kasdi Merbah University of OUARGLA

Faculty of new Information and
telecommunication Technologies

Department Of :
Electronic and Telecommunication

MASTER

Domain: Telecommunication

Field : Telecommunication system

Submitted by: NAAM RANIA et NAAM IMANE

Theme:

Finger knuckle print using ResNet 50 method

Evaluation Date: 21/06/2021

Before the Jury:

Dr.LATI . A	MCA	President	UKM Ouargla
Dr. BENSID .K	MCB	Supervisor	UKM Ouargla
Dr. BENLAMOUDI .A	MCB	Examiner	UKM Ouargla

Résumé

Ces derniers temps, la preuve de distinction individuelle programmée devient une nécessité importante dans les applications d'assortiment, par exemple, le contrôle d'accès, les systèmes de surveillance et les bâtiments physiques. La biométrie, qui gère l'identification des individus en fonction de leurs caractéristiques physiques ou comportementales, est apparue comme une puissante technologie d'identification programmée, qui offre plus de propriétés et quelques avantages sur la sécurité habituelle. Finger-Knuckle-Print (FKP) est une caractéristique biométrique importante. Qui donne l'unicité, la force et la capacité de reconnaissance élevée.Dans notre travail, un réseau résiduel (ResNet) a été utilisé pour séparer les attributs discriminants de la méthodologie FKP. Le système biométrique unimodal présente des problèmes tels que l'information des capteurs bruyants, la non-universalité, l'absence d'individualité, l'absence de représentation invariante et la vulnérabilité au contournement. Ainsi, pour vaincre ces inconvénients, un système biométrique multimodal est utilisé. Nos résultats de test, utilisant la base de données FKP (PolyU), présentent le meilleur système d'identification basé sur FKP proposé.

MOTS CLÉs:Biométrie , FKP, extraction des caractéristiques , identification , ResNet, ResNet 50, unimodal , multimodale, fusion .

Lately, programmed individual distinguishing proof is turning into a significant necessity in assortment applications, for example: access control, surveillance systems and physical buildings. Biometrics, which manages identification of individuals based on their physical or behavioral features, has been arising as a powerful programmed ID technology, which offers more properties and a few benefits over the customary security. Finger-Knuckle-Print (FKP) is one significant biometric feature. It gives uniqueness, strength and high recognize capacity. In our work,a residual network (ResNet) technique is utilized to separate the discriminant attributes of the FKP methodology. The unimodal biometric system that has some issue like boisterous sensor information, non-universality, absence of individuality, absence of invariant portrayal and vulnerability to circumvention. So for conquering these disadvantages, multimodal biometric system are utilized. Our test results, utilizing FKP database (PolyU), exhibit the best of the proposed FKP based identification system.

KEY WORDS: Biometrics, FKP, Feature extraction, Identification, ResNet,ResNet-50 , multimodal, fusion.

Contents

List of figures

List of Tables

List OF abbreviation

ADN:	Deoxyribonucleic Acid
DBF:	Directional Filter Bank
IBG:	International Biomatric Group
EER:	Equal Error Rate
FAR:	False Acceptance Rate
FRR:	False Rejection Rate
FKP:	Finger Knuckle Print
LED:	Light-Emitting Diode
LIF:	Left Index Fingers
LMF:	Left Middle Fingers
RIF:	Right Index Fingers
RMF:	Right Middle Fingers
ROI:	Region Of Interest
ROR:	Rank One Recognition
RPR:	Rank of Perfect Recognition
ReLU:	Rectified linear unit

General Intrduction

The biometrics is a term that we hear more and more about in everyone's life the days. While many applications today use biometrics, the which corresponds to the largest deployment is the implementation, planned for 2009 biometric passports using the face and fingerprint for the ID issuance and screening. However, biometrics is not really new[1]. Its appearance dates back to the 19th century, with the first studies then called anthropometry.

The authorities then utilized fingerprints to identify the individuals. This police usage has never been abandoned, and fingerprints are still utilized for criminal identification (now automatically with computer processing). Biometrics suffers from this police image and finds it difficult to get public acceptance for other sorts of applications.That said, biometrics is no longer limited to fingerprints and criminal identification. Many modalities are now used for applications to control access to premises or personal objects. Examples include the face, voice, signature, iris or hand shape, and others are being studied such as the gait, the shape of the ear, or the dynamics of keyboard typing and finger joints.

Feature extraction is the process of generating a new, smaller collection of features that nevertheless captures the majority of the valuable information. Again, feature selection retains just a subset of the original features, whereas feature extraction generates new ones[2][3].

For human identification, a multimodal biometric system employs more than one physiological or behavioral feature. For human identification, a unimodal biometric system utilizes only one or two behavioral characteristics. Each unimodal biometric system has advantages and disadvantages[4][5].

In this work, one of these systems has been chosen to be studied is that of the recognition of people by their images of the outside surfaces of fingers, or more exactly, a system that uses finger joint imprint (Finger Knuckle Print (FKP)) This modality was chosen according to their many remarkable advantages, in Knowing it is a technique acceptable to individuals, simple and easy to use. Finally, the combination of all the fingers (ten fingers in both hands) can be use to establish a robust and accurate biometric system.

As part of this work, in the first series of experiments, we designed a mono-biometric system, a system that uses a single biometric modality. For this, an algorithm, ResNet, was used for the most important phase, namely the extraction phase of the characteristics. This algorithm is widely used for texture analysis. In the second series of experiments,

multimodal fusion is examined in order to obtain a high-performance biometric system, a system that can be operated with a very small identification error, this error makes the system suitable for use in very high secure applications.

Our memory is divided into three chapters:

In the first, we defined biometrics and the various biometric techniques used. We also have an overview of the main application areas of biometrics and their contribution to the global market, and this chapter is finalized by Multimedal Fusion.

The second , In this chapter several notions on how to use and combine several modalities were discussed. Our contribution to feature extraction is also presented in this chapter. In this paper, concepts about the ResNet technique, as well as how to apply them to extract discriminant characteristics, are presented.

In the third chapter , we propose an automated method for finger knuckle pattern recognition that can attain excellent accuracy. The presented framework extracts ROIs fromthe capture finger knuckle images, which is followed by application of BSIF image descriptor on each ROI. Next, a PCA+LDA ba-sed dimensionality reduction scheme is employed to oser. Btain compact representation of theFKP trait. Lastly, nearest neighbor classifier is utilized to authenticate the user.

Chapter I

Security and Biometrics

I.1 Introduction

Today, automatic authentication of individuals is becoming a key approach to security and access control within IT infrastructures and systems. On one hand, the international growth of communications, such as the internet, both in volume and in diversity (physical displacement, financial transaction, access to services...), implies the need to ensure the identity of individuals. on the other hand, the importance of the issues motivates fraudsters to defeat existing security systems. There is, therefore, growing interest in electronic identification and authentication systems. Their common denominator is the need for a simple, practical, reliable, and inexpensive way to verify a person's identity and properties for access control has opened up with the proliferathe notion of systems, none of which prove to be effective against fraud, because all use an external identifier such as a badge, card, key, code, password...etc. These identifiers present a major problem in guaranteeing security because they are exposed to several risks such as duplication, theft, forgetting, loss, etc. On the contrary, biometric is one of the most reliable and most used means in

the recognition and authentication of individuals. It is a science-based on the biological, physical, or behavioral attributes of people, such as DNA, urine, face shape, hand shape, fingerprints, voice, gait... etc.
Biometric techniques based on biological attributes (DNA, saliva, urine, odor, etc.) are very expensive and difficult to implement for common use. For this, we will limit ourselves, in this chapter, to the presentation of the other two classes of biometric methods (physiological and behavioral). In this chapter, we will provide background on state-of-the-art biometrics, some examples of biometric recognition techniques, and their fields of application and establish a general (more or less comparative) picture of the techniques most used in the field.

I.2 Biometrics definition

Biometrics is a science that concerns the identification of people based on mathematical analysis and through behavioral or morphological biological attributes, these characteristics must be: Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability, Circumvention not changing with time, and recordable[6].

I.3 Characteristics of biometric

A number of Biometrics features are used in various applications. Each biometric trait has its advantages and disadvantages, therefore, the choice of techniques for a particular application depends on a variety of questions in addition to its performanc . Jain et al. [7] have identified seven factors that determine the suitability of physical or behavioural features to use in a biometric application:

- Universality: Any person with access to the application must possess the trait.
- Uniqueness: the line must be sufficiently different from one person to another.
- Permanence: A person's biometric trait must be sufficiently invariant over a period of time.
- Measurability: It should be possible to acquire and scan biometric data using an appropriate device.
- Performance: The accuracy of the recognition and the resources required to achieve the accuracy required by the constraints imposed by the application.
- Acceptability: Individuals who will use this application must be willing to present their biometric traits to the system.
- Circumvention: This is the ease with which an individual's character can be imitated by using objects (for example: false fingers in the case of physical traits and mimicry, in the case of behavioural traits) [8].

I.4 Biometrics techniques

The different techniques of biometrics: Biometric, techniques are divided into two groups according to the cooperation of the individual:

- Intrusive techniques: These techniques require physical contact with the individual to identify him, such as fingerprints, retina, reef, or hand shape. Their use is generally poorly accepted.
- Non-intrusive techniques: These techniques do not require the cooperation of the individual in question. They can be applied remotely using sensors that do not require direct contact with the user (face, gait, etc.). Biometrics allows the identification authentication of an individual on their own identifiable and verifiable databases.

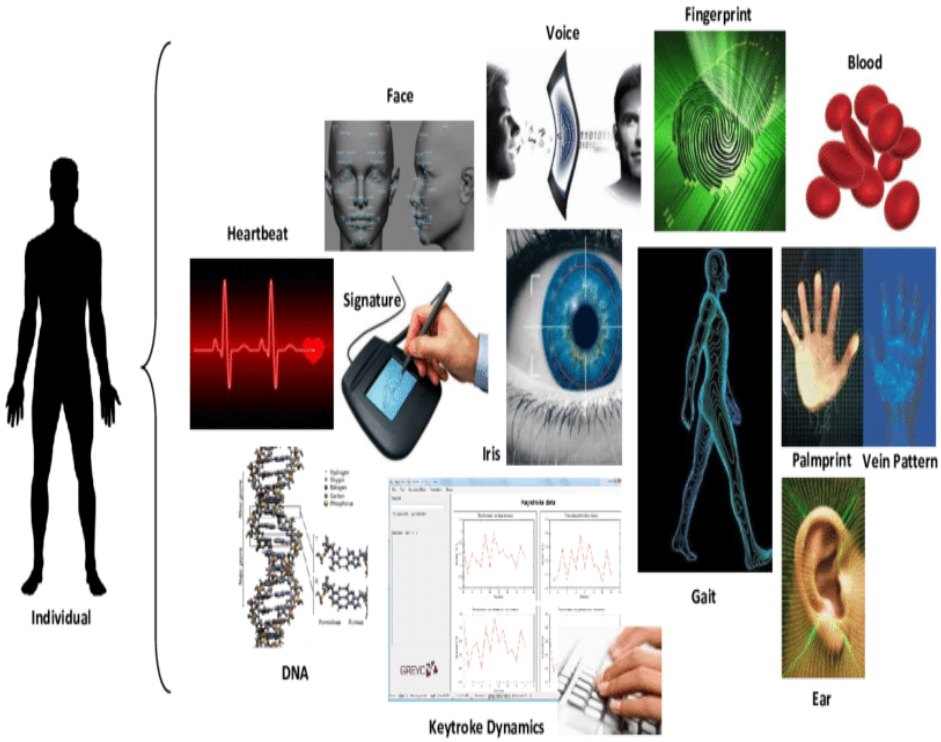


Figure I.1: Biometrics techniques

Biometrics is a technique for identifying in individual by means of its morphological characteristics and biological and behavioural:

I.4.1 Morphological Biometrics

I.4.1.1 Empreinte digitale

Fingerprint recognition is the technique most commonly used biometric. The latter are made up of local lines parallel with singular points and constitute a unique and permanent Fingerprint scanners scan and then pick up items to differentiate fingerprints. These are called minutia. There are several types of minutia: lake, bifurcation, delta or impasse,

etc. This type of technical biometric is used by financial institutions for their clients and is found in the same time in hospitals, schools, airports, etc[9].

Figure I.2: digitale Empreinte

Advantages:

- Low price.
- Biometric reader size is not large.
- System remains very simple to set up.
- Easy to use.

Disadvantages:

- The registration is by all the parts concerned whith what can pose a problem in the event of the illness either physical or psychological.

I.4.1.2 Face

Our faces are complex objects with features that can vary in time. However, humans have a natural ability to recognition faces and identify people at a glance. Of course, our ability to the natural recognition extends beyond the recognition of the face, where we are also quickly locate objects, sounds or smells. Unfortunately, this natural ability does not exist in computers, thus the need for artificially simulate recognition to create autonomous intelligent systems simulate our ability naturally.

Face recognition in machines is difficult but not in impossible task. Throughout our lives, many faces are seen and preserved naturally in our memories forming a kind of data. this type a rocognition is used as a surveillance system or identification by authorities or police forces primarily on the premises. It is one of the most acceptable techniques, but it requires a simple and fixed background for the result to be accurate [10].

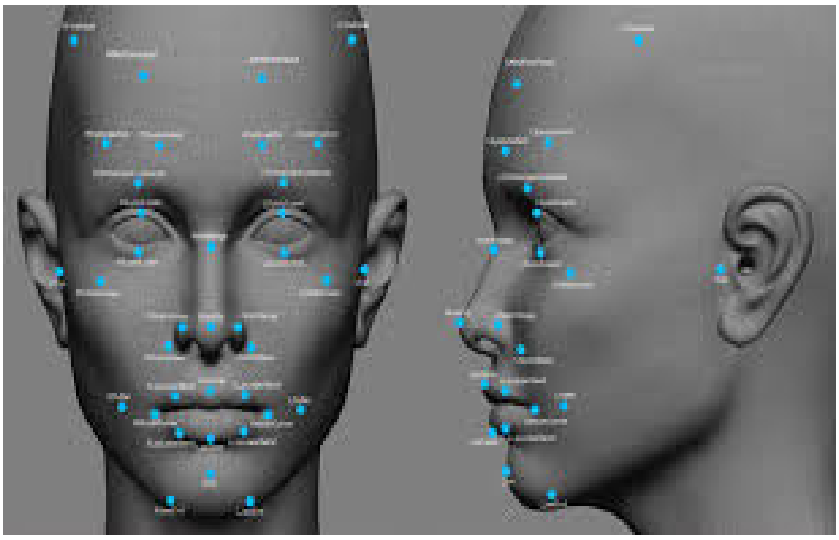


Figure I.3: Face modality

Advantages:

- Technique acceptable to the public.
- Simple operation.
- Inexpensive technique and can rely on the acquisition equipment of the current images .

Disadvantages:

- Identical twins are not differentiated.
- Physical changes can mislead the system.
- The technique is too sensitive to changing lighting or camera angle. . . etc.

I.4.1.3 Iris

The iris is the region, in the form of a ring, between the pupil and the white of the eye. The iris has an extraordinary structure and offers many texture characteristics that are unique to each individual. The recognition of iris is developed in the 80s that is why it is a more recent technology. The iris image is captured by a camera that contains an infrared camera, when the person stands about a short distance from the device[9].
Advantages:

Figure I.4: Iris

- Identical twins are not confused.
- Iris structures remain stable throughout life.
- Large amount of information in the iris.

Disadvantages:

- Image acquisition requires some training and practice.
- Reliability decreases in proportion to the distance between the eye and the camera.
- people are having trouble accepting this biometrics.

I.4.1.4 Finger knuckle Prints (FKP)

This is biometric technology based on the back surface of the finger , it contains distinctive features, such as main lines, branch lines and ridges, which can be extracted from the low-resolution images. The hand contains several fingers, for that, we must keep the information on each finger for a precise recognition in the field of identification[11].
Advantages:

- Accepted technique.
- Simple to use.
- By combining all the fingers of the hand, a system can be established robust and accurate biometrics.

Disadvantges:

Figure I.5: Finger knuckle Prints (FKP)

- Very similar for twins.
- Problem with cutting off a finger.
- Placing the wrong finger on the drive causes a big error.

I.4.1.5 Palm Print

This technique uses the inner surface of the palm to identify and/or verify of persons. It is well suited for systems medium security such as physical or logical access contro[9].

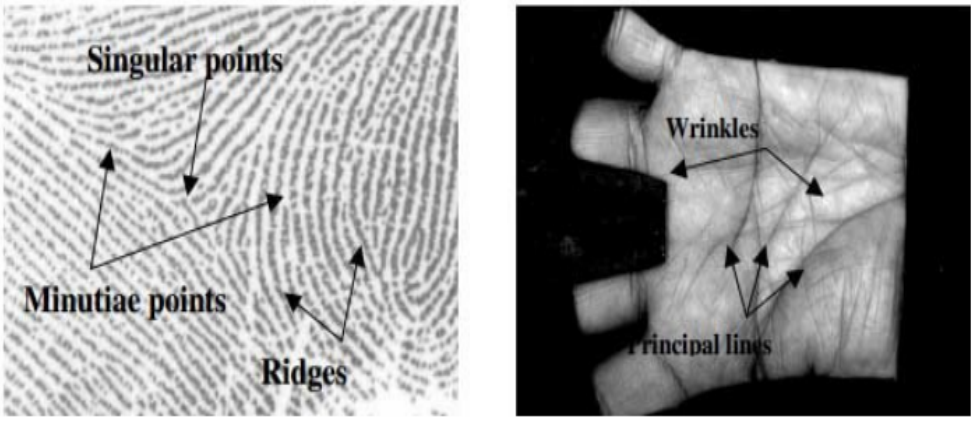


Figure I.6: Palm Print

Advantges:

- Easy to use, It has great acceptance.
- After use, the hand remains clean and leaves no trace.
- Almost available to all individuals.

Disadvantges:

- Could be similar in twins or family members.
- It is not permanent in terms of changes such as ageing.

I.4.2 Behavioral Biometrics

I.4.2.1 Voice

The human voice varies from person to person and can consist of physiological and behavioural components. Voice based identification shape and size of appendages (mouth, nasal cavities and lips) used in the sound synthesis. The recognition of speakers is rather used by phones, police forces, hospitals, etc[10].

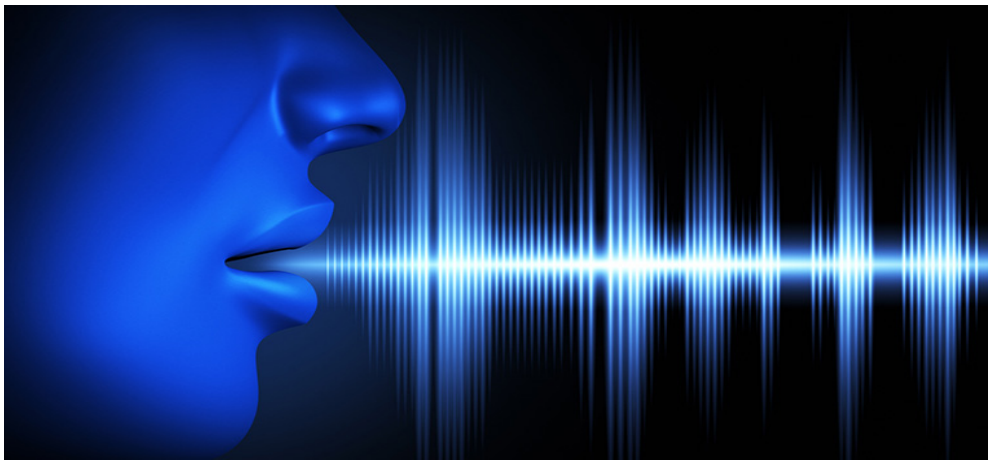


Figure I.7: Voice Signal

Advantges:

- Very well accepted because the voice is a natural signal to produce.
- Unique wave dynamics produced.

Disadvantges:

- Less permanent biometrics.
- Behavioural characteristics change over time.
- Possibility of fraud by registration.
- Noise sensitivity during acquisition.

I.4.2.2 Handwritten signature

It is a personal writing of an individual, the verification of the signature is based on two modes:
Static Mode: Static Signature Verification emphasizes shapes signature geometrics, in this mode in general, the signature is normalized to a known size then break down into simple element.
Dynamic mode: it uses dynamic features such as acceleration, the speed and trajectory profiles of the signature[9].

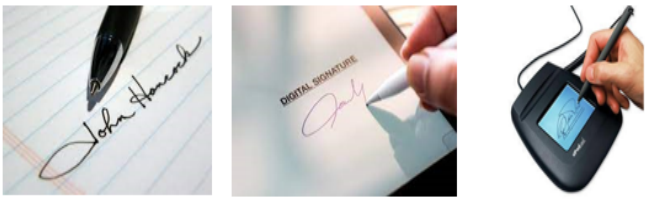


Figure I.8: Handwritten Signature

Advantges:

- Very acceptable by the user.
- Can protect all of your personal files.

Disadvantges:

- High variability over time (you cannot maintain the same form of signature for a lifetime).
- High potential for fraud.

I.4.2.3 Dynamic typing on the keyboard

It is a system of recognition of an individual based on the manner of his writings by a software device which calculates the typing speed, the sequence of letters, the typing time and the pause between each word[9].

Advantges:

- Strong user acceptance.
- Precise security.

Disadvantges:

- It is not more convenient.
- Not permanent throughout life (age, emotion, fatigue).

Figure I.9: Dynamic typing on the keyboard

I.4.2.4 Gait

Each person has a particular way of walking, we can identify individuals of the nature of leg, arm and joint movement or special motion obtained by a video in order to send it to a computer for analysis to determine the speed and acceleration of each individual[9].

Figure I.10: Gait

Advantges:

- Very acceptable to individuals.

Disadvantges:

- Not permanent (age, fatigue, illness).

I.4.3 Biological Biometrics

I.4.3.1 Hand Veins

The veins of the hand vary from person to person. Analysis of this difference makes it possible to maintain points for differentiated a person to an other[12].

Advantges:

Figure I.11: Hand Veins

- Does not require contact.
- Difficult to forge.

Disadvantges:

- very expensive.

I.4.3.2 DNA Analysis

It is the most accurate way to determine the identity of the person. It is impossible to find two people with the same DNA. This modality has the advantage of being unique and permanent throughout the lifetime[12].

Figure I.12: DNA Analysis

Advantges:

- Distinguish individuals with great precision.
- Facilitates detection of offenders.

Disadvantges:

- Slow to get results .
- require a high cost.

I.4.3.3 Thermogramme Faciale

The amount of heat emitted by different parts of the face characterizes each individual. It depends on the location of the veins but also on the thickness of the skeleton, the amount of tissues, muscles, fats, etc. contrary to facial recognition, plastic surgery has little influence on facial thermograms. To capture the image, it is possible to use a camera or a digital camera in the infrared field. The capture can be done in any lighting condition and even in darkness which is an additional advantage over the classic face recognition[12].

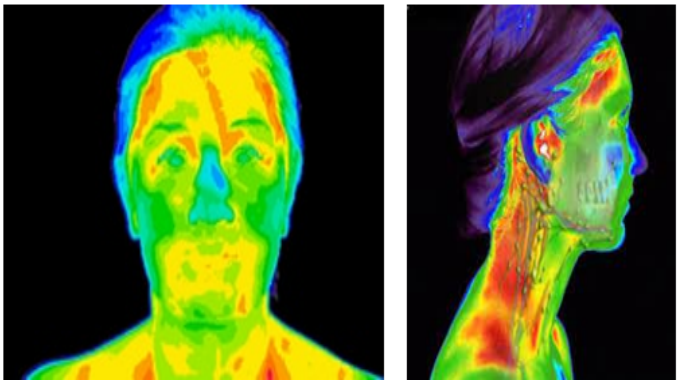


Figure I.13: Thermogramme Faciale

Advantges:

- Can recognize faces, even in darkness.
- Can distinguish from twins.

Disadvantages

- Influenced by factors such as body temperature and emotional state.

I.5 Architecture of a biometric system

In these days, biometric systems are increasingly used in the latest years. In general, a person recognition system based on their descriptors biometrics can be divided into two phases, enrolment phase (database creation) and recognition phase.

I.5.1 Biometric functioning

Each biometric system consist of two distinct phases:
Enrolment phase: The enrolment phase is defined by the collection of an individual's biometric traits. And convert them into a biometric reference (Template, characteristic vector), and store them in a database for later comparison.
Recognition phase: During recognition, the biometric modality measured, and; a set of distinguishing features (Template). Are extracted as during enrolment [13]. This phase can be divided into two modes:

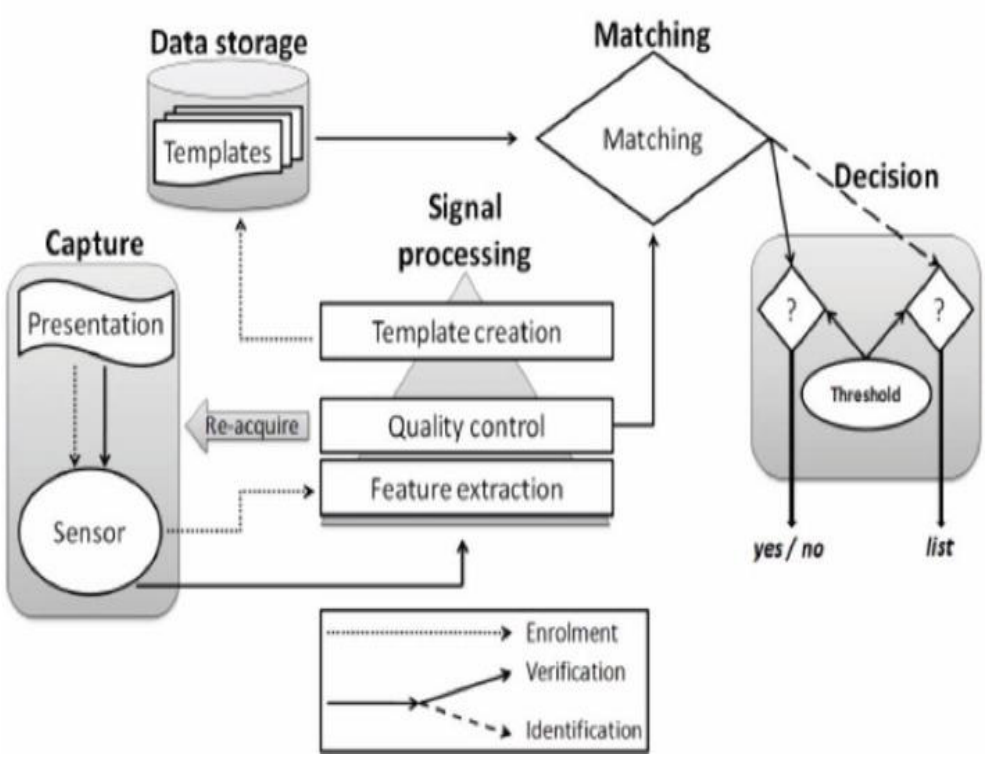


Figure I.14: Biometric System Architecture

- Verification Mode: The system must answer the question such as: "Am I The real user proposed by the system to identify?". The system must verify the identity of the individual and Verification mode is sufficient to compare the signal with only one of the models present in the database. In the audit, we are talking about a common problem since we assume that an individual who does not model in the database (imposter) can seek to be recognized.

- Identification mode: the system must guess the identity of the person. It, therefore, responds to a type of question: "Who am I ?". In this mode, the system compares the measured signal with the different models contained in the database. In general, when we talk about identification, we assume that the problem is closed, that is to say, that any person using the system has a model in the database.

- Identification in closed set mode: For example we use. this type identification in order to record the presence of persons in certain enterprises. In the system, if the samples has some degree of similarity with the samples, the person will be accepted.

- Identification in open set mode: If there is a high similarity between the biometric sample tested and all preregistered models and if this similarity is below (or above). The security threshold, this person is rejected. The means that the person is not one of those recorded by the system. Otherwise, the system is accepted.

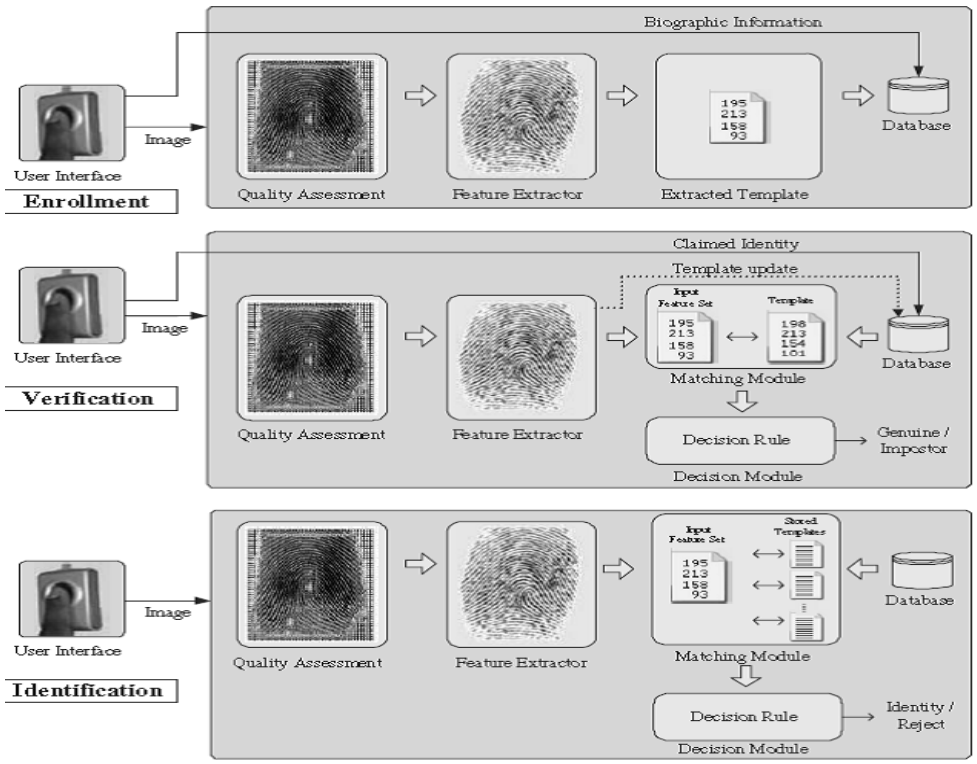


Figure I.15: Biometric Functionality

I.5.2 Major Modules

The biometric system is a system for identifying trends and storage of data to be saved or identified in the form of matrices. Then the system is ready to identify intruders. This system consists of four units: extraction of characteristics, comparison (measure of similarity) and decision. Registration or enrolment is used for future comparison while the decision is to recognize the person or not.

Data Acquisition: This phase collects biometric data from customers. Several industrial processes can be used for the acquisition such as a camera, fingerprint scanner, etc.

Feature Extraction: Images are processed to extract process characteristics. This process is applied to avoid unnecessary information that exists. So, this module is used to process the image to extract only the biometrics characteristics, in the form of a vector or template, which can then be applied to recognize people.

These characteristics are unique to each person and stable.

Comparison: In this module, the biometric features extracted are compared with a vector previously stored in the database and marking the degree of similarity (difference or distance).

Decision: Verifies identity affirmed by a user or determines the identity of a person is based on the degree of similarity between the extracted characteristics and the person stored vector.

I.6 Online and offline systems

Biometric recognition systems are classified into two categories: Online and offline recognition.

I.6.1 Online systems

In this type of systems, modality images are captured by a specific capture device, and the acquired digital images are processed in real time.

I.6.2 Offline systems

This type of systems processes images for each modality previously captured by a digital scanner. These approaches provide images high resolution, but not suitable for real time security systems.

I.7 Measuring the performance of biometric authentication systems

First, to understand how to determine the performance of a system We must clearly define four main criteria :

- The first criterion is called the False Reject Rate (FRR). This rate represents the percentage of people expected to be recognized but who are rejected by the system.
- The second criterion is the false accept rate or (FAR). This rate represents the percentage of people who are not expected to be recognized but still accepted by the system.
- The third criterion is known as ("Equal Error Rate" or EER). This rate is calculated from the first two criteria and constitutes a point of measurement of current performance. This point corresponds to the place where FRR = FAR, that is to say, the best compromise between false rejections and false acceptances.
- The fourth criterion is the success rate or equal TR (100-(FRR+FAR)).I.16 illustrates FRR and FAR from distributions of client scores and imposters while the ERR is shown inI.17[9].

The overall performance of an identity verification system is better characterised by its characteristic operating curve (Receiver Operating Characteristic or ROC), The ROC curve I.17 plots the false release rate as a function of the false acceptance rate . The more this curve tends to follow the shape of the benchmark, the more system is efficient, that is to say having a high overall recognition rate. The decision threshold must therefore be adjusted according to the targeted application: High security, low security or compromise between the two[10].

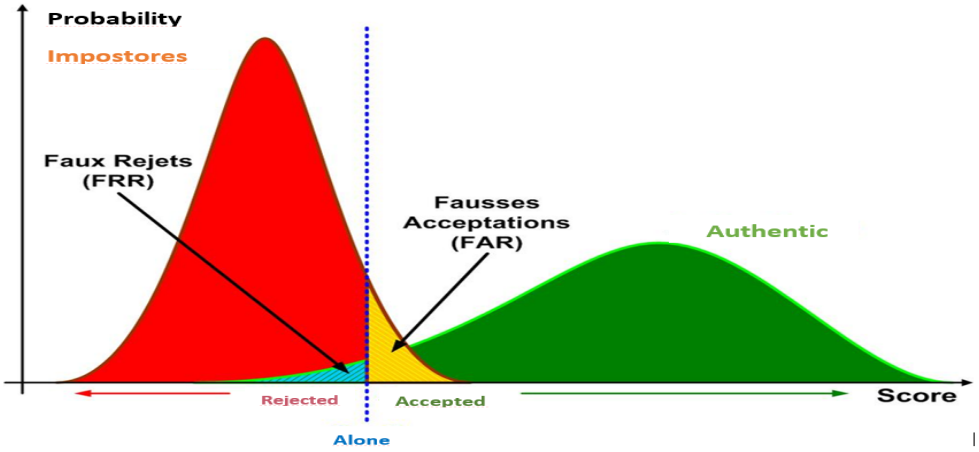


Figure I.16: Illustration of FRR and FAR

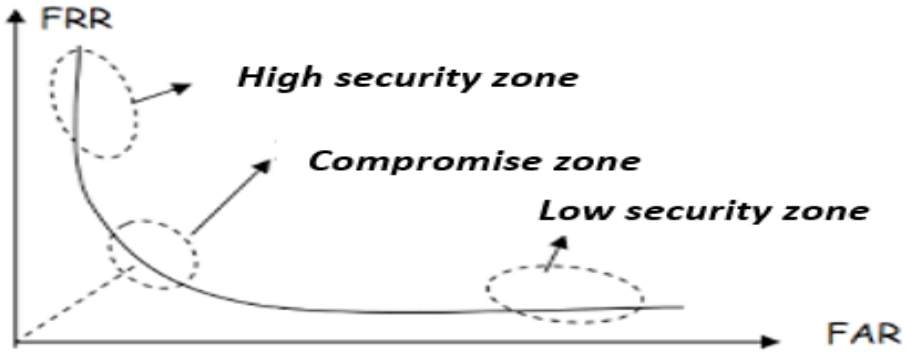


Figure I.17: Functional Characteristic Curve (ROC) of a Biometric Verification System

I.8 Application area

Biometrics meets security necessities by singular areas and organizations in allcountries. Biometric security covers pretty much every area. Today, biometric security is usedin admittance to organizations and data frameworks, electronic installment and information encryption.In general, biometric security applications can be characterized into four principle segments :[14]

I.8.1 Public Service

Control and security of government border buildings. Controls immigrants entering and leaving the country. Used in airports and health. Helping to pass the social insurance card.

I.8.2 Judicial power

The use of fingerprints to prove certain facts concerning criminal offences. The use of DNA extracted from blood or hair at the crime scene to obtain the criminal.

I.8.3 Banking sectors

Banking sectors Banking transactions (cash withdrawals, bank cards, payment by telephone and Internet). Reducing the proportion of fraud through the integration of chip cards with fingerprint recognition.

I.8.4 Physical and logical access

This refers to physical access control such as the security of the premises (building or room) or logical access control such as the security of a computer session (computer or database).

I.9 Biometrics market Regularly

A report on the global biometrics market is published by IBG (International Biometric Group). This study is a comprehensive analysis of turnover, growth trends, and industrial developments for the current and future biometric market. Reading this report is essential for institutions deploying biometric technology, investments in biometric enterprises, The turnover of the biometric industry, including judicial applications and those of the public sector, is growing rapidly. Much of the growth will be due to access control to information systems (computer/network) and electronic commerce, although public sector applications continue to be an essential part of the industry. Revenue from emerging markets (access to information systems, electronic commerce and telephony, physical access and surveillance) is expected to exceed revenue from more mature sectors (criminal identification and citizen identification)[15]. Fingerprints continue to be one of the main biometric technology in

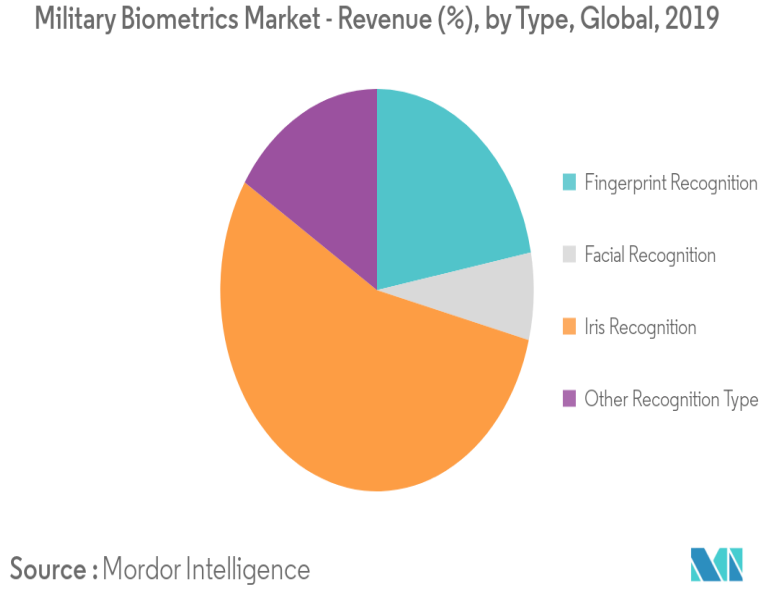


Figure I.18: Biometrics merket share by system type

market share, nearly(50%) of total turnover (excluding legal applications). Exceeds the

recognition of the hand, which had before second place in terms of revenue sources after fingerprints.

I.10 Multimodal biometrics

Unimodal biometric system uses more than one Physiological or behavioral characteristic for human identification. A unimodal biometric system uses only one Physiological or behavioral characteristic for human identification. Each unimodal biometric system has its pros and cons[16].

I.10.1 Unimodal biometric systems

The unimodal system is a simple system that uses only one biometric modality, with as the use of a single finger or algorithm to identify people. This type of system generally has a very high error rate. Thus, this type of system with several limitations can be made biometric secure inapplicable for particular companies or individuals.

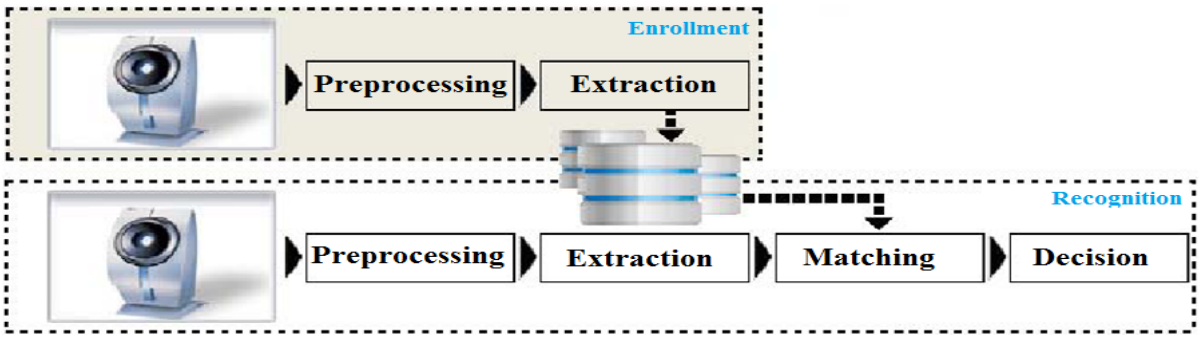


Figure I.19: Unimodal biometric systems

I.10.2 Multimodal biometric systems

Multimodal biometric frameworks utilize different sensors or biometrics to beat the limits of unimodal biometric systems. For occurrence iris acknowledgment frameworks can be undermined by maturing irises and electronic finger impression recognition can be deteriorated by exhausted or cut fingerprints. While unimodal biometric frameworks are restricted by the trustworthiness of their identifier, it is impossible that few unimodal frameworks will experience the ill effects of indistinguishable impediments. Multimodal biometric frameworks can acquire sets of data from a similar marker (numerous pictures of an iris, or sweeps of a similar finger) or data from various biometrics (requiring unique finger impression outputs and, utilizing voice acknowledgment, a spoken passcode).

Multimodal biometric frameworks can meld these unimodal frameworks consecutively,

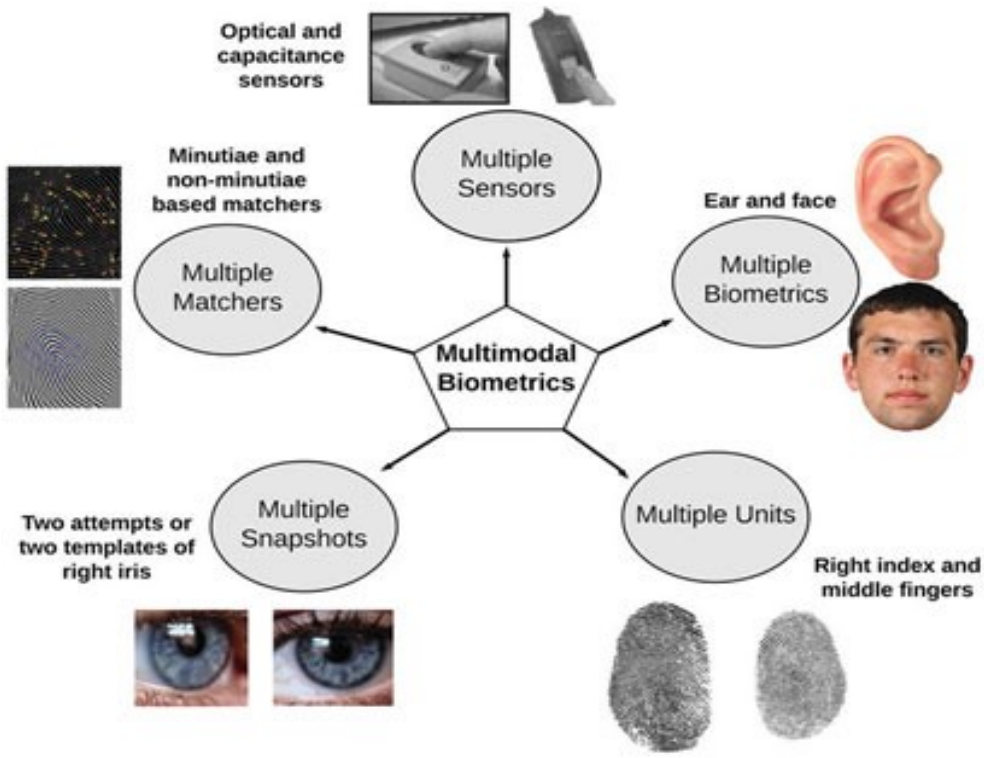


Figure I.20: Multimodal Biometric authentication

all the while, a mix thereof, or in arrangement, which allude to successive, equal, various leveled and sequential coordination modes, individually. Combination of the biometrics data can happen at various phases of an acknowledgment framework. If there should arise an occurrence of highlight level combination, the actual information or the highlights extricated from numerous biometrics are melded. Coordinating score level combination unites the scores created by multiple classifiers pertaining to various modalities. At long last, if there should be an occurrence of choice level combination the eventual outcomes of numerous classifiers are joined by means of methods such as majority casting a ballot. Highlight level combination is accepted to be more compelling than different degrees of combination in light of the fact that the list of capabilities contains more extravagant

data about the info biometric information than the coordinating with score or the yield choice of a classifier. Along these lines, a combination at the component level is required to give better acknowledgment results. Satire attacks consist of submitting counterfeit biometric characteristics to biometric frameworks and are a significant danger that can diminish their security. Multi-modular biometric frameworks are normally accepted to be naturally more powerful to parody assaults, yet ongoing studieshave shown that they can be dodged by mocking even a solitary biometric quality[17].

I.11 Conclusion

In summary, the expanded necessity for dependable and helpful confirmation frameworks, the accessibility of economical PC assets, the improvement of modest biometric sensors, and advances in signal handling added to the fast sending of biometric frameworks in foundations from supermarkets to air terminals. The development of multibiometric frameworks has fundamentally improved the presentation of distinguishing proof frameworks .

Chapter II

Feature Extraction and Matching

II.1 Introduction

In the previous decade, deep learning has become the main innovation in the field of man-made consciousness. It has gotten an advancement execution for some applications , like discourse recognition, common language handling, PC vision, picture and video analysis, and mixed media. In the field of biometrics, especially in FKP recognition , deep learning has become the most standard innovation.

Convolution neural organization (CNN) is quite possibly the main parts of deep learning technology, and has been generally utilized in different undertakings of image processing and PC vision, for example, target discovery, semantic segmentation and example recognition. For image based biometrics technologies, CNN is the most ordinarily utilized deep learning technique. Up to now, numerous exemplary CNNs have been proposed and great outcomes have been accomplished in numerous recognition tasks. Biometrics are gener-

ally used alternately to describe characteristics of a person. These characteristics define a measurable physiological (face, FKP, palms, hand geometry, ear) and behavioral (speech, hand writting,dynamic typing on the keyboard,gait, signature)...etc. These elements are essential to identify a person. A biometric system is a pattern recognition system, which provides data required to extract all the features from it, and compare it with the model set stored in the database.

II.2 Features extraction

Feature extraction is for creating a new, smaller set of features that stills captures most of the useful information. Again, feature selection keeps a subset of the original features while feature extraction creates new ones.

As with feature selection, some algorithms already have builtin feature extraction. The best example is Deep Learning, which extracts increasingly useful representations of the raw input data through each hidden neural layer[18].

II.3 Machine learning

Machine learning is an application of computer science that allows computers how to learn and operate without being a neural network. More specifically, machine learning is a data analysis methodology that entails creating and updating models that allow programs to "learn" from experience. Machine learning is an application of computer science that allows computers how to learn and operate without being a neural network. More specifically, machine learning is a data analysis methodology that entails creating and updating models that allow programs to "learn" from experience. It involves the construction of algorithms that adapt their models to improve their ability to make predictions. According to Tom Mitchell, professor of Computer Science and Machine Learning at Carnegie Mellon, a computer program is to learn from experience E concerning some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E. A mathematical way of indicating that software uses machine learning if it improves at problem-solving over time. The first applications and discussions of machine learning dates back to the 1950s, and its use has grown dramatically in the last 10 years. Image recognition, natural language processing, artificial intelligence design, self-driving vehicle technology, and Google's online search algorithm are common applications of machine learning [19].

II.4 Deep learning

Deep learning is a way of creating a neural network model from an existing model that has been tested on a dataset by transferring the data; hence, the model is not developed from scratch. The data from the model that was trained on the dataset. Is transferred to the new model by training the model input layer on the model with the new dataset and then fine-tuning the model. In this study, deep learning is used to a model trained on

the ImageNet dataset. The model that had been trained on the dataset ImageNet may be utilized in a variety of applications [20] .

II.5 CNN Models

A convolutional neural organization (CNN or ConvNet), is a network architecture for deep learning which gains straightforwardly from data, taking out the requirement for manual feature extraction. CNNs are especially valuable for discovering designs in pictures to recognize objects, faces, and scenes. They can likewise be very viable for classifying non-picture data such as audio, time arrangement, and signal data. Applications that call for object recognition and PC vision, for example, self-driving vehicles and face recognition applications depend intensely on CNNs[21].
What Makes CNNs So Useful? Using CNNs for deep learning is popular due to three important factors:

- CNNs eliminate the need for manual feature extraction,the features are learned directly by the CNN.
- CNNs produce highly accurate recognition results.
- CNNs can be retrained for new recognition tasks.

CNNs provide an optimal architecture for uncovering and learning key features in image and timeseries data. CNNs are a key technology in applications such as:

- Medical Imaging: CNNs can examine thousands of pathology reports to visually detect the presence or absence of cancer cells in images.
- Audio Processing: Keyword detection can be used in any device with a microphone to detect when a certain word or phrase is spoken. CNNs can accurately learn and detect the keyword while ignoring all other phrases regardless of the environment.
- Stop Sign Detection: Automated driving relies on CNNs to accurately detect the presence of a sign or other object and make decisions based on the output.
- Synthetic Data Generation: Using Generative Adversarial Networks (GANs), new images can be produced for use in deep learning applications including face recognition and automated driving.

How CNNs Work?
A convolutional neural network can have tens or hundreds of layers that each learn to detect different features of an image. Filters are applied to each training image at different resolutions, and the output of each convolved image is used as the input to the next layer. The filters can start as very simple features, such as brightness and edges, and increase in complexity to features that uniquely define the object.

II.5.1 Feature Learning, Layers, and Classification

Like other neural networks, a CNN is composed of an input layer, an output layer, and many hidden layers in between.

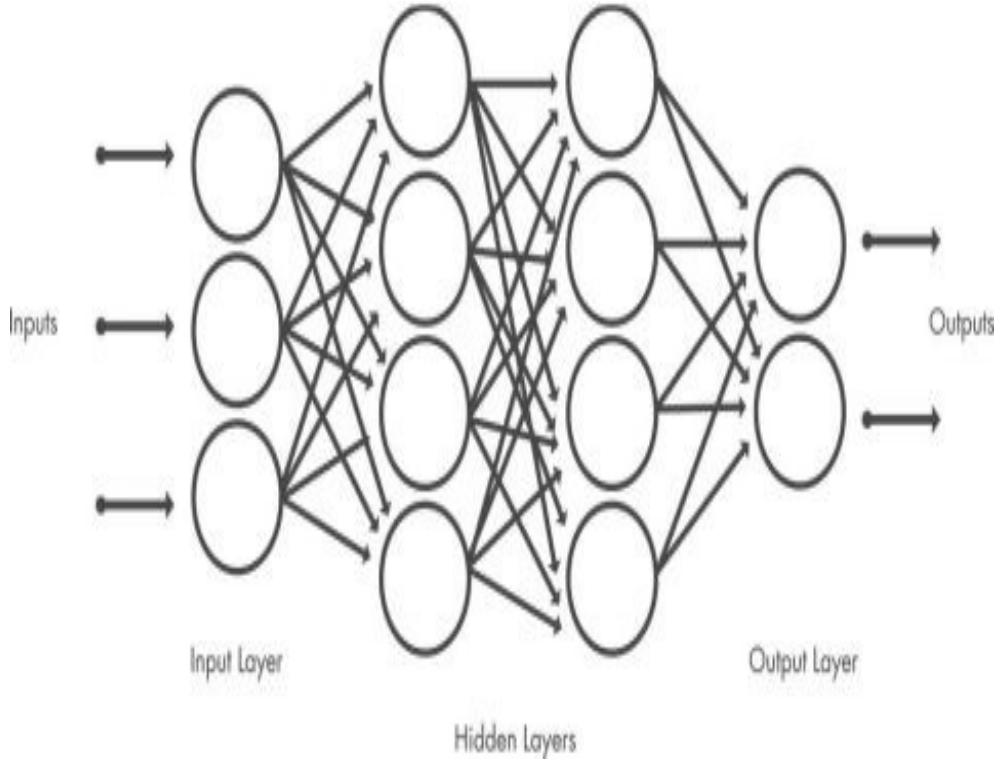


Figure II.1: Architecture CNN

These layers perform operations that alter the data with the intent of learning features specific to the data. Three of the most common layers are: Convolution, activation or ReLU, and pooling.

- Convolution puts the input images through a set of convolutional filters, each of which activates certain features from the images.
- Rectified linear unit (ReLU) allows for faster and more effective training by mapping negative values to zero and maintaining positive values. This is sometimes referred to as activation, because only the activated features are carried forward into the next layer.
- Pooling simplifies the output by performing nonlinear downsampling, reducing the number of parameters that the network needs to learn.

These operations are repeated over tens or hundreds of layers, with each layer learning to identify different features[22]. Example of a network with many convolutional layers. Filters are applied to each training image at different resolutions, and the output of each convolved image is used as the input to the next layer.

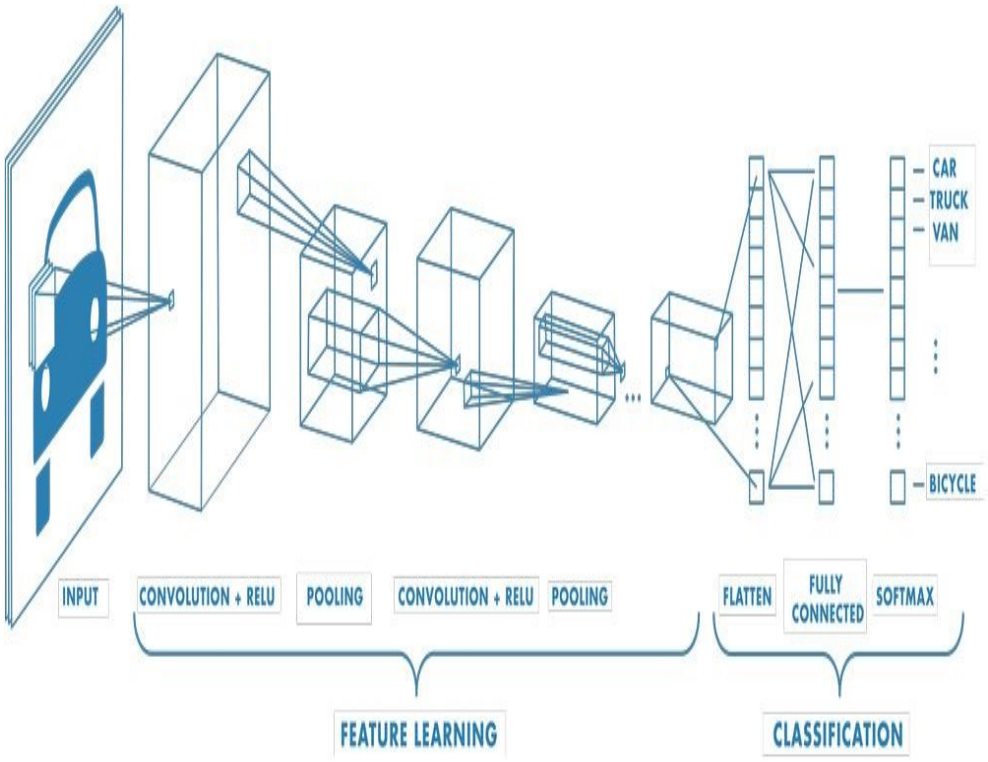


Figure II.2: Deep learning and convolutional neural networks for computer vision

II.5.2 Classification Layers

After learning features in many layers, the architecture of a CNN shifts to classification. The next to last layer is a fully connected layer that outputs a vector of K dimensions where K is the number of classes that the network will be able to predict. This vector contains the probabilities for each class of any image being classified.

The final layer of the CNN architecture uses a classification layer such as softmax to provide the classification output[23].

II.6 ResNet

Ones all agree that features are isolated from the more significant network. In general, accomplish better than that isolated from shallow associations. Regardless, with the organization's significance expanding, two issues are unavoidable. The tendencies may be dissappear/explode, and the precision may be doused and a short time later spoil quickly. To settle these two issues the significant waiting framework called 'ResNet' is proposed. ResNet earned a spot in the yearly competition ILSVRC-2015, demonstrating its dominance over alternative association structures. Observe how challenging it is to match the concept yield arranging with the stacking layer. Fitting the lingering design and limiting the waiting time to zero is a lot more capable and advantageous. The recently proposed substitute way affiliations' in ResNet can change the customary fitting rule. The standard piece of 'substitute way affiliations' was to make the info maps be

character arranging. Also, two particular construction blocks are for the most part used in existing ResNet structures. The main sort is considered the mix of two exceptional nonlinear mappings of data maps, while the resulting kind is the summation of character arranging and nonlinear arranging. The association used in our work is 50-layer ResNet. The development of the ResNet explained in II.3[24].

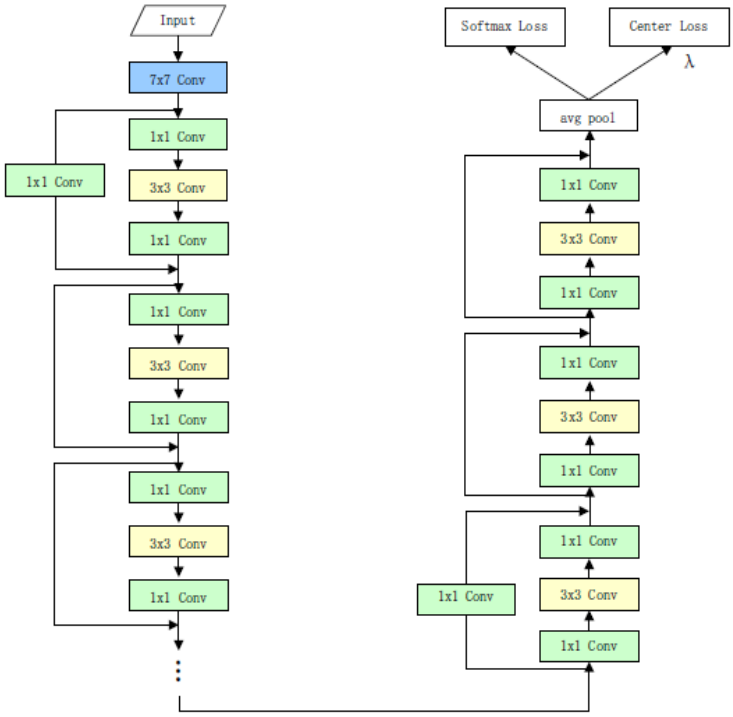


Figure II.3: Structure of the proposed network

II.7 ResNet 50

Is a deep residual architecture of CNN network and has accomplished very encouraging recognition execution in a wide scope of utilizations. Contrasted with the exemplary CNN network architecture, skip associations are acquainted in ResNet-50 with address the issue of debasement when preparing a very deep network. The residual network has lower combination loss without over the top overfitting issue. In particular, a deep residual network is made out of a progression of residual blocks, and every one of which is made out of a few stacked convolutional layers (we respect amended linear unit layer (ReLu) and BN layers as the part of convolutional layer). A residual block is detailed as : [25]

$$h_{l+1} = \mathrm{Relu}\left(h_l + \mathrm{f}\left(h_l, w_l\right)\right) \tag{II.1}$$

Where hl and h(l+1) address information and output of the l-th residual block respectively , ReLu(.) is corrected linear unit function ,F(.) is the residual mapping function and wl are the parameters of the residual block. The basic architecture of residual block is

shown in II.4. The interested authors canrefer to for more details. Each residual structure is activated by a function as below:

$$h_{l.} = h_{l.} + \sum_{i=l}^{L-1} \mathrm{f}\left(h_i, w_i\right) \tag{II.2}$$

The input of the L residual unti can be expressed by the sum of the input of a deep residual unit and all the center complex mappings. Let loss function be , the back propagation is derived:

$$\frac{\partial \theta}{\partial h_l} = \frac{\partial \theta}{\partial h_L}\frac{\partial h_L}{\partial h_l} = \frac{\partial \theta}{\partial h_L}\left(1 + \frac{\theta}{\partial h_l}\sum_{i-l}^{L-1} \mathrm{f}\left(h_i, w_i\right)\right) \tag{II.3}$$

The neural network registering inclination advancement based on the back spread strategy, and the back propagation for secret layer angle based on the chain rule. The angle characteristics might be a development of items motivating the shallow gradient of hidden layer.

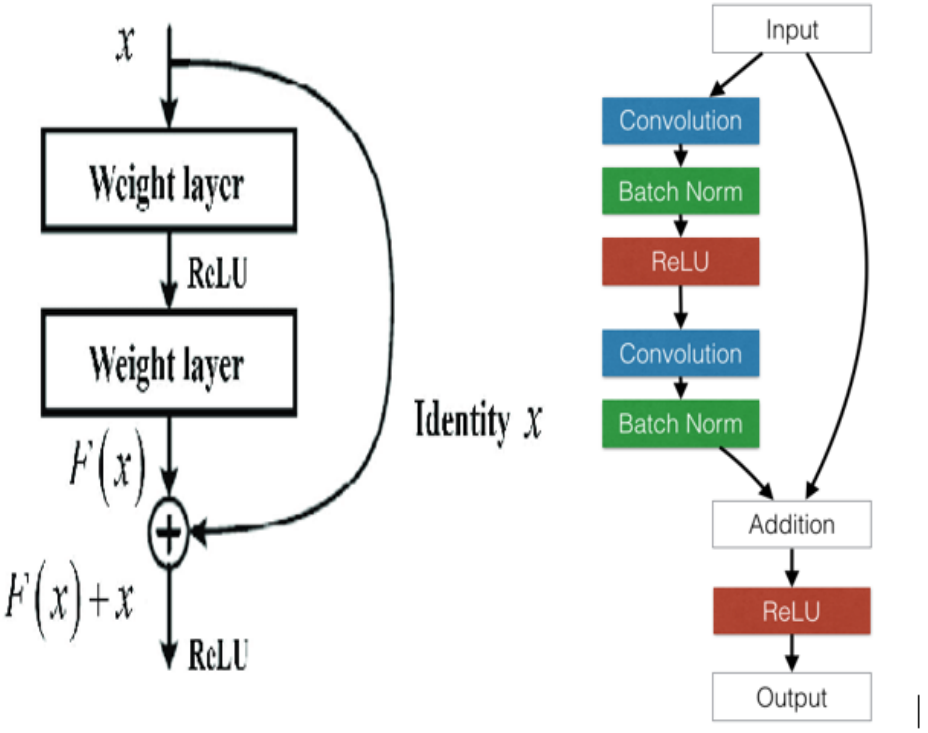


Figure II.4: ResNet 50

II.8 Feature Selection

Feature selection (FS) algorithms approach dimension reduction in a different way. Rather than transforming the data to an entirely new set of dimensions, determine the "best" minimal subset characteristics. In the process of knowledge discovery, interpreting the output of feature extraction methods might be challenging, as the transformed features

may have no physical meaning to the do-Main expert. In contrast, the dimensions retained by a feature selection technique may usually be interpreted directly. Feature selection in the context of deep classification is a reasonably well posed Problem. The purpose can be to uncover traits that are linked to or predictive of the class designation. Nevertheless, the objective may be to choose data that will help to build the highest accurate classifier. The object is less well-posed in unsupervised feature selection, and as a result, it is a lot less studied area.

II.9 Features Matching

Matching score is a measure of similarity between the test (input) and train (template) feature vectors. The process of creating correspondences between two images of the same scene/object, known as feature matching or image matching, is a component of many computer vision applications such as image registration, camera calibration, and object identification. The detection of a group of interest points from image data. recently , several methods have been used in this field ,and in our biometric identification system we used four different types:

II.9.1 K-Nearest Neighbor Algorithm (KNN)

is a type of instance-based learning or lazy learning where the function is only approximated locally and all computation is deferred until classification. The k-nearest the neighbor algorithm is amongst the simplest of all machine learning algorithms: an object is classified by a majority vote of its neighbors, with the object being assigned to the class most common amongst its k nearest neighbors (k is a positive integer, typically small). If k = 1, then the object is simply assigned to the class of its nearest neighbor. The training phase for KNN consists of simply storing all known instances and their class labels. If we want to tune the value of K, n-fold cross-validation can be used on the training dataset. The testing phase for a new instance “T”, in a given known set “I” is as follows:

- Compute the distance between T and each instance in I.
- Sort the distances in increasing numerical order and pick the first K elements .
- Compute and return the most frequent class in the K nearest neighbors KNN learning algorithm has been tested because it needs few parameters to tune and has been frequently used in recent AOCR research[26].

II.9.2 Support vector machine (SVM)

SVM tool is based on statistical learning theory proposed, in 1979, by Vapnik . The principal motivation of this technique is the probabilistic search of limits that minimize errors and "empirical risk" while maximizing the margin of separation. SVM tool constitutes a separation of regions with optimal hyper planes in a multidimensional data space which ensures the learning systems convergence. Applications of SVM concern, essentially, pattern recognition and statistical analysis. [27].

II.9.3 Radial basis function (RBF)

A general and efficient plan approach utilizing a radial basis function (RBF) neural classifier to adapt to little preparing sets of high measurement, which is an issue as often as possible experienced in FKP recognition, is introduced. To keep away from overfitting and diminish the computational weight, FKP features are first separated by the main part examination (PCA) technique. Then, the resulting features are further processed by Fisher's linear discriminant (FLD) procedure to procure lower-dimensional discriminant designs. A novel paradigm is proposed whereby information data is typified in deciding the construction and starting boundaries of the RBF neural classifier before learning takes place. A hybrid learning algorithm is utilized to prepare the RBF neural networks so the element of the hunt space is radically diminished in the angle worldview. Recreation results directed on the ORL database show that the framework accomplishes astounding execution both as far as to mistake paces of classification and learning efficiency[28].

II.10 Conclusion

In this chapter, we combine convolutional network, namely ResNet, with center loss based biometric learning methods . The center loss embedded after the last hidden layer of ResNet can efficiently boost the performance of the base network by compacting intraclass images. Our experimental results demonstrate the effectiveness of the proposed network.

Chapter III

Experimental Results

III.1 Introduction

In today's highly interconnected society, automated personal identification techniques have become vital of security systems, which require high classification schemes. One such person recognition technique is :biometrics, that is identifying a person based on their physiological and behavioral characteristics . Biometrics have several advantages compared to conventional methods such as passwords or ID cards, it can be forgotten or lost In fact, many biometrics traits have been proposed and widely being accpeted as well as used in diverse applications ranging from border crossing to mobile authentication. Recently, FKP characteristics is one of the hand based biometrics that is prominent emerging trait owing to advantages: (1) the acquisition of finger knuckle surfaces is relatively easy with low cost and low resolution simple cameras, (2) FKP based access systems can be used under various environmental conditions such as indoor and outdoor, (3) FKP features are stable and remain unchanged over time, FKP patterns are age-invariant, (4) FKP based biometric recognition systems are very reliable that gives high performances .

III.2 The FKP Recognition System Design

The proposed FKP recognition system is composed of an FKP image acquisition device and a data processing module. The device 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 coding, and feature matching. A basal block and a triangular block are used to fix the position of the finger joint. III.1 show two sample images acquired by the developed device[11].

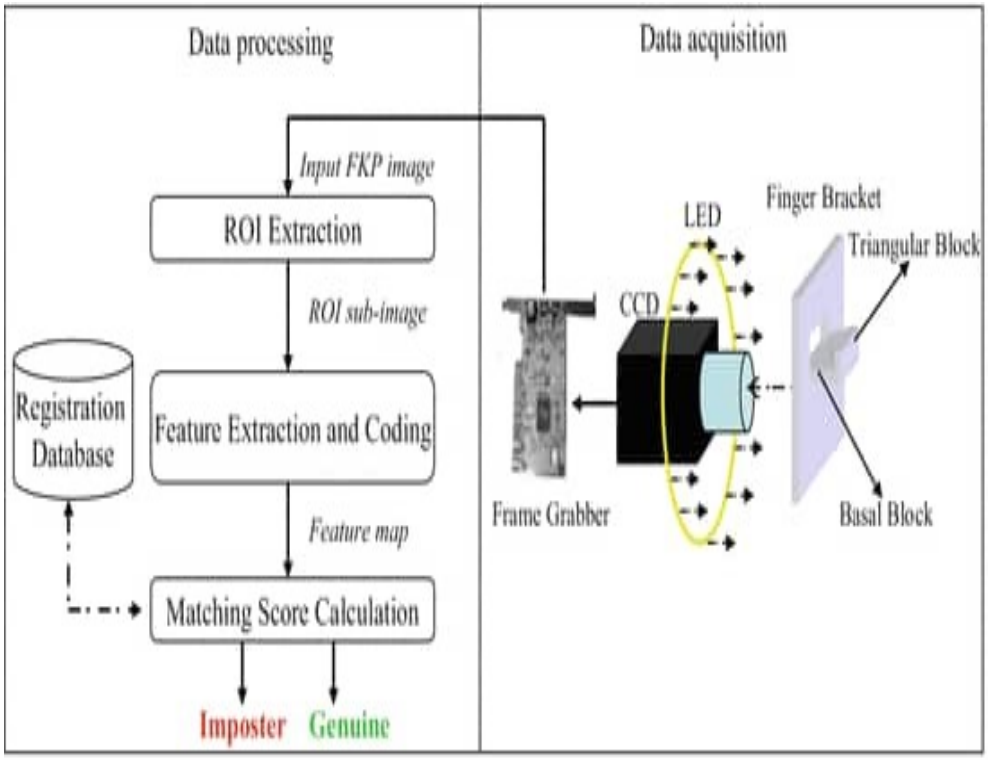


Figure III.1: FKP image acquisition device

III.3 The proposed FKP biometric system

Proposed FKP ROI Extraction This section proposes an efficient finger-knuckle-print ROI extraction technique. The prime objective of any ROI extraction technique is to segment same region of interest consistently from all images. The central knuckle point as shown in Figure III.2 can be used to segment any finger-knuckle-print consistently. Since finger-knuckle-print is aligned horizontally, one can now easily extract the central region of interest from any finger-knuckle-print that contains rich and discriminative texture using this point. The proposed ROI extraction algorithm performs in three steps; detection of knuckle area, central knuckle-line and central knuckle-point. the extracted features are fed to the decision-making classifier to determine the identity of the person[11].

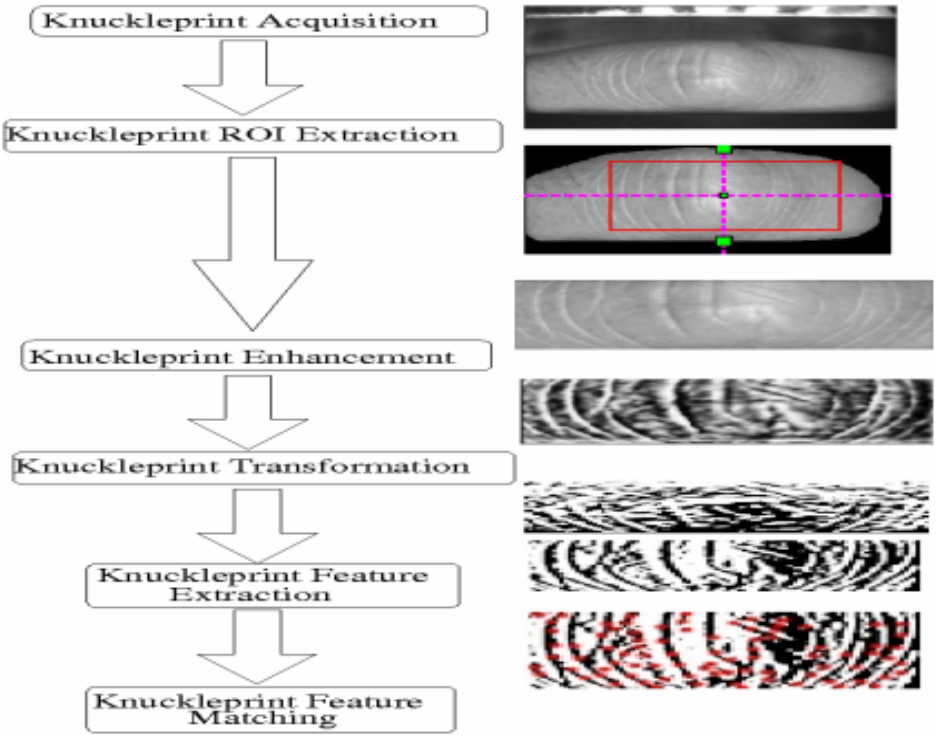


Figure III.2: Overall architecture of FKP recognition system

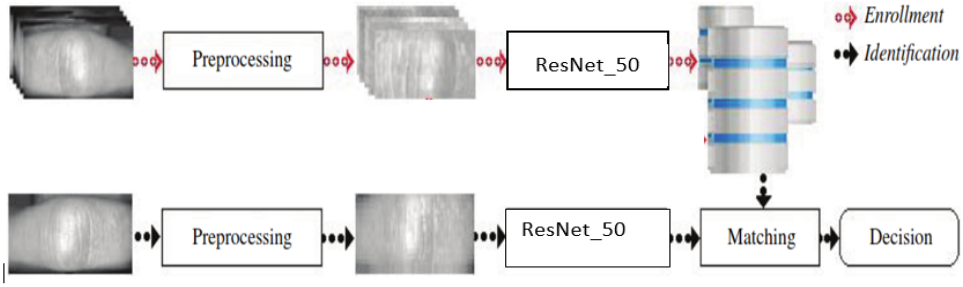


Figure III.3: The proposed biometric system

III.4 Experiment results

Here, we report two different experiments:

- We used ResNet-50 and many classifier .
- Multibiometric FKP recognition system.

III.4.1 Database

The proposed system has been tested on the publicly available FKP dataset that provided by Hong Kong Polytechnic University (PolyU) This database has 7920 images collected from 165 persons with 125 males and 40 females, their age is in the range of [20–50] years old. The images were captured in two sessions, with 48 different FKP images of each individual. Four finger types of every person have been collected that are: left

index (LIF), left middle (LMF), right index (RIF) and right middle (RMF). Every finger type has 6 images in each session. There are total 1980 number of images for each finger type.

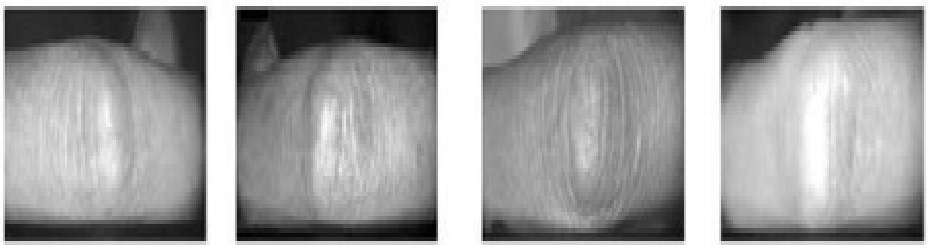


Figure III.4: some images from the Poly U-FKP database

III.5 Experimental protocol

In this work we have divided database into two parts: text and train

- In which in train we took a number of individual photos to each person that is [1,3,5,7,9,11].
- Whereas at text we took a number of photos to each person that is [2,4,6,8,10,12].

And how does the method work with unimodal,than with multimodal.

III.6 Unimodal results

In this section, we are first interested in presenting the different biometric identification systems based on a single biometric modality (one finger), using the methods described in the chapter(1)

Table III.1: Unimodal Identification Test Results Using SVM classifier

SVM				
Fingers	Open Set		Closed Set	
	EER(%)	T_o	ROR(%)	RPR
LIF	0.0037	0.8790	99.59	03
LMF	0.0148	0.7170	99.79	16
RIF	0.2020	0.6070	99.39	95
RMF	0.0172	0.7220	99.79	14

tableIII.1 shows the results of unimodal system by using ResNet50 features and SVM classifier , in which we note: That the results are good with all the fingers at open set identification where as LIF has the best results because it gave us the lowest result ,

EER=0.0037 -In addition, for the closed set identification, we note that the results of all fingers are good, RMF and LMF are the best , because ROR = 99.79%, which is the high value, and since RMF has reached the 14th rank that is the lowest, therefore ,the best value is RMF.

Table III.2: Unimodal Identification Test Results Using KNN classifier

KNN				
Fingers	Open Set		Closed Set	
	EER(%)	T_o	ROR(%)	RPR
LIF	0.1010	0.1157	99.19	14
LMF	0.2020	0.1789	98.98	33
RIF	0.3030	0.1726	99.09	71
RMF	0.1010	0.1121	99.29	58

tableIII.2 shows the results of unimodal system by using KNN classifier,in which we note: That the results are good with all fingers at open set identification where as LIF and RMF are the best results because it gave the lowest result , ERR=0.1010 In addition, for the closed set identification, we note that the results of all fingers are good, RMF is the best , because ROR = 99.29%, which is the highest value.

Table III.3: Unimodal Identification Test Results Using RBF classifier

RBF				
Fingers	Open Set		Closed Set	
	EER(%)	T_o	ROR(%)	RPR
LIF	0.1922	0.6880	99.39	26
LMF	0.1010	0.6860	99.69	12
RIF	0.1010	0.7420	99.39	138
RMF	0.0105	0.8100	99.49	06

tableIII.3 shows the results of unimodal system by using RBF classifier , in which we note: That the results are good with all fingres at open set identification where as RMF has the best results because it gave us the lowest result , EER=0.0105 In addition, for the closed set identification, we note the results of all fingers are good, LMF is the best , because ROR = 99.69%, which is the highest value.

tableIII.4 represents the results of unimodal system by ResNet classification , in which we note: That the results are good with all fingers at open set identification whereas LIF has the best results, because it gave us the lowest result , EER=0.0036 -In addition, for the closed set identification, we note that the results of all fingers are good, LMF and LIF are the best , because ROR = 99.59%, which is the highest value, and since LIF has reached the 03rd rank that is the lowest, therefore ,the best value is LIF.

Table III.4: Unimodal Identification Test Results Using ResNet Classification

RESNet classification				
Fingers	Open Set		Closed Set	
	EER(%)	T_o	ROR(%)	RPR
LIF	0.0036	0.267	99.59	03
LMF	0.2017	0.0029	99.59	24
RIF	0.2020	0.0080	99.19	97
RMF	0.1010	0.035	99.39	30

III.7 Comparison of all results

Through our compariisen to the results of tables , we found that there is two variables ResNet classification and SVM produced the results in both open set and closed set. and since the ResNet classification took longer,we consider SVM to be the best

III.8 Multimodal results

The aim of multimodality is to improve the level of security of the system such that the identification rate of the merged biometric modalities is higher than the maximum of the identification rates of the modalities taken separately. Thus, by using the different modalities (four modalities: four fingers for FKP) as well as the characteristic extraction method (ResNet), several multimodal systems can be exploited.

Table III.5: Multimodal Identification Test Results Using LIF+LMF

LIF+LMF				
Rules	Open Set		Closed Set	
	ERR(%)	T_o	ROR(%)	RPR
SUM	0.00	0.729	100	01
PROD	0.00	0.601	100	01
MIN	0.00	0.775	100	01
MAX	/	/	99.39	02

Table III.5 shows the results of Multimodal system by using LIF+LMF , in which we note: That the results of all rools are good in both open set and closed set, SUM and PROD and MIN are the best , because EER = 00.00 and ROR=100% and at rank RPR=01.

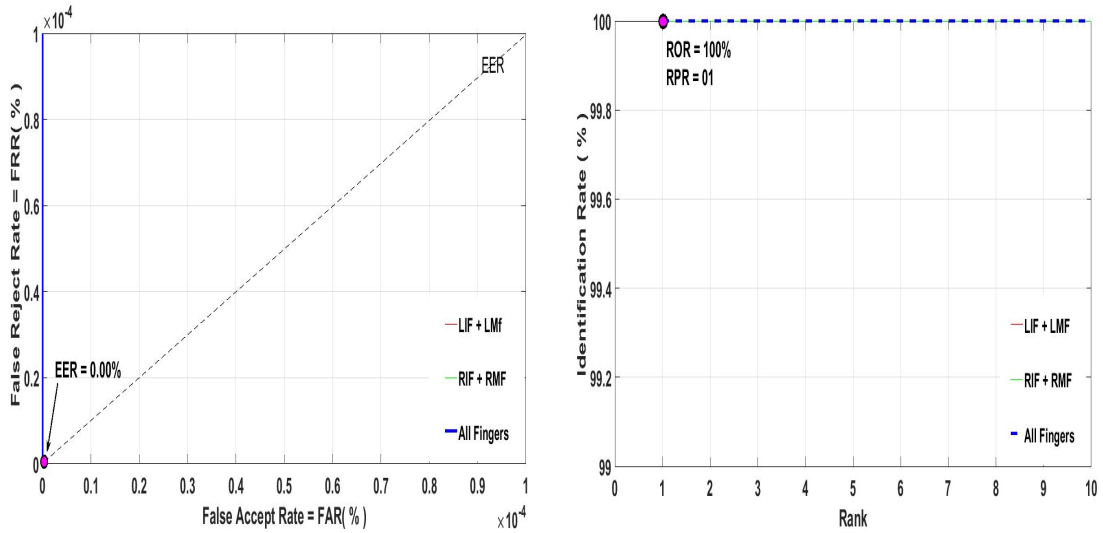
tableIII.6 shows the results of Multimodal system by using RMF+RIF , in which we note: That the results of all rools are good in both open set and closed set, SUM and PROD are the best , because EER = 00.00 and ROR=100% and at rank RPR=01.

Table III.6: Multimodal Identification Test Results Using RMF+RIF

RMF+RIF				
Fingers	Open Set		Closed Set	
	ERR(%)	T_o	ROR(%)	RPR
SUM	0.00	0.792	100	01
PROD	0.00	0.573	100	01
MIN	0.00123	0.93	100	01
MAX	/	/	100	01

Table III.7: Multimodal Identification Test Results Using LIF+LMF+RMF+RIF

LIF+LMF+RMF+RIF				
Fingers	Open Set		Closed Set	
	ERR(%)	T_o	ROR(%)	RPR
SUM	0.00	0.545	100	01
PROD	0.00	0.124	100	01
MIN	0.00	0.525	100	01
MAX	/	/	99.39	02



(a) **(b)**

Figure III.5: Multimodal biometric identification system test results. (a) ROC curves (FRR against FAR), (b) CMC curves, identification rate against rank.

TableIII.7 and Figure III.5 show the results of Multimodal system by using LIF+LMF+RMF+RIF in which we note: That the results of all rools are good in both open set and closed set, SUM and PROD and MIN are the best , because EER = 00.00 and ROR=100% and at rank RPR=01.

III.9 Comparison of all results

Through our comparison to the results of tables , we found that the results of all rools are good but in terms of security take all fingers on the basis of increased security,the

hacking program cannot pinch all fingers together.

III.10 Comparison of Multimodal and Unimodal results

Finally, the FKP identification system is a reliable system that allows a good separation between the categories of customers and fraudsters, and we consider that the results of the multimodal are good and safer compared to the results of unimodal.

III.11 Conclusion

In this chapter, the biometric work presented has led to the development of a system identification of persons by recognition of fingerprints of the finger joints. To do this, we have proposed several biometric systems. In addition to uni modal systems, we have explored some multimodal systems. These different systems are tested to improve modality identification rate in both modes identification, open and closed set. By validating these systems on a data of 165 people, we found a significant improvement in the rate identification (100%).

General Conclusion

Biometrics are mainly used to identify persons with a view to validating or controlling access, and biometrics may be sufficient to reduce rather than eliminate fraud. Similarly, the complete replacement of an existing security system with a biometric system may require a high-performance biometric system, or the required performance may exceed what current technology can provide. From biometrics that give the user some control over data acquisition, sound, face, and fingerprint systems. The latter has undergone the greatest study and testing, and thus occupy the bulk of this work.

Deep learning allows computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction. These methods have dramatically improved the state-of-the-art in speech recognition, visual object recognition, object detection and many other domains . Deep learning discovers intricate structure in large data sets by using the back propagation algorithm to indicate how a machine should change its internal parameters that are used to compute the representation in each layer from the representation in the previous layer. Deep convolutional nets have brought about breakthroughs in processing images, video, speech and audio.

This work presents the context of the automatic identification of people based on their biometric descriptors. We used a new biometric modality of finger knuckle print , to realize our proposed biometric, unimodal and multimodal systems. After introducing the general concepts of biometrics, we presented a state-of-the-art of methods for merging biometric modalities, using the different techniques and levels of fusion.

We also presented some methods for extracting texture-based characteristics. Our tests based on finger knuckle print (FKP) data from Hong Kong Polytechnic University (PolyU) showed that our method can provide excellent results in terms of Equal Error Rate (ERA), recognition rates and overall separation of distributions of clients. We can conclude that we got good results from our study ,recognition rank 100% and EER 0.00%.

Our future work will project to use other presentation of FKP like (2D and 3D) with other transfer learning methods (like AlexNET, GoogleNet).

Bibliography

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[2] M. D. Levine, "Feature extraction: A survey," *Proceedings of the IEEE*, vol. 57, no. 8, pp. 1391–1407, 1969.

[3] S. Khalid, T. Khalil, and S. Nasreen, "A survey of feature selection and feature extraction techniques in machine learning," in *2014 science and information conference*. IEEE, 2014, pp. 372–378.

[4] K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. KailasaRao, "Multimodal biometric systems-study to improve accuracy and performance," *arXiv preprint arXiv:1011.6220*, 2010.

[5] A. K. Jain, L. Hong, and Y. Kulkarni, "A multimodal biometric system using fingerprint, face and speech," in *2nd Int'l Conf. AVBPA*, vol. 10, 1999.

[6] J. Chen and R. Patton, "The international series on asian studies in computer and information science," 1999.

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

[8] R. Bhatia, "Biometrics and face recognition techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, 2013.

[9] M. Moulay and M. Arbaoui, "authentification des personnes par l'articulation du doigt," *UNIVERSITE KASDI MERBAH OUARGLA*, 2015.

[10] A. OUAMANE, "Etude de la fusion de modalités pour l'authentification en biométrie (visage, voix)," Ph.D. dissertation, Faculté des sciences et de la technologie UMK-Biskra, 2011.

[11] L. Zhang, L. Zhang, and D. Zhang, "Finger-knuckle-print: a new biometric identifier," in *2009 16th IEEE International Conference on Image Processing (ICIP)*. IEEE, 2009, pp. 1981–1984.

[12] A. BENAGGA and L. TELIB, "Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt," 2016.

[13] A. Babich, "Biometric authentication. types of biometric identifiers," 2012.

[14] A. I. Piotrowska, M. Polasik, and D. Piotrowski, "Prospects for the application of biometrics in the polish banking sector," *Equilibrium. Quarterly Journal of Economics and Economic Policy*, vol. 12, no. 3, pp. 501–518, 2017.

[15] J. Woodward, "Biometrics: privacy's foe or privacy's friend?" 1997.

[16] A. E. Hassanien, M. Tolba, and A. T. Azar, "Advanced machine learning technologies and applications," in *Second international conference, AMLTA*, vol. 488. Springer, 2014.

[17] E. Cherrat, R. Alaoui, and H. Bouzahir, "Système d'identification biométrique par fusion multimodale."

[18] G. Hu, K. Wang, Y. Peng, M. Qiu, J. Shi, and L. Liu, "Deep learning methods for underwater target feature extraction and recognition," *Computational intelligence and neuroscience*, vol. 2018, 2018.

[19] G. Bonaccorso, *Machine learning algorithms*. Packt Publishing Ltd, 2017.

[20] R. Rahadian and S. Suyanto, "Deep residual neural network for age classification with face image," in *2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE, 2019, pp. 21–24.

[21] X. Yang, Y. Ye, X. Li, R. Y. Lau, X. Zhang, and X. Huang, "Hyperspectral image classification with deep learning models," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 56, no. 9, pp. 5408–5423, 2018.

[22] W. Zhang, X. He, and W. Lu, "Exploring discriminative representations for image emotion recognition with cnns," *IEEE Transactions on Multimedia*, vol. 22, no. 2, pp. 515–523, 2020.

[23] L. Liu, C. Shen, and A. van den Hengel, "The treasure beneath convolutional layers: Cross-convolutional-layer pooling for image classification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 4749–4757.

[24] R. Zhang, Q. Wang, and Y. Lu, "Combination of resnet and center loss based metric learning for handwritten chinese character recognition," in *2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*, vol. 5. IEEE, 2017, pp. 25–29.

[25] H. Lei, T. Han, W. Huang, J. Y. Kuo, Z. Yu, X. He, and B. Lei, "Cross-modal transfer learning for hep-2 cell classification based on deep residual network," in *2017 IEEE International Symposium on Multimedia (ISM)*. IEEE, 2017, pp. 465–468.

[26] M.-L. Zhang and Z.-H. Zhou, "Ml-knn: A lazy learning approach to multi-label learning," *Pattern recognition*, vol. 40, no. 7, pp. 2038–2048, 2007.

[27] R. Noori, A. Karbassi, A. Moghaddamnia, D. Han, M. Zokaei-Ashtiani, A. Farokhnia, and M. G. Gousheh, "Assessment of input variables determination on the svm model performance using pca, gamma test, and forward selection techniques for monthly stream flow prediction," *Journal of hydrology*, vol. 401, no. 3-4, pp. 177–189, 2011.

[28] A. Meraoumia, S. Chitroub, H. Bendjenna, and A. Bouridane, "An automated finger-knuckle-print identification system using jointly rbf & rft classifiers," in *2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS)*. IEEE, 2016, pp. 17–22.