.

Chapter two contain some explanation of Feature extraction, deep learning technique and we gave an overview of the FKP system , descriptor of the texture, Conventional neural network (CNN) and Support vector machine (SVM)

Chapter three presents the results and discussion of the identiftcation system by the FKP modalities. In unimodal system case based on four fingers (left index finger, left middle finger, right index finger and right middle finger), and fusion of the two

samples (left finger and right finger) and of three samples (left index finger, left middle and right middle finger) forming a multimodal system case.

CHAPTER 01

1 The biometric

1.1- Introduction:

The biometric traits possessed by each individual are unique and has the potential to recognize an individual. Biometric traits can be physical and behavioral. Therefore, biometrics are used for verification or identification of individuals for many critical applications like border control, access control, immigration, forensic and different law enforcement. There are two phases in every conventional biometric system: Enrolment phase and authentication or identification.

In the enrolment stage, the original biometric trait is captured and saved in the database. During the authentication stage, the system matches that stored template every time the user access the system by providing the live biometric.[1]

1.2- Definition of Biometrics:

The word "biometrics" comes from two Greek words meaning "measure of life" (the word "bio" means life and "measurement" means measurement). Biometrics is a branch of biology that uses measurement and statistical analysis to understand humans or animals .[2]

They are human physical or behavioral characteristics that can be used to digitally identify a person to give them access to systems, devices, or data. Examples of these vital identifiers are fingerprints, facial patterns, voice or writing rhythm. Each of these identifiers is unique to the individual and can be used together to ensure greater accuracy in identification.

Biometrics is also the most appropriate way to identify and validate individuals in a reliable and rapid manner.

1.3- History of Biometrics:

While the earliest accounts of biometrics can be dated as far back as 500BC in Babylonian empire, the first record of a biometric identification system was in **1800s**, Paris, France. Alphonse Bertillon developed a method of specific body measurements for the classification and comparison of criminals. While this system was far from perfect, it got the ball rolling on using unique biological characteristics to authenticate identity .

Fingerprinting followed suite in the **1880s**, not only as a means of identifying criminals but also as a form of signature on contracts. It was recognized that a fingerprint was symbolic of a person’s identity and one could be held accountable by it. Through there are debates on who exactly instigated fingerprinting for identification, Edward Henry is denoted for the development of a fingerprinting standard called the Henry Classification System.

This was the first system for identification based on the unique architectures of fingerprints. The system was quickly adopted by law enforcement replacing Bertillon’s methods becoming the standard for criminal identification. This began a

century's worth of research on what other unique physiological characteristics could be used for identification.

Within the following century, biometrics grew exponentially as a field of research. There were so many advances within the **1900s** that it'd be crazy to try and list them all, so here are the highlights from the second half of the century:

By 1969, fingerprint and facial recognition was so widely used in law enforcement, the FBI put funding towards developing automated processes. This was a catalyst for the development of more sophisticated sensors for biometric capture and data extraction .

In the **1980s**, the National Institute of Standards and Technology developed a Speech group to study and push forward the processes for speech recognition technology.

These studies are the basis for the voice command and recognition systems we use today[3-4] .

1974: Hand Geometry, first commercial hand geometry system becomes available

1976: Voice, first prototype of a speaker recognition system is released

In 1985, the concept that much like fingerprints, irises, were unique to everyone was proposed and by 1994, the first iris recognition algorithm was patented. In addition, it was discovered that blood vessels patterns in eyes were unique to everyone and were used for authentication as well.

In 1991, facial detection technology was developed making real time recognition possible. While these processes had many faults, it skyrocketed interest in face recognition development.

1998: DNA indexing system is released by the FBI

1999: Fingerprint System , FBI released the first automated fingerprint identification

2000: Multi biometric, new biometric systems have been released and more recent techniques combine different biometric traits.

1.4- Biometric modalities:

The choice of a biometric trait for a particular application depends on issues besides the matching performance. Raphael and Young identified a number of factors that make a physical or a behavioral trait suitable for a biometric application.[5] The following seven factors are taken from an article by Jain et al[6]

- **Universality :** Every individual accessing the application should possess the trait.

1 The biometric

- **Uniqueness :** The given trait should be sufficiently different across members of the population.
- **Permanence :**The biometric trait of an individual should be sufficiently invariant over time with respect to a given matching algorithm .A trait that changes significantly is not a useful biometric.
- **Measurability :** It should be possible to acquire and digitize the biometric trait using suitable devices that do not unduly inconvenience the individual. Furthermore, the acquired raw data should be amenable to processing to extract representative features.
- **Performance :**The recognition accuracy and the resources required to achieve that accuracy should meet the requirements of the application.
- **Acceptability :** Individuals in the target population that will use the application should be willing to present their biometric trait to the system.
- **Circumvention :** The ease with which a biometric trait can be imitated using artifacts—for example, fake fingers in the case of physical traits and mimicry in the case of behavioral traits—should conform to the security needs of the application.

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 traitscan then be used for authentication of a person's identity by using pattern recogni-tion 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)[2] :

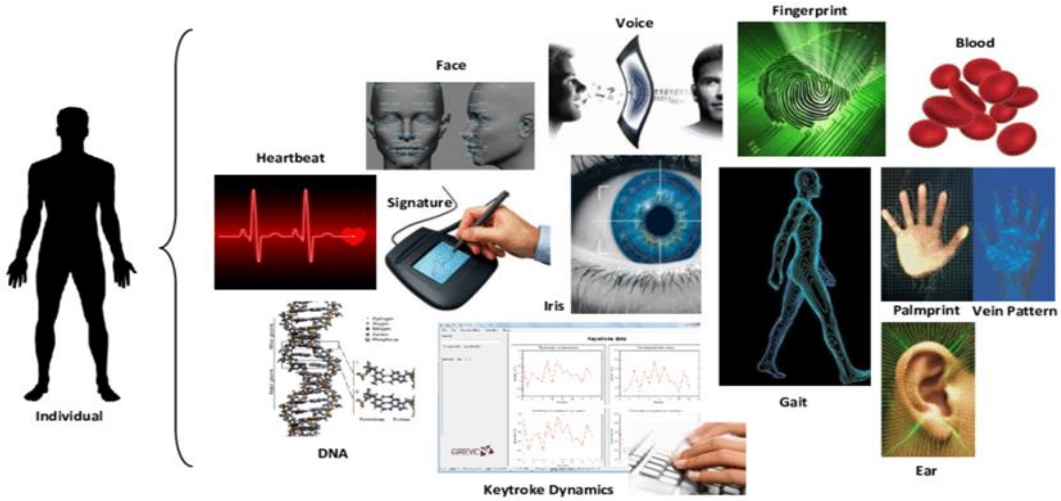

Figure 1.1 : Different physiological and behavioral Biometrics characteristics

1 The biometric

1.5- Types of Biometrics:

Biometric sensors or access control systems are classified into two types such as Physiological Biometrics and Behavioral Biometrics.

1.5.1- Behavioral biometrics:

Are based on patterns unique to each person. How you walk, speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

- **Voice Recognition :**Voice recognition technology is used to produce speech patterns by combining behavioral and physiological factors that can be captured by processing speech technology. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence. Voice recognition can be separated into different categories based on the kind of authentication domain, such as a fixed text method, in the text-dependent method, the text-independent method, and conversational technique
- **Signature Recognition :**Signature recognition is one type of biometric method used to analyze and measure the physical activity of signing like the pressure applied, stroke order and speed. Some biometrics are used to compare visual images of signatures. Signature recognition can be operated in two different ways, such as static and dynamic.

1.5.2 -physiological Biometrics:

They can be either morphological or biological.

Morphological identifiers mainly consist of fingerprints, the hand's shape, the finger, vein pattern, the eye (iris and retina), and the face's shape.

For biological analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics.

- **Fingerprint :**Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae, and furrows. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation, and ridge.
- **Face Recognition:** A face recognition system is one type of biometric computer application that can identify or verify a person from a digital image by comparing and analyzing patterns. These biometric systems are used in security systems. Present facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face. Nodal points are nothing but endpoints used to measure variables on a person’s face, which includes the length and width of the nose, cheekbone shape, and eye socket depth.

- **Iris Recognition :** Iris recognition is one type of bio-metric method used to identify the people based on single patterns in the region of ring-shaped surrounded the pupil of the eye. Generally, the iris has a blue, brown, gray or green color with difficult patterns that are noticeable upon close inspection.
- **Hand Geometry :** The actual shape and dimensions of your hand are sometimes used for access control and time-and-attendance operations in the workplace. However, they are not as unique as fingerprints, so aren't viable in high-security applications.
- **Finger knuckle print (FKP) :** is one of the emerging biometric traits. The region of in terestis the area where the maximum information is centered, for a finger knuckle it is the area surrounding the knuckle region.[2]
- **DNA** : is an emerging biometric trait that can be used for recognizing individuals. The specific area of the long DNA sequence is observed to find the identical feature. DNA itself is unique for each individual, except the identical twins. Therefore, it achieves high accuracy. DNA can be acquired easily from hair, saliva, skin follicles etc..

1.5.2.1-Strengths and weaknesses of Physiological Biometrics:

The table below shows the strengths and weaknesses of some biometrics:

BIOMETRICS	Strengths	Weaknesses
Fingerprint	• Most used biometrics • High matching speed • Ability to Enroll Multiple Fingers	• Sensors can be foiled by tricked fingerprints . • Small but significant failure to enroll rate
Face Recognition	• Ability to Operate without Physical Contact or User Complicity • Ability to Enroll Static Images	• Changes in Physiological Characteristics That Reduce Matching Accuracy • Potential for Privacy Abuse Due to Non-cooperative Enrollment and Identification
Iris Recognition	• Stability of Characteristic over Lifetime • Suitability for Logical and Physical Access	• Difficulty of Usage • User Discomfort with Eye-Based Technology • Need for a Proprietary Acquisition Device
Hand Geometry	• Ability to Operate in Challenging Environment • Established, Reliable Core Technology	• Inherently Limited Accuracy • Form Factor That Limits Scope of Potential Applications • Price

Table 1.1 : Strengths and weaknesses of Physiological Biometrics.

1.6- Biometric application:

1.6.1 -Airport Security:

Thousands of people pass through airport terminals and identifying these passengers can be very difficult. Biometric technology to verify passenger identifier is now used in many airports across the globe. The top modality choice for immigration control is iris recognition in many airports and in order to be able to use the iris recognition, travelers have to first go through a process of enrolment by having their iris and face captured by a camera. These captured details contain unique details which are stored in an international database. The database is then used at points of entry and exit for traveler's identification verification. The verification is done first by allowing the camera capture the iris again and then uses a software program to match what is stored in the database. If there is a match, access is granted[7] .

Figure 1.2 : Biometric of Airport Security

1.6.2 -Law Enforcement:

Biometrics is also used in organizations such as Federal Bureau of Investigations (FBI). It can be used in the identification of criminals. It is also widely used for jail and prison management whereby it provides a solution that can safely and securely manage prisoner identity [7] .

Figure 1.3 : Biometric of Law Enforcement

1.6.3 -Mobile Access and Authentication:

Perhaps one of the most common uses of biometric technology is smartphone security. Apple were the first to introduce the Touch ID solution – using fingerprint recognition technology – and since then, mobile phone security has evolved toutilise a number of biometric technologies including facial recognition, iris recognition and voice recognition.

All new mobile phones are now integrating some form of biometric modality as a way of securing your device or specific applications such as banking apps and it is expected that biometrics will be used alongside traditional password and PIN options as a form of two-factor authentication.

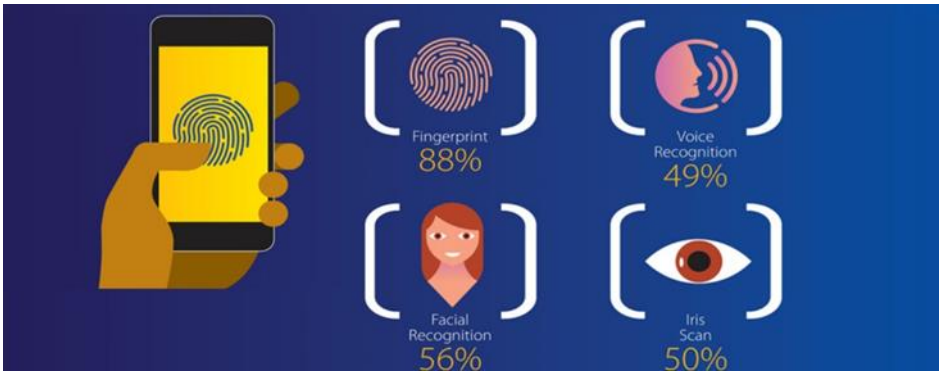

Figure 1.4 : Biometric of Mobile Access and Authentication.

1.6.4 -Banking:

The banking sector is another embracing biometrics across a range of services in order to deliver a more seamless experience for customers.

Seven Bank in Japan is rolling out a trial of Facial Recognition at ATMs. Facial Recognition will be used as an additional level of security to authenticate that the owner of the card is the person using the card.

As global financial entities become more digitally based, banks are also implementing biometric technology to improve customer and employee identity management in an effort to combat fraud, increase transaction security, and enhance customer convenience.

Customers are also worried about identity theft and the inconvenience associated with constantly having to prove their identities. As a result, more and more customers are looking for banks that have biometric authentication in place prompting banks to research the technology for implementation.

Figure 1.5 : Biometric of Banking.

1.6.5 -Home Assistants:

Anyone who is familiar with Google Home, Alexa and Siri will already be accustomed to using voice recognition as a biometric identifier. Google Assistant that powers Google Home as well as the assistant on Android devices is compatible with a wide range of IoT (Internet of Things) devices including light bulbs, door locks, security cameras, security lights and more.

Of course, when linking your home assistant with any of these connectable devices, security is imperative. You wouldn't want them controlled by just anyone. That's why Google Assistant's ability to recognise the voice of authorised users is critical.

Figure 1.6 : Biometric of Home Assistants.

1.6.6 -Building Access:

Whether it is your home or the workplace, biometric technology is now used commonly as a means of allowing access to buildings, or specific areas within a building.

Biometrics bring many advantages when it comes to access control. The technology can provide a frictionless entry experience when utilising facial or iris recognition to control access secure areas within a building.

Fingerprint recognition is the most widely utilised biometric used for accessing buildings and it provides an extra layer of security for building managers. Whereas a key, access card or a PIN number can be stolen, it's much more difficult to steal a biometric identifier, making it a much more secure way to secure buildings.

Figure 1.7: Biometric of Building Access

1.6.7-Public Transport:

Biometric adoption within public transportation is still in its early phases,However the potential uses within public transport are wide ranging and include security and enhancing customer experience.

Early adopters of biometric technology include the Dallas Area Rapid Transit (DART), the largest municipal transit agency in North Texas. DART implemented facial recognition technology cameras in its trains. These cameras integrate biometricsfor several purposes including keeping track of train capacity, medical emergencies and allowing the police to know when a wanted person is on board.

Other applications of biometric technology include the use of smart ID cards and smart ticketing to match a person using facial recognition in order to access transit systems, allowing for safer travel and simplifying the process of ticketing and

Figure 1.8 : Biometric of Public Transport .

1.6.8 -Blood Banks:

When it comes to giving blood, identity is extremely important. In the past, donors were issued with cards containing all the information required. However, this data is now frequently being stored digitally – with donors using fingerprint or iris recognition to access their vital details.

The use of biometric identifiers eliminates the risk of duplication, data entry issues and the need to carry national identification cards, making the process more secure as well as improving the customer experience of giving blood.

Figure 1.9: Biometric of Blood Banks.

1.7- Biometric system :

A typical biometric system is constituted of four principal modules (Figure 1.10):

1- **Biometric sensor:** it is responsible for capturing the biometric characteristics from the biometric subject and converting it to a digital form to be transferred to the subsequent module. The performance of the overall process depends heavily on the quality of the acquired raw data. In fact, this data is a result of transforming a real continuous phenomenon (such as a face) to a digital discreet form (face image) resulting in a loss of data. The quality of the acquired data depends on the technology of the reader, the added noise and the degree of the interoperability of the user with the system.[8]

2- **Enrollment:** Biometric data is preprocessed to enhance its quality. Some relevant discriminatory features are extracted to generate a compact representation called "template" The generated template is then sent to the storage system

3- **Storage system:** the storage system can be a simple file in a simple smartcard as it can be a big database managed by an SGBD. In association with the generated template, some biographic information (name, passwords, address, etc.) can be stored. In any case, the important factor to deal with is the security of the stored template. A compromised template can help to reconstruct the original biometric characteristics, which constitutes a real threat[8]

4- **Matching module:** In this step, the input query biometric template is matched with the stored biometric template. Generally, matching is done by distance metrics such as Euclidean distance, Hamming distance, pixel counts, etc. However, recently, a learning based classifier is gaining popularity to classify the authorized and unauthorized person. A matching score is computed by finding the degree of similarity between the live and the stored biometric template. Based on the matching score, a decision is made whether the person is legitimate or not. [1]

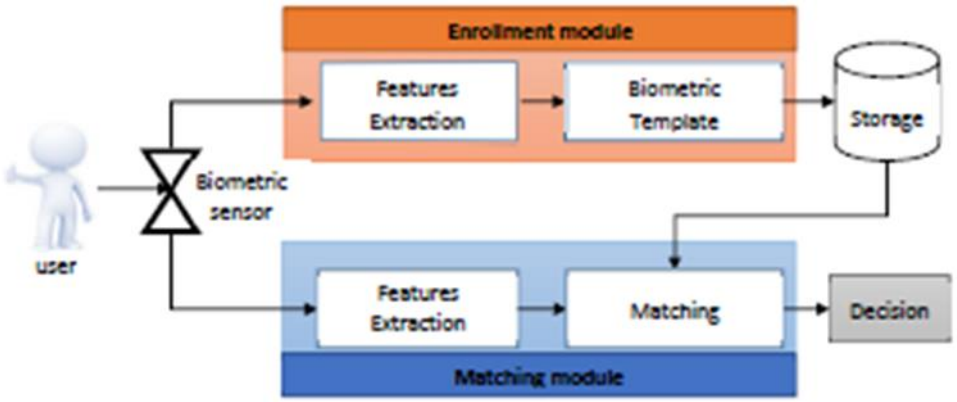

Figure1.10:A typical biometric system architecture

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?).[9]

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?). [9]

1.8- Biometrics market and applications:

Biometrics has successfully convinced wide range of applications to be adopted not only as a fundamental component in their security architecture, but as an economical tool that can lead directly or indirectly to saving costs and reducing financial risks (Nanavati,Thieme,Raj,&Nanavati, 2002). It had advanced quickly and significantly over the two decades .

Recent researches confirm that the market of biometrics would grow from 8,7 billion dollars in 2013 to nearly 27,5 billion dollars by 2019 registering an annual growth of 19,8% between 2014 and 2019. Fingerprint modality will still dominate the market as shown in (Figure 1.11). This acceleration is justified by the proliferation of the electronic services that necessitate identification, along with the rise of fraud acts and identity theft that must be fought. In addition to that, the adoption of the electronic documents especially .[8]

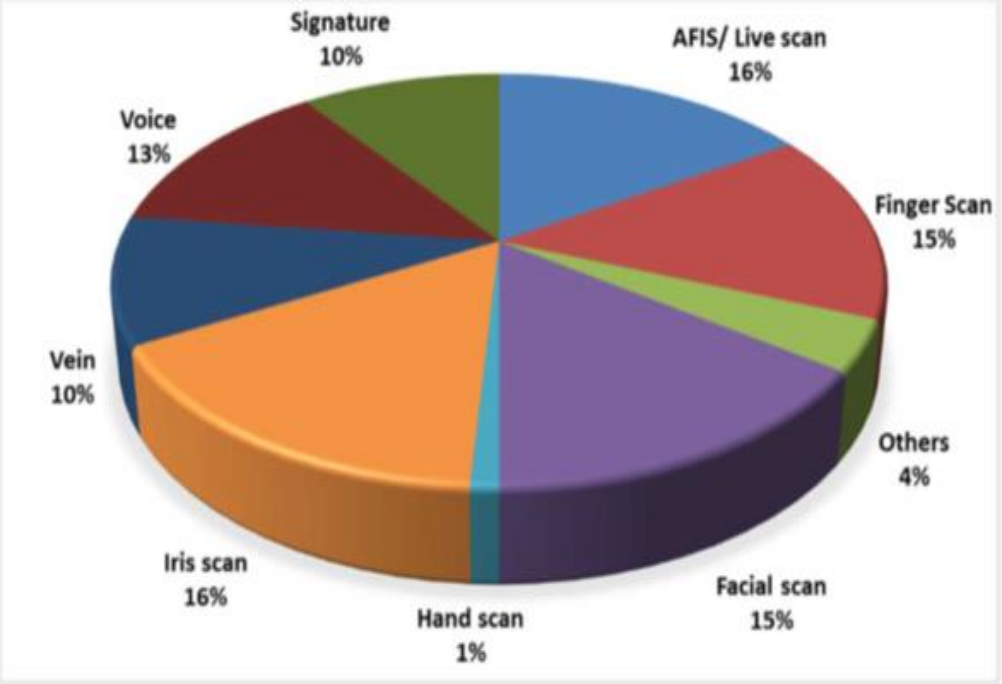

Figure 1.11: Biometrics Market by modality (2015) .

1.9- Advantages and disadvantages of biometrics :

Advantage	Disadvantage
• Quicker Authentication • Improves the Security System • Complete Control Over Access • Scalability • Flexible • Complete Data Accuracy • Less Processing time • Increased Security • Ease of work	• Intra-class variability and inter-class similarity • Segmentation • Noisy input & population coverage • System performance (error rate, speed, cost) • The individuality of biometric characteristics • Fusion of multiple biometric attributes • Scalability • Attacks on the biometric system

Table 1.2 : Advantages and disadvantages of biometrics .

1.10- Conclusion:

Through this chapter, we have introduced the concept of a biometrics, its history and its different applications .

In the next chapter we will discuss about new approach for personal authentication, using finger back surface imaging (finger knuckle) based on feature selection method.

CHAPTER 02

2 Finger knuckle print Methods

2.1- Introduction :

In recent years, finger knuckle print (FKP) identification has become an increasingly important research topic in biometric applications. The FKP refers to the inherent skin patterns that are formed at the joints on the surface of the backs of the fingers. It has been found that the FKP is highly rich in texture and can be used in the unique recognition of a person. The rich features of the FKP are a key challenge for personal recognition systems, in addition to variations in illumination and orientation and noisy sensors, making the task of identification critical .

2.2- Overview of the Finger knuckle print system :

Developing secure and effective access-control systems requires personal-identification technologies that are reliable and convenient. Hand-based biometrics exploits several internal and external features that are quite distinct in a given individual. User acceptance of hand-based biometrics systems is very high, and they are becoming more convenient and user friendly with the introduction of peg-free and touch less imaging.

The anatomy of the human hand is quite complicated. The finger-back surface—the ‘dorsum’ of the hand—can be very useful in user identification, but it has not yet attracted significant attention of researchers. In particular, the image-pattern formation from finger-knuckle bending is highly unique and thus makes this surface a distinctive biometric identifier. The anatomy of our fingers allows them to bend forward and resist backward motion. This asymmetry results in a very limited number of creases and wrinkles on their palm side. Therefore, finger-knuckle patterns are a promising avenue for further developments in touch less personal identification. [10]

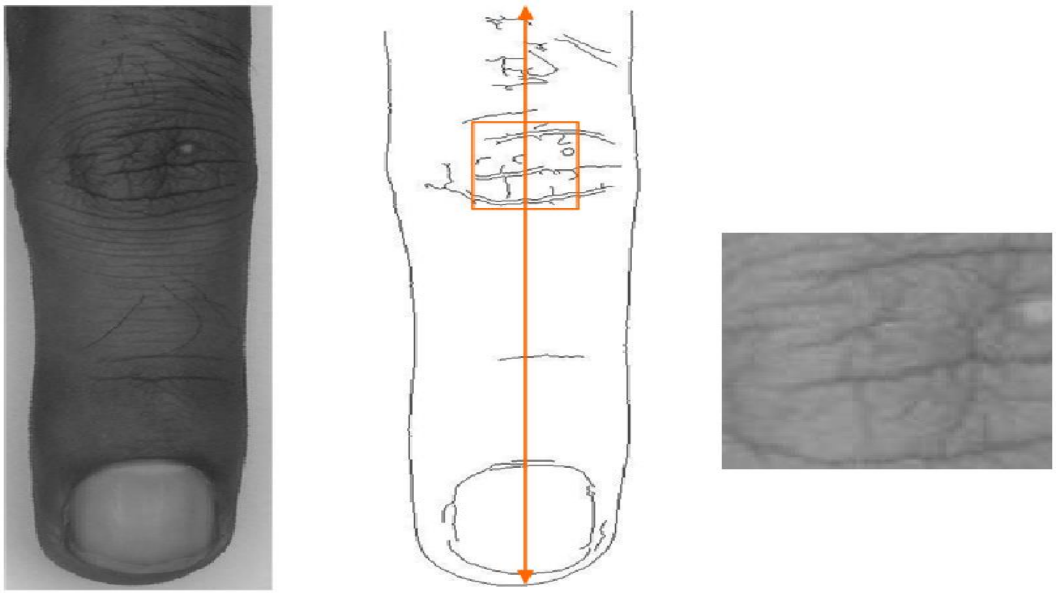

Figure 2.1: Automated extraction of finger knuckles for identification .

2 Finger knuckle print Methods

2.2.1- The FKP Recognition System :

The proposed system captures the image around the finger knuckle area of a finger directly, which largely simplifies the following data preprocessing steps. Meanwhile, with such a design the size of the imaging system can be greatly reduced, which improves much its applicability. Since the finger knuckle will be slightly bent when being imaged in the proposed system, the inherent finger knuckle print patterns ca-n be clearly captured and hence the unique features of FKP can be better exploited. For matching FKPs, we present an efficient and effective Band-Limited Phase-Only Correlation based method. Compared with the existing finger knuckle surface based biometric systems [11], the proposed system performs much better in terms of both recognition accuracy and speed.

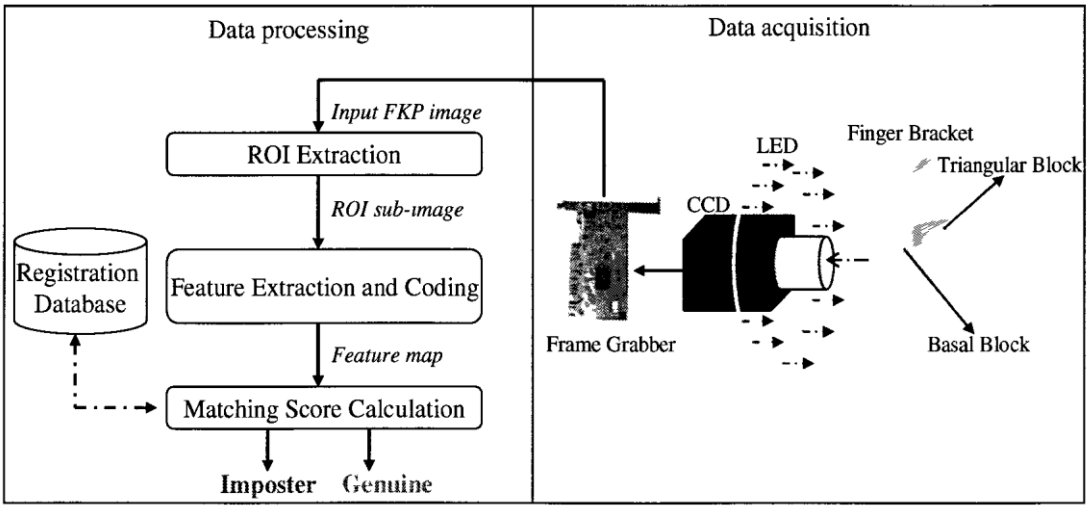

Figure 2.2 : FKP image acquisition device.

The proposed FKP recognition system is composed of an FKP image acquisition device and a data processing module. The device (referring to Figure2.2) is composed of a finger bracket, a ring LED light source, a lens, a CCD camera and a frame grabber. The captured FKP image is inputted to the data processing module, which comprises three basic steps: ROI (region of interest) extraction, feature extraction, and feature matching. Refer to Figure2.2, a basal block and a triangular block are used to fix the position of the finger joint. The vertical view of the triangular block is illustrated in Figure2.2. Figure2.3 shows a sample image acquired by the developed device.[12]

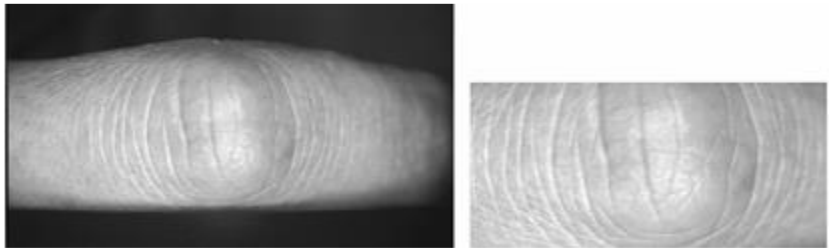

Figure2.3: Sample FKP image and the ROI image

2 Finger knuckle print Methods

A critical issue in data acquisition is to make the data collection environment as stable and consistent as possible so that variations among images collected from the same finger can be reduced to the minimum. In general, a stable image acquisition process can

effectively reduce the complexity of the data processing algorithms and improve the image recognition accuracy. Meanwhile, we want to put as little constraint as possible on the users in order for high user friendliness of the system. With the above considerations, a semi-closed data collection environment is designed in our system. The LED light source and the CCD camera are enclosed in a box so that the illumination is nearly constant. One difficult problem is how to make the gesture of the finger be nearly constant so that the captured FKP images from the same finger are consistent. In our system, the finger bracket is designed for this purpose.

Refer to Figure 2.2, a basal block and a triangular block are used to fix the position of the finger joint. In data acquisition, the user can easily put his/her finger on the basal block with the middle phalanx and the proximal phalanx touching the two slopes of the triangular block. Such a design aims at reducing the spatial position variations of the finger in different capturing sessions. The triangular block is also used to constrain the angle between the proximal phalanx and the middle phalanx to a certain magnitude so that line features of the finger knuckle surface can be clearly imaged. The angle of the triangular block is 135°. That means when the FKP sample is being collected, the person's finger is bent with an angle about 135°.

After the image is captured, it is sent to the data processing module for preprocessing, feature extraction and matching . The size of the acquired FKP images is 768x576 under a resolution about 400 dpi. Figure 2.4 shows four sample images acquired by the developed device. Example images for the same finger were captured at two different collection sessions with an interval of 56 days. We see that by using the developed system, images from the same finger but collected at different times are very similar to each other. Meanwhile, images from different fingers are very different, which implies that FKP has the potential for personal identification.

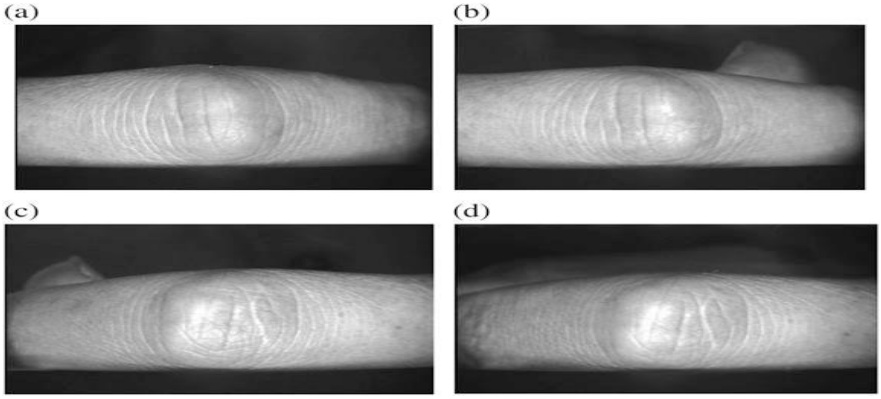

Figure 2.4: Sample FKP images acquired by the developed system. (a) and (b) are from one finger while (c) and (d) are from another finger. Images from the same finger are taken at two different sessions with an interval of 56 days

2.2.2- Database Establishment :

In order to evaluate the proposed FKP-based personal authentication system, an FKP database was established by using the developed FKP image acquisition systemFigure2.5 .

Figure 2.5: The outlook of the developed FKP image acquisition device The device is being used to collect FKP samples.

This database is intended to be a benchmark to evaluate the performance of various FKP recognition methods, and it is now publicly available at [13].The FKP images were collected from 165 volunteers, including 125 males and 40 females. Among them, 143 subjects are 20-30 years old and the others are 30-50 years old. The volunteers were students and teachers from the Hong Kong Polytechnic University and Harbin Institute of Technology.

We collected the samples in two separate sessions. In each session, the subject was asked to provide 6 images for each of the left index finger, the left middle finger, the right index finger and the right middle finger. Therefore, 48 images from 4 fingers were collected from each subject. In total, the database contains 7,920 images from 660 different fingers. The average time interval between the first and the second sessions was about 25 days. The maximum and minimum time intervals were 96 days and 14 days respectively.

2.2.3- Data Preprocessing and ROI Extraction :

2.2.3.1- Selection of the Image Resolution :

Resolution	EER(%)
200dpi	1.73
170dpi	1.41
150dpi	1.36
120dpi	1.71
100 dpi	1.92

Table 2.1: EERs obtained under different resolutions .

The resolution of original FKP images acquired in our system is about 400 dpi, which may not be optimal in terms of the accuracy and efficiency of FKP verification.

In fact, many factors, such as the storage space, the computational cost, the employed feature extraction and matching method, and the recognition accuracy, should be considered in selecting a suitable resolution of the FKP images for a more efficient biometric system. To this end, conducted a series of experiments to select the "optimal" resolution and set the selection criterion as: the minimum resolution with which a satisfying verification performance could be obtained. The verification performance was measured by the Equal Error Rate (EER), which is defined in section 1.2. The experiments were performed on a sub-dataset of the whole FKP database. In this sub-dataset, there were 120 classes, including 1,440 images. With respect to the feature extraction method, the Comp Code , was used [14, 15]. smoothed the original images by using a Gaussian kernel and then down-sampled the images to five lower resolutions:

200dpi, 170 dpi, 150 dpi, 120 dpi and 100 dpi. The experimental results are summarized in Table 2.1.

Based on the results listed in Table 2.1, it can be seen that 150 dpi is a good choice. It leads to the lowest EER, while the resolution is much smaller than the original one (400 dpi). Such a downloading step will reduce the computational cost and speed up the feature extraction and matching processes significantly. Therefore, in all of the following experiments, used the FKP images with a resolution 150 dpi .

2.2.3.2- ROI Extraction :

It is necessary to construct a local coordinate system for each FKP image. With such a coordinate system, an ROI can be cropped from the original image for reliable feature extraction. The detailed steps for setting up such a coordinate system are as fol-lows.

Step 1: determine the X-axis of the coordinate system. The bottom boundary of the finger can be easily extracted by a Canny edge detector. Actually, this bottom boundary is nearly consistent to all FKP images because all the fingers are put flatly on the basal block in data acquisition. By fitting this boundary as a straight line, the X-axis of the local coordinate system is determined.

Step 2: crop a sub-image Is. The left and right boundaries of Is are two fixed values evaluated empirically. The top and bottom boundaries are estimated according to the boundary of real fingers and they can be obtained by a Canny edge detector.

Step 3: Canny edge detection. Apply the Canny edge detector to Is to obtain the edge map IE

Step 4: convex direction coding for IE. We define an ideal model for FKP “curves”. In this model, an FKP “curve” is either convex leftward or convex right-ward. We code the pixels on convex leftward curves as “1”, pixels on convex right-ward curves as “-1”, and the other pixels not on any curves as “0”.

2 Finger knuckle print Methods

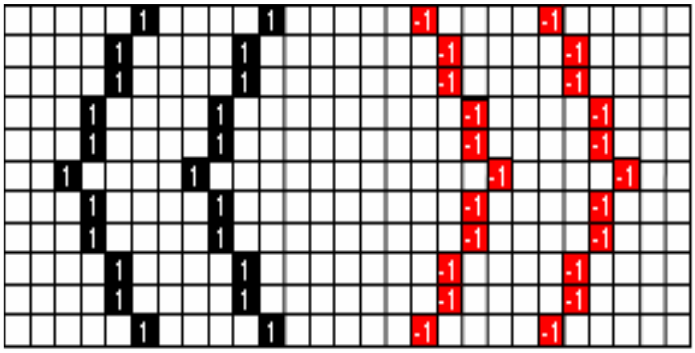

Figure 2.6 : Convex direction coding scheme.

Figure2.6 illustrates this convex direction coding scheme and the pseudo codes are presented as follows:

Convex_Direction_Coding (IE)

Output: ICD (convex direction code map)

Ymid = height of IE/2

for each IE (i, j) :

if IE (i , j) = 0

ICD (i, j) ;

else if IE (i+1, j-1) = 1 IE and (i+1, j+1) = 1

ICD (i , j) = 0 ;

else if (IE (i+1, j-1) = 1 and i<= Ymid) or (IE (i+1, j+1) = 1 and i 1> Ymid)

ICD (i, j) = 1 ;

else if (IE (i+1, j+1= 1and i<=Ymid) or(IE (i+1, j-1)= 1 and i > Ymid)

ICD (i, j) = -1;

end if

end for

Step 5: determine the Y-axis of the coordinate system. For an FKP image, "curves" on the left part of phalangeal joint are mostly convex leftward and those on the right part are mostly convex rightward. Meanwhile, "curves" in a small area around the phalangeal joint do not have obvious convex directions. Based on this observation, at a horizontal position x (x represents the column) of an FKP image, we define the "convexity magnitude" as:

$$conMag(x) = abs \sum_w I_{CD} \qquad (1)$$

where W is a window being symmetrical about the axis X = x. W is of the size d×h, where h is the height of Is. The characteristic of the FKP image suggests that con-Mag(x) will reach a minimum around the center of the phalangeal joint and this posi-tion can be used to set the Y-axis of the coordinate system. Let

$$x'_0 = \text{argmin}(\text{conMag}(x)) \qquad (2)$$

Then X =$x'_0$is set as the Y-axis.

Step 6: crop the ROI image. Now that we have fixed the X-axis and Y-axis, the local coordinate system can then be determined and the ROI sub-image IROI can be ex-tracted with a fixed size. Figure 2-3 shows an example of the extracted ROI images.

2.3- Feature extraction:

An image defined in the "real world" is considered to be a function of two real variables. 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 .

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 (ThawarArif, 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[2] .

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 AlexNet and GoogleNet algorithm and SVM , RBF, KNN classifier .

2.4- Machine Learning :

Machine learning is a field that is focused on the construction of algorithms that make predictions based on data. A machine learning task aims to identify (to learn) a

function f : X → Y that maps the input domain X (of data) onto output domain Y (of possible predictions) [16].

Functions f are chosen from different function classes, dependent on the type of learning algorithm that is being used. Mitchell (1997) defines "learning" as follows: "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E" [17]. The performance measure P tells us quantitatively how well a certain machine learning algorithm is performing. For a classification task, the accuracy of the system is usually chosen as the performance measure, where accuracy is defined as the proportion for which the system correctly produces the output. Experience E that machine learning algorithms undergo are datasets. These datasets contain a set of examples that are used to train and test these algorithms

2.5- Deep learning features:

Deep learning (DL) is a subfield of machine learning based on learning multiple levels of representations by making a hierarchy of features where the higher levels are defined from the lower levels and the same lower level features can help in defining many higher level features [18]. DL structure extends the traditional neural networks (NN) by adding more hidden layers to the network architecture between the input and output layers to model more complex and nonlinear relationships. This concept gained the researchers interest in the recent years for its good performance to become the best solution in many problems in medical image analysis applications such as image denoising, segmentation, registration and classification.[19. 20,21]

Deep Learning methods are a modern update to Artificial Neural Networks that exploit abundant cheap computation.

They are concerned with building much larger and more complex neural networks and, as commented on above, many methods are concerned with semi-supervised learning problems where large datasets contain very little labeled data.

The most popular deep learning algorithms are:

- Deep Boltzmann Machine (DBM)
- Deep Belief Networks (DBN)
- Convolutional Neural Network (CNN)
- Stacked Auto-Encoders .

There are various DL architecture, convolutional neural networks (CNN) is a common used architecture in recent years. A typical CNN architecture is a sequence of feed forward network layers. CNN architecture has an advantage of not requiring a feature extraction process before being trained. But training a CNN from scratch is a time consuming and difficult as it needs a very large labeled dataset for training

before the model is ready for classification which is not always available. It's a typical feed forward Network which the input flows from the input layer to the output layer through a number of hidden layers. Deep Neural Network (DNN) is widely used for classification or regression with success with success in many areas.

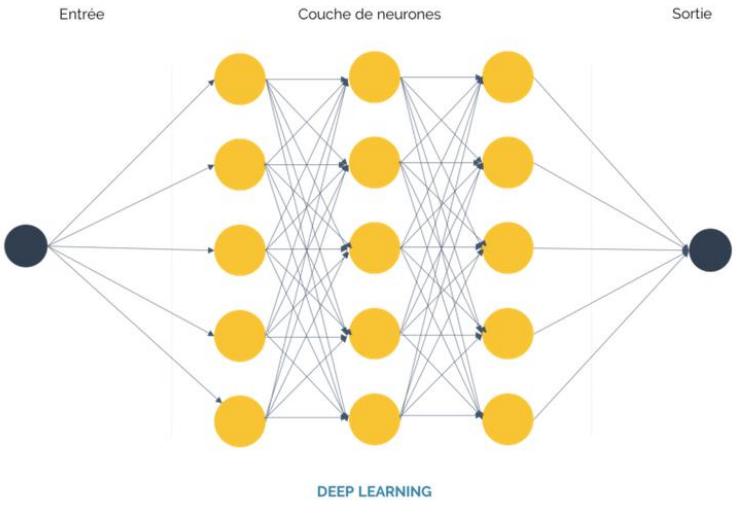

Figure2.7:DNNs architecture.

Finger Knuckle Print verification is one of the most popular approaches for personal authentication due to its high accuracy. In this study, convolutional neural networks (CNNs) along with transfer learning are exploited to extract features from Finger Knuckle print ROIs. The extracted ROIs are fed to the system, which is composed of two modules. These modules are a pre-trained CNN architecture as a feature extractor and a machine learning classifier. The experiments demonstrated that the ROI extraction module could extract the appropriate ROIs from the Finger Knuckles.

2.5.1- Conventional neural network (CNN) :

CNN is used to automatically generate features and combine it with the classifier. The architecture is inspired by AlexNet. It consists of six layers of Conv2D,ReLu,Max-pooling and fully connected layer. The dropout layer randomly drops certain number of neurons during forward pass (input to the function) and remembers the neurons that are left during the forward pass. And only updates the non-dropped during backward pass.

This avoids the over fitting during the training phase and regularization of the model It is a significantly slower operation than, say max pool, both forward and backward. If the network is deep, each training step is going to take much longer.

A novel CNN architecture specifically for FKP recognition has been designed. The batch-normalized CNN architecture is shown in Figure1, which includes 4 convolution layers and 3 fully connected layers. ‘C’ denotes the convolution layer, the max pooling layer and the full connection layer are represented by ‘MP’ and ‘FC’, respectively.

2 Finger knuckle print Methods

During the training stage, the input of the CNN is a 220 ×110 grayscale image; all the images are cropped into 110 ×110 randomly as the input of the entire network. The parameters of each layer are optimized based on multiple experimental verification. Owing to the small FKP database, the solution to avoid over fitting is crucial. Hence, to prevent the training over fitting, a dropout layer is adopted in the proposed CNN and a batch of normalized layer is added after each convolution layer.[22]

CNN configurations comprise of a multitude of hidden layers. In each layer, activation volumes are altered with the use of differentiable functions. Four principle layer types exist that are used to build CNN configurations

- **Convolutional Layer (CONV):** Convolutional filters are used to derive an activation map from the input data.
- **Rectified Linear Unit Layer (ReLU):** Filters negative values to provide only positive values for a much faster training time.
- **Pooling Layer (POOL):** Performs nonlinear down-sampling and cuts down the amount of parameters for a simpler output.
- **Fully Connected Layer (FC):** Computes the class probability scores by outputting a vector of C dimensions, with C being the number of classes. All neurons are connected to this layer

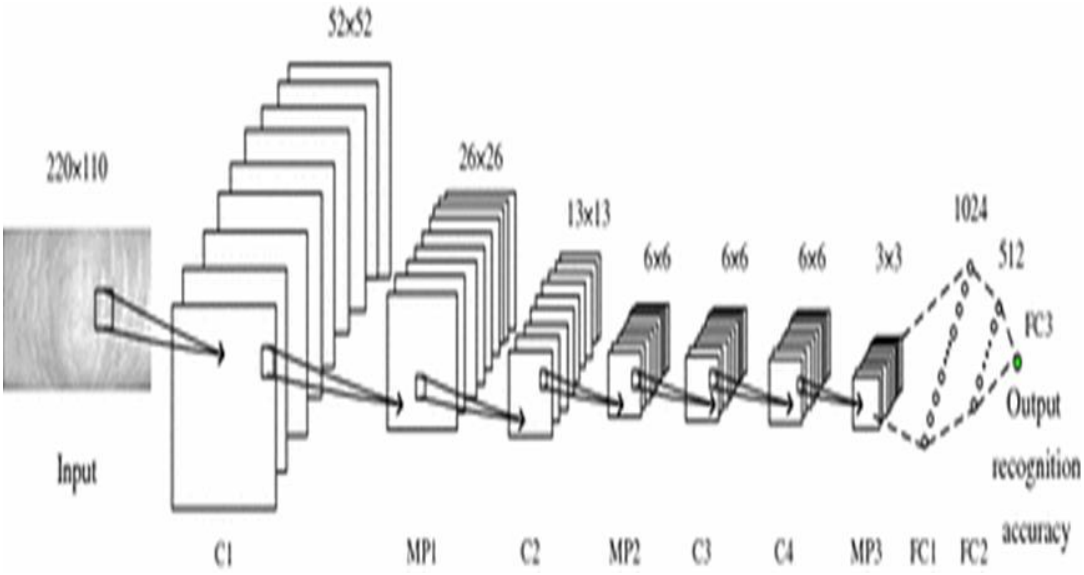

Figure2.8: Architecture of CNN

2.5.1.1- AlexNet:

AlexNet[23]was proposed by Alex Krizhevsky in 2012. It has been successfully trained on ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) dataset [24] that contains 1.2 million natural images of 1,000 different categories. It was the winner of ILSVRC 2012. Its architecture encompasses 60 million parameters,

650,000 neurons, and 630 million connections, with five convolutional layers, max-pooling layer at each three convolution layers, and three fully connected layers. The input layer takes the image size of 227 × 227.

The first convolutional layer applies 96 filter of 11x11 on the input images at stride 4 in Conv1, whereas 3 × 3 filters are applied at stride 2 in pool1. Likewise, the second convolutional layer applies 256 filters of 5 × 5. Similarly, 3 × 3 filter size is used in the third, fourth, and fifth layer with the filters of 384, 384, and 256. ReLU activation function is applied in each convolution layer. Fully connected layers are fc6 and fc7, and each has 4096 neurons. Furthermore, output layer fc8 uses softmax classifier that initiates 1000 neurons according to the classes of ImageNet.

Alexnet is also known as transfer learning model where knowledge is learnt from training large amount of datasets. It consists of 25 layers that combine a few stacks of convolutional layers and fully connected layers [25]. An illustration of the architecture of AlexNet is shown in Figure 2.9

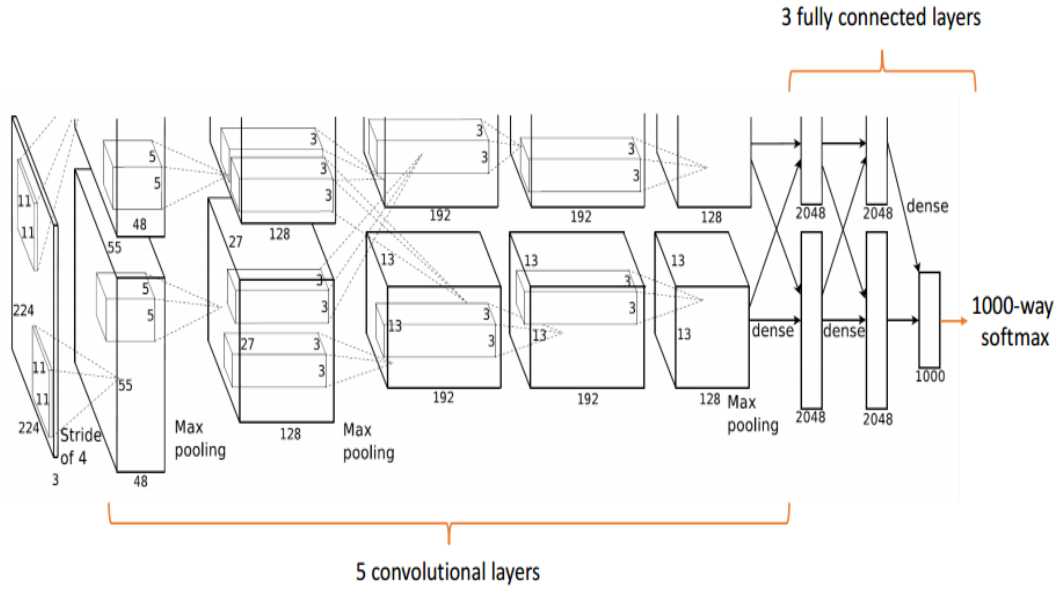

Figure 2.9 : An illustration of AlexNet layers

2.5.1.2- GoogleNet:

GoogLeNet, a 22-layer CNN and the winner of ILSVRC'14 [26], is an efficient deep neural network model designed for computer vision. When other CNN-based models are trapped in serious negative effects brought by size growth, GoogLeNet is able to significantly increase the depth and width of the network for improving performance while keeping the demand of computational workload at a

reasonable level. The key reason for such a success is the introduction of a bunch of inception modules that are usually stacked on the higher layers. The structure of an inception , where 1 × 1 convolutions are added before expensive 3 × 3 and 5 × 5 convolution as the dimension reduction modules. This approach significantly reduces

the total number of parameters in the network (GoogLeNet with 7 00 000 parameters versus AlexNet with 60 000 000 parameters) .

The initial purpose of designing this inception module is to approximate a local sparse structure of CNN by using readily available dense components (matrices) which can make efficient use of computational resources in current computing infrastructures. Moreover, in GoogLeNet, considering back propagate gradients, extra auxiliary classifiers are added onto intermediate layers, which is expected to reduce the effects of vanishing gradient [27] while providing regularization.

Googlenet achieved a top-5 error rate of 6.67% [28].This was very close to human level performance which the organizers of the challenge were forced to evaluate. As it turns out, this was actually rather hard to do and required some human training in order to perform the task. The human expert (Andrej Karpathy) was able to achieve a top-5 error rate of 5.1% (single model) and 3.6% (ensemble). The network used CNN inspired by LeNet but implemented a novel element which is dubbed an inception module. It used batch normalization, image distortions and RMSprop. This model is based on several very small convolutions in order to drastically reduce the number of parameters. Their architecture consisted of 22 layers of deep CNN but the number of parameters is reduced from 60 million (AlexNet) to 4 million (Googlenet). An illustration of the layers in GoogleNet is shown in Figure 2.10 .

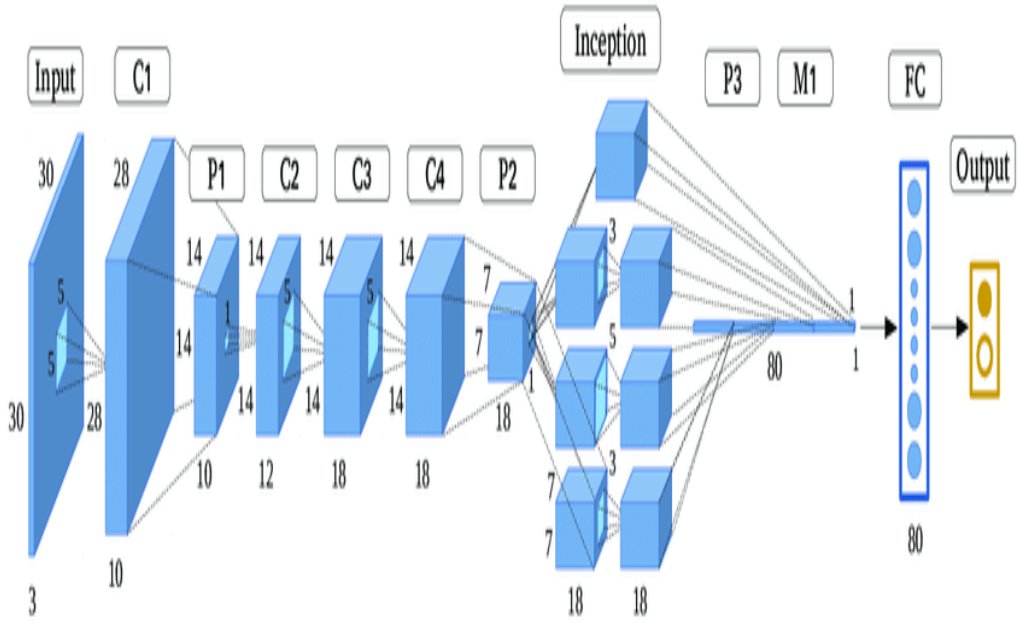

Figure 2.10: An illustration of the layers of GoogleNet

2.6- Feature Matching:

In image processing, point feature matching is an effective method to detect a specified target in a cluttered scene. Rather than detecting several objects, this approach detects a single object. For example, one may identify one particular person in a cluttered scene using this approach, but not any other person. The algorithm works by evaluating and comparing point correspondences between the reference and target images. If any part of the cluttered scene shares correspondences greater than the threshold, that part of the cluttered scene image is targeted and considered to include the reference object there

And also feature matching is a measure of similarity between the test (input) and train (template) feature vectors. The high match score can be determined by examining the match scores appertaining to all the comparisons and reporting the identity of the template corresponding to the largest similarity score. Recently, several methods have been used in this field, and in our biometric identification system we used three different types (Support Vector Machine (SVM) , k-Nearest Neighbor (KNN), and radial basis function (RBF)).

2.6.1- Support vector machine (SVM):

Support Vector Machine (SVM) is a kind of machine learning algorithm that can be used to solve problems like classification, regression, and detection. It consists in separating two or more sets of points by a hyper plane

Since the past decade, SVM has gained its popularity in various types of classification applications and has been reported as one of the best performing classification approaches. It can be used as a discriminative classifier and has been shown to be more accurate than most other classification models. The good generalization characteristic of the SVM is due to the implementation of Structural Risk Minimization (SRM) principle, which entails finding an optimal separating hyper-plane, thus guaranteeing the highly accurate classifier in most applications. Equation (3) represents the equation of a hyper-plane which can be used to partition data points in a SVM .

$$w \cdot x + b = 0 \qquad (3)$$

Figure2.11 illustrates a linearly separable case, where data points of one category (represented by "◦") and data points of another category (represented by "•") are separated by the linear optimal separating hyper-plane (the solid straight line).

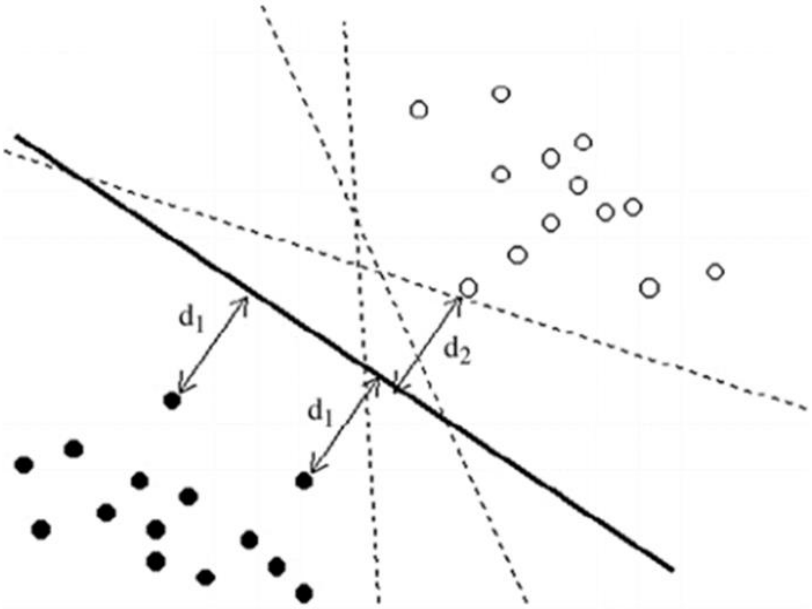

Figure2.11: Optimal separating hyper-plane

- **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 hyper plane. 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 hyper plane separating the best points. In this paper, we use the multiclass SVM .[29]

- **Normalisation 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,

$$\widetilde{D} = \frac{D - min\,(D)}{max(D) - min(D)} \qquad (4)$$

Where represent the normalized vector. However, these scores are compared, and the lowest score is selected. For perfect matching, the matching score is zero[2]

2.6.2- k-Nearest-Neighbor (KNN) :

The k-nearest-neighbor approach to classification is a relatively simple approach to classification that is completely nonparametric. Given a point X_0that we wish to classify into one of the K groups, we find the k observed data points that are nearest toX_0 . The classification rule is to assign $X_0$to the population that has the most observed data points out of the k-nearest neighbors. Points for which there is no

majority are either classified to one of the majority populations at random, or left unclassified.

The advantage of nearest-neighbor classification is its simplicity. There are only two choices a user must make: (1) the number of neighbors, k and (2) the distance metric to be used. Common choices of distance metrics include Euclidean distance, Mahalanobis distance, and city-block distance. The number of neighbors is usually selected by either cross-validation or testing the quality of the classifier on a second, test data set .

2.6.3- Euclidean distance:

The utmost famous distance applied for arithmetical data analysis is the Euclidean distance. Euclidean distance is a direct straight- line interval among two entities in the Euclidean region. While executing clustering, the Euclidean distance is considered, where if the interval between two points from the centroid is the same, but the points either in the same or opposite directions, then also they may fall into the same cluster. Euclidean distance achieves ex-cellent results when the datasets are arranged in compact groups (Mao& Jain, 1996). In spite of the fact that Euclidean distance is extraordinarily in clustering, there is a shortcoming: when two en-tities do not have uniform standards, then they may vary in distance than other pairs of entities holding a similar attribute value. The normalization of all features is a reply to this drawback

(Jain, Murty& Flynn, 1999) [30] .

Figure2.12 shows the generalized concept of Euclidean distance .

The Euclidean distance describes as :

$$E = \sqrt{(X-Y)^T(X-Y)} = \sqrt{\sum_{p=1}^{n}(X_p - Y_p)^2} \quad (5)$$

Here, ‘ X ’ and ‘ Y ’ are two classes

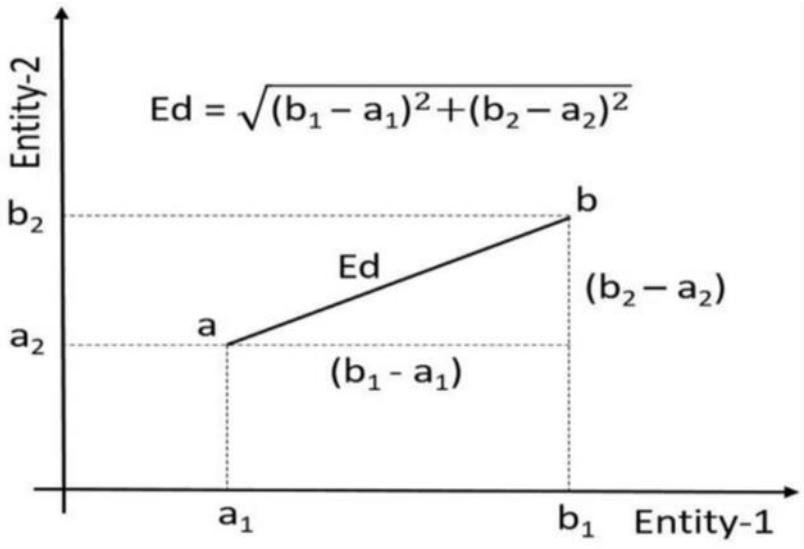

Figure 2.12: Euclidean distance between two entities.

2.6.4- Radial Basis Function (RBF) :

radial basis function (RBF) interpolation to solve the problem of constrained texture mapping. The users control the mapping process by interactively defining and editing a set of constraints consisting of 3D points picked on the surface and the corresponding 2D points of the texture. RBF is invoked to interpolate the user-defined constraints to provide an analytic parameterization of the surface. The energy-minimization characteristic of RBF also ensures that the mapping function smoothly interpolates the constraints with satisfying non-deformation properties.

2.7- Conclusion :

In this section, we gave an overview of the FKP system and deep learning method, which based by descriptor of the texture, Conventional neural network (CNN) and Support vector machine (SVM) .

CHAPTER 03

3 Experimental result and discussions

3.1- 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 AlexNet,GoogleNet in feature extraction and SVM, KNN and RBF classifier in matching setup, in unimodaldatabase the 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.

3.2- 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 3.1). Kumar et al.[31] 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.

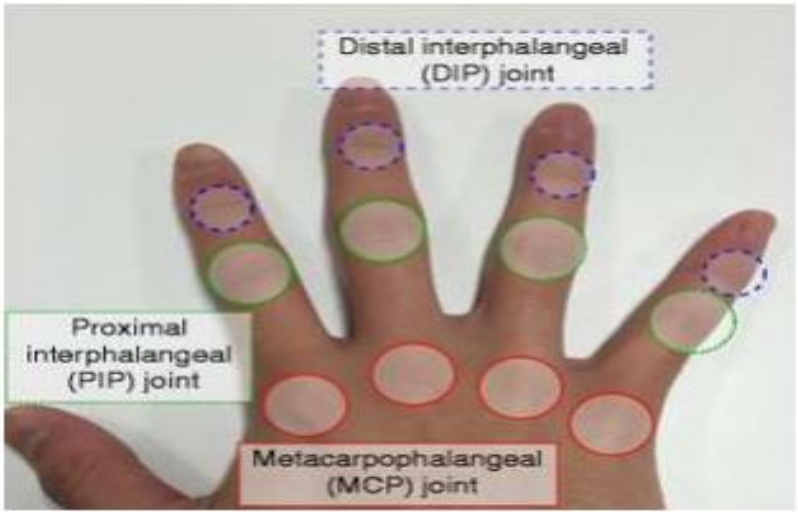

Figure 3.1:A taxonomy of finger knuckle joints: Blue-colored circles indicate distal interphalangeal (DIP) joints, green-colored circles indicate proximal interphalangeal (PIP) joints, and red-colored circles indicate metacarpophalangeal (MCP) joints.

3 Experimental result and discussions

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 [32]. 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 for the enrollment and the same for the identification. Therefore, 48 images from 4 fingers were collected from each subject.

3.3- Experimental protocol :

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

- **First step:** we choose the best parameter between AlexNet and GoogleNet feature extraction algorithm using KNN, SVM and RBF feature matching.
- **Second step:**we compare the best result between the three feature matching algorithmsusing AlexNet or GoogleNet.
- **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 for that we use the best result found in second step in multimodal tests.

3.4- 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 AlexNet or GoogleNetwhich the characteristics of an FKP image are effectively and clearly demonstrated by AlexNet or GoogleNet, where a different representation can be displayed for several levels to give high-level properties and using SVM,KNN and RBF 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[33] .

3 Experimental result and discussions

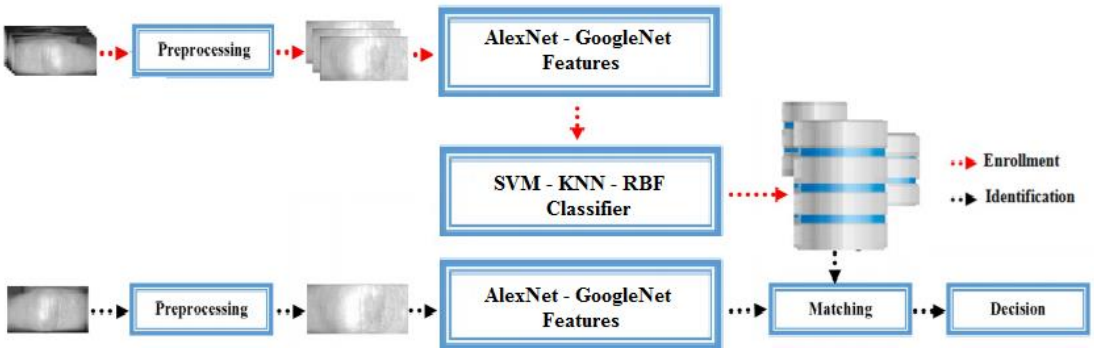

Figure3.2: Multimodal finger print identification system.

3.5- Biometric Performance Measures:

In order to examine and compare the performance of biometric technologies, there are some key measures identified below that are usually used to test such systems .

3.5.1 -False Acceptance Rate (FAR):

The FAR is also known as “Type I error”. FAR is a measure the percentage of impostors that are incorrectly accepted as genuine users. As almost all biometric systems aim to attain correct identity authentication, this number should be as low as possible .

3.5.2 -False Rejection Rate (FRR):

The FRR is also known as “Type II error”. FRR is a measure of the percentage of genuine users that are incorrectly rejected. In order to minimize inconveniences or embarrassment to the genuine user, this number should also be low as possible. In general, this error is more acceptable because the user can make a second attempt .

3.5.3 -Equal Error Rate (EER):

FAR and FRR are related. A stringent requirement for FAR (as low as possible) will inadvertently increase the FRR. The point where the FRR is equal to FAR is given by this measure. Lowering the rate of EER will increase the performance of the system as it indicates a good balance in the sensitivity of the system. (Yun 2002)

3.5.4 -Crossover Error Rate (CER):

A comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR.The lower the CER, the more accurate and reliable the biometric device.

Usually FRR and FER used to rate biometric accuracy. Both methods used to check the system’s ability to allow limited entry to authorized users. However, these measures vary significantly, depends upon how you adjust the sensitivity of the mechanism that matches the biometric. For example, you can require a tighter match between the measurements of hand geometry and the user’s template (increase the sensitivity).This will probably decrease the false-acceptance rate, but at the same time

can increase the false-rejection rate. So be careful to understand how vendors arrive at quoted values of FAR and FRR.

Because FAR and FRR are interdependent, it is more meaningful to plot them against each other, as shown in Figure1.11 . Each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate. The lower the CER, the more accurate the system would be. Generally, physical biometrics is more accurate than behavioral biometrics. [8]

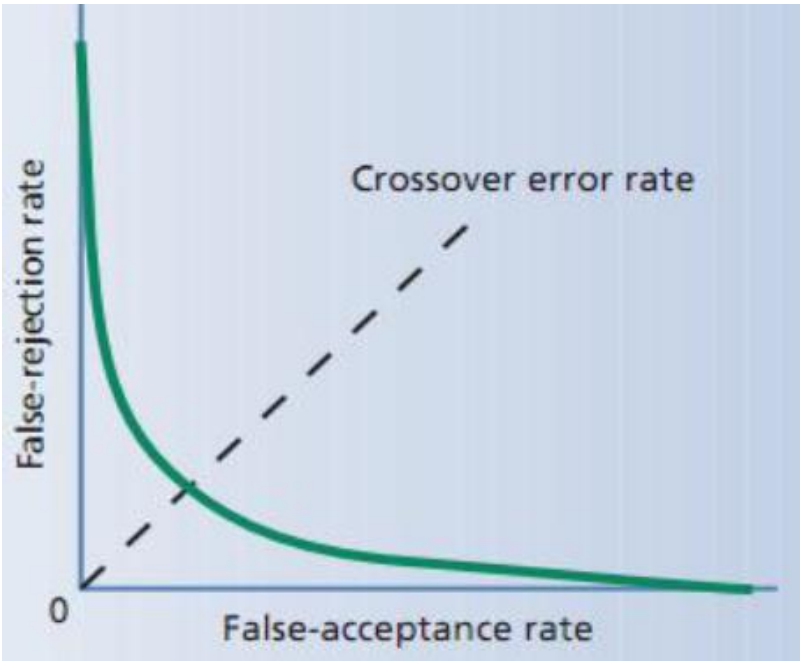

Figure3.3: Crossover error rate attempts to combine two measures of biometricaccuracy .

3.6- Unimodal identification system results :

A unimodal (or single) biometric system is a system that uses a single biometric trait [34-35] , or one source of information for verification or identification[36]. Unimodal systems have said to have improved steadily in accuracy and reliability however, they often suffer from problems in the enrollment process because of non-universal biometric traits, spoofing and lack of accuracy due to noisy data as stated earlier. Furthermore, unimodal biometric systems achieve less desired performances in real world applications. Hence, a method to solve these issues is making use of a multimodal biometric authentication system [37]. The problems associated with unimodal biometric systems are discussed further. Table 1 shows the performance of the various biometric sensing systems .

3 Experimental result and discussions

1- Feature matching based on SVM

- **a-Using AlexNet feature selection**

Finger	EER	TO	ROR	RPR
LIF	0,099	0,69	99,89	3
LMF	0,092	0,706	99,79	8
RIF	0,1016	0,634	99,56	22
RMF	0,062	0,78	99,69	9

Table 3.1: Result of simulation SVM –AlexNet

The table 3.1 illustrates the resultsof unimodal system using AlexNet feature selection and SVM classifier, in this table we note that:

- **Open set:**All results are good with a small error value also indicate thatthe performance of RMF is better than LIF, LMF, and RIF
- **Closed set:**In term of ROR all results are good and indicate that LIF performance is better than LMF, RIF, and RMF.

- **b-Using Google Net feature selection**

Finger	EER	T0	ROR	RPR
LIF	0,1768	0,8	98,28	47
LMF	0,202	0,71	99,29	11
RIF	0,38	0,686	98,48	65
RMF	0,101	0,769	98,48	78

Table 3.2: Result of simulation SVM –GoogleNet

The tables 3.2 illustrate the result of unimodal system using GoogleNet feature selection and SVM classifier in this table we note that:

- **Open set:**All results are good with a small error value also indicate that the performance of RMF is better than LIF, LMF, and RIF
- **Closed set:**In term of ROR all results are good and indicate that LMF performance is better than LIF, LMF and RIF,

Comparing the result of the two methods AlexNet and GoogleNet found AlexNet give a good result in both open set and closed set

3 Experimental result and discussions

2- Feature matching based on KNN :

- **a-Using AlexNet feature selection :**

Finger	EER	T0	ROR	RPR
LIF	0.058	0,1062	99,596	4
LMF	0.1010	0,1432	99,19	67
RIF	0.276	0,177	98,989	27
RMF	0.2020	0,1987	99,596	65

Table 3.3: Result of simulation KNN –AlexNet

The table 3.3 illustrates the results of unimodal system using AlexNet feature selection and KNN classifier , in this table we note that:

- **Open set:**All results are good with a small error value also indicate that the performance of LIF is better than RIF, LMF, and RMF
- **Closed set:**In term of ROR all results are good and indicate that RIF performance is better than LIF, LMF, and RMF.

- **b-Using GoogleNet feature selection :**

Finger	EER	T0	ROR	RPR
LIF	0.9090	0,124	94,44	94
LMF	0.642	0,1374	96,16	42
RIF	1.01	0,110	96,36	110
RMF	0.668	0,1271	96,96	98

Table 3.4: Result of simulation KNN –GoogleNet .

The table 3.4 illustrates the results of unimodal system using AlexNet feature selection and KNN classifier , in this table we note that:

- **Open set:**All results are good with a small error value also indicate that the performance of LMF is better than RIF, RMF, and LIF
- **Closed set:**In term of ROR all results are good and indicate that RMF performance is better than LIF, LMF, and RIF.

Comparing the result of the two methods AlexNet and GoogleNet found AlexNet give a good result in both open set and closed set

3- Feature matching based on RBF :

- **a-Using AlexNet feature selection :**

Finger	EER	T0	ROR	RPR
LIF	0	0,942	100	1
LMF	0,303	0,675	98,88	96
RIF	0,2	0,636	99,39	79
RMF	0,003	0,828	99,89	3

Table 3.5: Result of simulation RBF –AlexNet

The table 3.5 illustrates the results of unimodal system using AlexNet feature selection and RBF classifier , in this table we note that:

- **Open set:**All results are good with a small error value also indicate that the performance of LIF is better than RIF, LMF, and RMF
- **Closed set:**In term of ROR all results are good and indicate that LIF performance is better than LMF, RIF, and RMF.

- **b-Using GoogleNet feature selection**

Finger	EER	T0	ROR	RPR
LIF	1,21	0,726	93,13	71
LMF	1,56	0,714	89,19	147
RIF	0,859	0,727	95,35	61
RMF	0,564	0,763	95,95	55

Table 3.6: Result of simulation RBF –GoogleNet

The table 3.6 illustrates the results of unimodal system using AlexNet feature selection and RBF classifier, in this table we note that:

- Open set:All results are good with a small error value also indicate that the performance of RMF is better than LIF, LMF, and RIF
- **Closed set:**In term of ROR all results are good and indicate that RMF performance is better than LIF, LMF, and RIF.

Comparing the result of the two methods AlexNet and GoogleNet found AlexNet give a good resultin both of open set and closed set.

- **Unimodal results:**

3 Experimental result and discussions

By using different feature extraction (AlexNet,GoogleNet) with different classifier methods (SVM, KNN, RBF) found AlexNet give a good results in all classifier methods. For more details found

SVM give a good result in LMF and RIF

RBF give good results in LIF and RMF

3.7- Multimodal identification system results :

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 . A typical example is the issue of worn fingerprints that may result in error. In a multimodal biometric system such error or failure may not seriously affect an individual because other biometric technology systems are employed. Hence, the failure to enroll rate is reduced in a multimodal system, which is one of its major advantages [38-39] .

3.8- Levels of fusion in multimodal biometric system :

When we employ the data from any of the modules discussed i.e. 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 [40-41] .

In our study we interest about matching score level fusion, this involves the joining of identical scores produced by a matching module for each input feature and template biometric feature vector within the database [see Figure 3.2]. The feature levels are processed separately rather than combining them and an individual matching score is derived, depending on the accuracy of each biometric channel composite matching score that can be achieved by fusing the matching level that is further sent to the decision level[42]

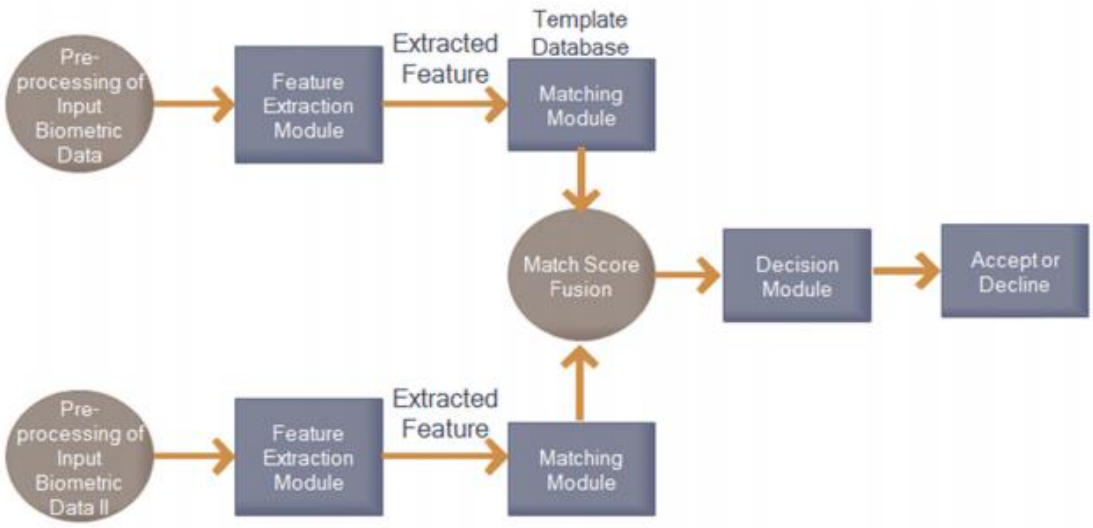

Figure 3.4: Process of Fusion at the Matching Score Level .

3 Experimental result and discussions

3.9- Methods of fusion :

There is various fusion methods used in multimodal biometric systems. Fusion methods can be divided into three categories namely: Classification based method, Estimation-based method and Rule-based method, in our study we focused on Rule-based method.

3.9.1- C–based fusion method :

Studies have revealed that a theoretical framework has been developed for merging the evidence collected from various classifiers using methods such as sum, product, max and min rules. These methods are also called unsupervised methods of fusion as there is no training process because learning rules are most suitable for physical applications that work for pre-decided target marks. Based on this theory, the posterior probabilities obtained from matching scores of real or fake identities can be fused using sum, product, max and min rules [43] .

a- Sum rule :

This is seen as one of the most effective rules as it eliminates the issue of noise that could lead to difficulty during classification. In the sum rule, to obtain the final score, transformed scores of every class are added together to obtain the final score.

b- Product rule :

This rule yields fewer results compared to the sum rule, as it is based on the statistical independence of the feature vectors.

c- Max rule :

Here, the max rule approximates the average of the posterior probability by the maximum value of the input pattern.

d- Min rule :

In the min rule, a minimum posterior probability is collected from of all classes.

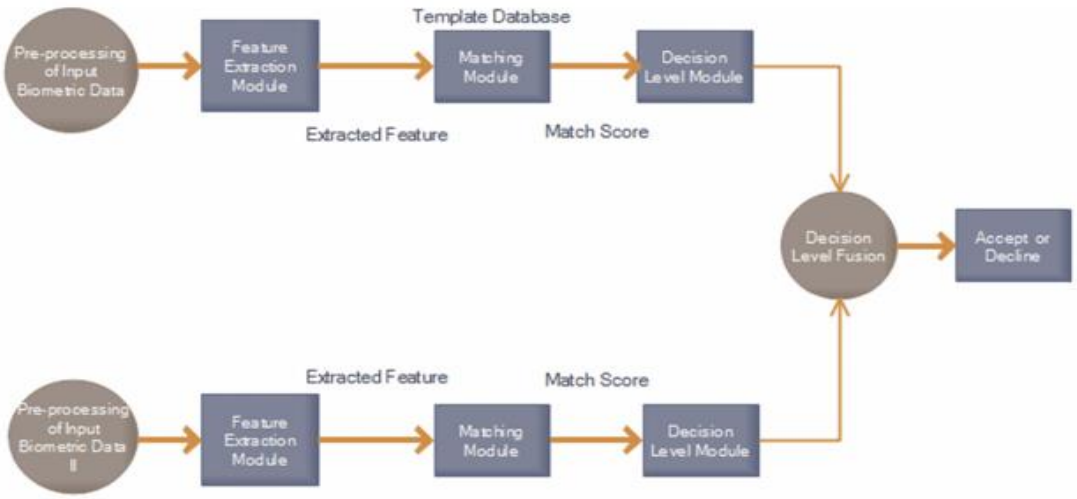

Figure 3.5: Process of Fusion at the Decision Level .

In our work, we use rule-based technique for fusing the scores produced by the different unimodal identification systems using AlexNet feature selection and SVM classifier. Thus, maximum rule (MAX), minimum rule (MIN), sum rule (SUM) and product rule (PROD) are used.

3 Experimental result and discussions

It is noted that, there are three different combinations of fingers for the fusion purpose, the two fingers for the same hand (LIF-LMF and RIF-RMF) and the four fingers (LIF-LMF-RIF-RMF for simplified it is noted ALL). Also, in these experiments, the results obtained for the identification tests are given in terms of EER and ROR in tables bellow [44] .

- **Open-set**

COMBINATION	SUN		PROD		MIN		MAX	
	ERR	T0	ERR	T0	ERR	T0	ERR	T0
LIF-LMF	0	0,892	0	0,839	0	0,94	/	/
RIF-RMF	0	0,799	0	0,519	0	0,882	/	/
ALL	0	0,659	0	0,128	0	0,476	/	/

Table 3.7: Performance of multimodal open-set identification system (fusion matching score level fusion) .

The experimental results for the open-set identification mode, respecting all combinations and fusion rules, are presented, as EER, in Table 3.7.The results in Table 3.7 show that, generally, the use of fusion resulted in perfect performance,Moreover, it is observed that theall combination (LIF-LMF,RIF-RMF and ALL)with SUM,PRODand MIN rules successfully reduces the EER to zero for the fused biometrics.

- **Closed-set**

COMBINATION	SUN		PROD		MIN		MAX	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
LIF-LMF	100	1	100	1	100	1	99,39	2
RIF-RMF	100	1	100	1	100	1	100	1
ALL	100	1	100	1	100	1	99,39	2

Table 3.8: Performance of multimodal Closed-set identification system (fusion matching score level fusion)

The experimental results for the closed-set identification mode, respecting all combinations and fusion rules, are presented, as ROR, in Table 3.8.The results in Table 3.8 show that, generally, the use of fusion resulted in perfect performance,Moreover, it is observed that theRIF-RMF combination is equal to 100% with all rules. For LIF-LMF and ALL give good results 100% in SUN, PROD and MIN,except the MAX rule give a good result 100% with RIF-RMF and 99.39 with LIF-LMF and ALL.

3 Experimental result and discussions

3.10- Conclusion :

In this chapter, we have designed a biometric recognition system based on the fusion of FKP modalities. Fusion at the matching-score level improves the performance of the system. A database of 165 persons was used for testing the system. The experimental results showed that information fusion at the matching score level improves the results of the identification. The obtained results showed that the proposed system has thecapacities to be used in the environments that require a high security.

General conclusion

General conclusion

Biometrics is a promising and exciting area, where different disciplines meet and provide an opportunity for a more secure and responsible world. There are a number of popular biometrics mechanisms currently deployed, some with strong histories, and some relatively new mechanisms. Each mechanism has its own strengths and weaknesses. When properly applied, biometrics can be used to combat fraud, and ensure that timekeeping systems are honest and accurate. Using one biometric feature can lead to good results, but there is no reliable way to verify the classification. To achieve robust identification and verification two different biometric features can be combined. A multimodal biometrics can provide a more balanced solution to the security and convenience requirements of many applications recent advances in biometric technology have resulted in increased accuracy at reduced costs; biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions .

The work presented in this dissertation is provides results obtained on FKP based identification system using the combination of multiple fingers and by using the AlexNet technique for feature extraction process and SVM classifer for identification process. For that purpose, the fusion of the sub-systems outputs is carried out at matching score level. The proposed schemes are evaluated using the FKP database from the Hong Kong polytechnic university (PolyU) which consists of FKP images from LIF, LMF, RIF and RMF fingers. Experimental results have shown that the combination of four fingers images performs better when compared against the individual finger and other combinations for both identification modes resulting in an EER of 0.000% for open-set identification and a ROR of 100% for closed-set identification. Experimental results also show that the fusion at matching score level gives an excellent result (efficiency) than the fusion at feature level, this rate is very interesting what makes our reliable system where it meets the objective that we set at the start.

Bibliography

Bibliography

[1] Kaur G, Verma C K. 2014. Comparative analysis of biometric modalities. International Journal of Advanced Research in Computer Science and Software Engineering, 4(4): 603-613.

[2] Mokadem A .2018. Efficient person identification by Finger-Knuckle-Print based on Discrete Cosine Transform Network . Master Academic Systems Of Communications .UnivOuargla, 4-37p.

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

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

[5] Raphael D E, Young J R. 1974. Automated Personal Identification, Palo Alto Calif.: SRI International.

[6] Jain A K, Bolle R, Pankanti, S. 2006. Biometrics: personal identification in networked society, Springer Science & Business Media, 479.

[7] Ahmed A A. 2019. Future Effects and Impacts of Biometrics Integrations on Everyday Living. Al-Mustansiriyah Journal of Science, 29(3): 139-144.

[8] BELHADJ.F.2017.Biometric system for identification and authentication. Doctoral dissertation .p-14 .

[9] Sareen, P. 2014. Biometrics—introduction, characteristics, basic technique, its types and various performance measures. Int J Emerg Res Manag Technol, 3: 109-119.

[10] Kumar A, Ravikanth C. 2009. Personal authentication using finger knuckle surface. IEEE Transactions on Information Forensics and Security, 4(1): 98-110.

[11] Woodard D L, Flynn P J. 2005. Personal identification utilizing finger surface features. In: Proc. CVPR, 2: 1030-1036.

[12] Zhang L, Zhang L, Zhang D, Guo Z. 2012. Phase congruency induced local features for finger-knuckle-print recognition. Pattern Recognition, 45(7): 2522-2531.

[13] Zhang L, Zhang L, Zhang D and ZhuH. 2010.PolyU Finger-Knuckle-Print Database.Online finger-knuckle-print verification for personal authentication. Pattern recognition, 43(7), 2560-2571

[14] Kong A. ZhangD. 2004. "Competitive coding scheme for palm-printnverification", in Proc. ICPR: 520-523.

[15] Zhang L, Zhang L, Zhang D. 2009. "Finger-knuckle-print: a new biometric identifier", in Proc. ICIP: 1981-1984.

[16] BekkermanR, BilenkoM. LangfordJ. 2012. Scaling Up Machine Learning, Cambridge University Press.

[17] Mitchell T. 1997. Machine Learning. McGraw Hill.

[18] Tharani S, Yamini C. 2016. Classification using convolutional neural network for heart and diabetics datasets. Int J Adv Res Comp CommunEng, 5(12):417e22.

[19] Litjens G, Kooi T, Bejnordi BE, Setio AA, Ciompi F, Ghafoorian M. 2017. A survey on deep learning in medical image analysis. Med Image Anal, 42:60- 88.

Bibliography

[20] Ravì D, Wong C, Deligianni F, Berthelot M, Andreu-Perez J, Lo B. 2017. Deep learning for health informatics. IEEE J Biomed Health Inf, 21(1):4e21.

[21] Anuse A, Vyas V. 2016. A novel training algorithm for convolutional neural network. ContrIntell Syst, 2(3):221e34.

[22] Zhai, Y, Cao H, Cao L, Ma H, Gan J, Zeng J, WangJ. 2018. A novel finger-knuckle-print recognition based on batch-normalized CNN. In Chinese conference on biometric recognition: 11-21 pp.

[23] Mohsen H, El-Dahshan A S, El-Horbaty E S M, Salem M A B. 2018. Classification using deep learning neural networks for brain tumors. Future Computing and Informatics Journal, 3(1) : 68- 71.

[24] KrizhevskyA, SutskeverI, HintonG E. 2012. ImageNet classification with deep convolutional neuralnetworks. In Advances in Neural Information Processing Systems: 1097–1105.

[25] Russakovsky O, Deng J, Su H, Krause J, Satheesh S, Ma S, Huang Z, Karpathy A, Khosla A, Bernstein M. 2015. Imagenet large scale visual recognition challenge. Int. J. Comput. Vis. 115(3) : 211–252

[26] Dubey S R, Jalal A S. 2012. Detection and Classification of Apple Fruit Diseases

[27] Szegedy C. 2015. “Going deeper with convolutions,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR): 1–9.

[28] Sa I, Ge Z, Dayoub F, Upcroft B, Perez T, Mc Cool C. 2016. Deepfruits: A fruit detection system using deep neural networks. Sensors (Switzerland), 16(8).

[29] DericheM. 2008. "Trends and Challenges in Mono and Multi biometrics," presentedat the Image Processing Theory, Tools and Applications,First Workshops on, Sousse: 1-9.

[30] Patel S P., Upadhyay S H. 2020. Euclidean distance based feature ranking and subset selection for bearing fault diagnosis. Expert Systems with Applications, 154: 113400.

[31] Amirthalingam G. 2013. "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues, 10(5): 234-241.

[32] El-Abed M, Charrier C. 2012. "Evaluation of Biometric Systems", New Trends and Developments in Biometrics: 149 – 169.

Bibliography

[33] Mokadem Amina Efficient person identification by Finger-Knuckle-Print based on Discrete Cosine Transform Network 2018 .

[34] S. Venkatraman and I. Delpachitra, ‘‘Biometrics in banking security: A case study,’’ Inf. Manage. Comput. Secur., vol. 16, no. 4, pp. 415–430, 2008.

[35] A. Drygajlo, ‘‘Multimodal biometrics for identity documents and smart cards: European challenge,’’ in Proc. 15th Eur. Signal Process. Conf., Sep. 2007, pp. 169–173.

[36] H. Saevanee, N. Clarke, and S. Furnell, ‘‘SMS linguistic profiling authentication on mobile device,’’ in Proc. 5th Int. Conf. Netw. Syst. Secur. (NSS), Sep. 2011, pp. 224–228.

[37] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, ‘‘‘A study of users’ acceptance satisfaction biometric systems,’’ in Proc. IEEE Int. Carnahan Conf. Secur. Technol.(ICCST), Oct. 2010, pp. 170–178.

[38] 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.

[39] 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.

[40] 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.

[41] X. Zhao and L. Du, ‘‘Feature points adjusting based realistic 3D face synthesizing,’’ in Proc. Int. Symp. Intell. Multimedia, Video Speech Process., Oct. 2004, pp. 254–257.

[42] A. Ross and A. K. Jain, ‘‘Multimodal biometrics: An overview,’’ in Proc. 12th Eur. Signal Process. Conf., Sep. 2004, pp. 1221–1224.

[43] M. Soltane, N. Doghmane, and N. Guersi, ``Face and speech based multimodal biometric authentication," Int. J. Adv. Sci. Technol., vol. 21, no.6, pp. 41_56, 2010.

[44] A.Meraoumia,M.Korichi ,S.Chitroub and A.Bouribane ‘‘ Finger-Knuckle-Print Identification Based on Histogram of Oriented Gradients and SVM classifier. Conf., · November 2015, pp. 5–6.

[45] Usha K, Ezhilarasan M. 2016. “Personal Recognition using Finger KnuckleShape Oriented Features and Texture Analysis", Journal of King SaudUniversity, Computer, and Information Sciences, 28(4): 416-431.

[46] Damon L, Woodard, Patrick Flynn J. 2005. “Finger surface as a BiometricIdentifier”, Computer Vision and Image Understanding, 100(3): 357-384.

[47] Gao G, Zhang L, Yang J, Zhang L, Zhang D. 2013. “Reconstruction Based Finger-Knuckle-PrintVerification With Score Level Adaptive Binary Fusion”, IEEE Transactions on Image Processing,22(12).

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, AlexNet, GoogleNet for feature extraction and Support Vector Machine (SVM) classification ,k-Nearest-Neighbor (KNN), Radial Basis Function (RBF) methods.

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 multimodal 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, AlexNet, GoogleNet , SVM , KNN, RBF , unimodal , multimodal.

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, AlexNet et GoogleNet pour l'extraction et la classification de débogage SVM (support machine vectorielle), méthodes k-Nearest-Neighbor (KNN), fonction de base radiale (RBF).

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, FBR , KNN, SMV , monomodal, multimodal, SVM

ملخص

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 الإصبع من خلال واصف نسيج جديد ، AlexNet و GoogleNet ، دعم آلة متجه ، k- أقرب الجار وظيفة الأساس الشعاعي.

يعتبر مفصل الإصبع إحدى السمات البيومترية الناشئة. وقد وجد أن بصمة مفصل الإصبع 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 .