People's Democratic Republic of Algeria
Ministery of Higher Education and Scientific Research
Mohamed El Bachir El Ibrahimi University of Bordj Bou Arréridj
Faculty of Mathematics and Informatics
Informatics Department

DISSERTATION

Presented in fulfillment of the requirements of obtaining the degree

Master in Informatics

Specialty: Networks and Multimedia

THEME

Deep Features for FKP Verification Systems

Presented by :

Benterki Abdelghani

Ben Saci Ala Eddine

Publicly defended on: 10/06/2023

In front of the jury composed of:

President : Dr Belhadj Foudil

Examiner: Dr Khelifi Hakima

Supervisor: Dr Benabid Sonia

2022/2023

Dedication

Abdelghani

I offer this significant moment in my life as a tribute to the memory of my beloved father. It is my heartfelt wish that, from the realm he now resides in, he perceives this simple gesture as an expression of gratitude from a son who has consistently prayed for the salvation of his soul. May the Almighty and Merciful God bestow His divine mercy upon the departed and grant him entrance into His expansive paradise.

To my dear mother, no matter what I do or say, I will never be able to thank you as you deserve.

Finally, I extend my sincerest thanks to all my siblings and their spouses and to my three nephews. Without you i would never be here

Ala Eddine

To my Father I dedicate this humble work to

his memory , I constantly pray to the good god , that he

may grant you his mercy .

To my dear mother, no matter what I do or say, I will never be able to thank you as you deserve.

To my siblings , and all of my family and

my dear friends. i am indebted to all of you for your love,

support and encouragement. I could not finish without

saying thank you for everything.

Acknowledgment

All our gratitude and thanks go to our Almighty **God** who gave us the strength, patience, courage and will to carry out this work.

our sincere thanks go to the **president** and the members of **jury** who did us the honor of reviewing this work.

we particularly thank our supervisors **Dr.Benabid Sonia** and **Dr.Attia Abdelouhab**.

To our **mothers** and **siblings**, who have given us support and sympathy throughout these years of work, know that it gives us great pleasure to express our heartfelt thanks to you.

Abstract

Biometrics refers to the automated identification of individuals through their physiological and behavioral traits. It serves as a means to ensure certainty when dealing with familiar or unfamiliar individuals, thereby determining their eligibility for specific rights or denying certain privileges. The underlying principle of biometrics is based on the assumption that individuals possess unique physical and behavioral characteristics that set them apart from others.

The advancement of human identification techniques is currently focused on the exploration of new emerging methods. This development arises from growing security concerns and the emergence of counterfeiting techniques. The emphasis lies in leveraging distinct parts of the human body that can be utilized for accurate identification, such as fingerprints, iris, and lips, among others. However, many existing systems and methods either suffer from slow processing or necessitate costly technical equipment.

Finger knuckle prints have emerged as a promising biometric modality for person identification due to their distinctiveness and stability. This master's thesis presents a comprehensive study on the use of deep features for finger knuckle print verification systems using some CNN models for feature extraction such as VGG16, ResNet50, Squeezenet and AlexNet and for classification we used the k-Nearest-Neighbor (KNN) and Linear Discriminant analysis (LDA).

Keywords : FKP, identification, deep feature, feature extraction, CNN, classification, KNN, LDA

Résumé

La biométrie fait référence à l'identification automatisée des individus à travers leurs traits physiologiques et comportementaux. Elle sert de moyen pour garantir la certitude lorsqu'on traite avec des individus familiers ou non familiers, déterminant ainsi leur admissibilité à des droits spécifiques ou refusant certains privilèges. Le principe sous-jacent de la biométrie repose sur l'hypothèse selon laquelle les individus possèdent des caractéristiques physiques et comportementales uniques qui les distinguent des autres.

Les techniques d'identification humaine évoluent actuellement vers l'exploration de nouvelles méthodes émergentes. Ce développement découle de préoccupations croissantes en matière de sécurité et de l'émergence de techniques de contrefaçon. L'accent est mis sur l'utilisation de parties distinctes du corps humain qui peuvent être utilisées pour une identification précise, telles que les empreintes digitales, l'iris et les lèvres, entre autres. Cependant, de nombreux systèmes et méthodes existants souffrent soit d'un traitement lent, soit nécessitent un équipement technique coûteux.

Les articulations des doigts ont émergé en tant que modalité biométrique prometteuse pour l'identification des personnes en raison de leur distinction et de leur stabilité. Cette thèse de master présente une étude complète sur l'utilisation de caractéristiques profondes pour les systèmes de vérification des empreintes des phalanges des doigts en utilisant certains modèles de réseaux de neurones convolutifs (CNN) tels que VGG16, ResNet50, Squeezenet et AlexNet. Pour l'extraction des caractéristiques, nous avons utilisé l'analyse du plus proche voisin (KNN) et l'analyse discriminante linéaire (LDA) pour la classification.

Mots clés : FKP, identification, caractéristique profonde, extraction de caractéristiques, CNN, classification, KNN, LDA

ملخص

تشير القياسات الحيوية إلى التحديد الآلي للأفراد من خلال سماتهم الفسيولوجية والسلوكية. إنه بمثابة وسيلة لضمان اليقين عند التعامل مع أفراد مألوفين أو غير مألوفين ، وبالتالي تحديد أهليتهم للحصول على حقوق معينة أو رفض امتيازات معينة. يعتمد المبدأ الأساسي للقياسات الحيوية على افتراض أن الأفراد يمتلكون خصائص جسدية وسلوكية فريدة تميزهم عن الآخرين.

يركز التقدم في تقنيات تحديد الهوية البشرية حاليًا على استكشاف طرق جديدة ناشئة. ينشأ هذا التطور من المخاوف الأمنية المتزايدة وظهور تقنيات التزييف. يكمن التركيز في الاستفادة من أجزاء مميزة من جسم الإنسان يمكن استخدامها لتحديد دقيق ، مثل بصمات الأصابع وقزحية العين والشفاه وغيرها. ومع ذلك ، فإن العديد من الأنظمة والطرق الحالية إما تعاني من بطء المعالجة أو تتطلب معدات تقنية باهظة الثمن.

ظهرت مفصل الإصبع كطريقة بيومترية واعدة لتحديد هوية الشخص نظرًا لتميزها واستقرارها. تقدم أطروحة الماجستير هذه دراسة شاملة حول استخدام الميزات العميقة لأنظمة التحقق من بصمات الأصابع باستخدام بعض نماذج CNN لاستخراج الميزات مثل VGG16 و ResNet50 و Squeezenet و AlexNet وللتصنيف استخدمنا k-Nearest-Neighbor (KNN) و تحليل التمييز الخطي (LDA).

الكلمات الرئيسية: FKP ، التعريف ، الميزة العميقة ، استخراج الميزات ، CNN ، التصنيف ، LDA, KNN
.

Table of contents

List of figures

List of tables

General Introduction

Biometric systems have gained significant attention in recent years as reliable means of authentication and identification. Fingerprints have long been utilized as a primary biometric modality; however, alternative biometric traits are being explored to address challenges such as skin conditions, injuries, or intentionally altered fingerprints. Finger knuckle prints, characterized by the unique patterns and textures on the knuckle region of fingers, have emerged as a promising and robust biometric trait for personal identification. Traditional finger knuckle print verification systems have relied on handcrafted features and conventional classification algorithms. However, these methods often struggle to capture the intricate details and subtle variations present in finger knuckle prints, limiting their accuracy and robustness. In recent years, the emergence of deep learning has revolutionized the field of biometrics, providing a powerful tool for feature representation and classification. This master's thesis aims to investigate the application of deep learning techniques for finger knuckle print verification systems. Specifically, it focuses on leveraging deep features extracted from finger knuckle print images using convolutional neural networks (CNNs) to improve the accuracy and reliability of the verification process. The utilization of deep features allows for the automatic learning of discriminative representations that capture the unique patterns and characteristics of finger knuckle prints.

The main structure of this research are as follows:

Chapter one : includes an introduction to the biometric concept, the basic module of a biometric system, operating modes of the biometric system. This chapter is ftnalized with an overviews of unimodale and multimodale, and at the end of this chapter we will give an definition for deep and machin learning with an explanation to the Convolutional Neural Network.

Chapter 02 : this chapter includes the state of the art of the FKP recognition system with spotlight on deep learning feature extraction modalities and classifiaction with their architecture .

Chapter 03 : the third chapter presents the results of simulations, a description of the database used. And finally we end this work with a conclusion.

Chapter 01: BIOMETRICS FUNDAMENTALS

1.1 Introduction

Biometrics falls within the technological field which makes it possible to process the verification of identity or identification of people using their individual characteristics, which can be physical or behavioral. Given its importance, this field has become a research axis in its own right. Authentication by biometrics is stronger than that using conventional means of identification such as cards, keys or passwords, because it constitutes a strong and permanent link between a natural person and his identity, in this chapter we will present biometrics and its modalities, we will start with the definition and use of biometrics. Then we describe the modules of biometric, after that we present its mode of operation, Next we will talk about biometric modalities , and we mentioned the the difference between unimodal and multimodal and we gave a simple explanation of some biometric techniques

1.2 Definition of biometrics

Biometric technology may be defined as the automated use of physiological or behavioral characteristics to determine or verify an individual’s identity. The word biometric also refers to any human physiological or behavioral characteristic which possesses the requisite biometric properties [1]. Biometric identifiers can include fingerprints, facial features, iris and retina patterns, voiceprints, and even behavioral patterns like typing rhythm. Biometric authentication is used in various applications such as access control, identity verification, and law enforcement. It offers a more secure and convenient method of identity verification compared to traditional methods like passwords or PINs, which can be easily forgotten, lost, or stolen.

1.3 Main modules in a biometric system

A biometric system typically consists four modules that work together to capture, process, and analyze biometric data. These modules include [2]:

Sensor module: The sensor module is responsible for capturing biometric data from the individual, such as fingerprint, iris, or face. The sensor module can be a camera, a scanner, or any other device that can capture biometric data.

Feature extraction module: The feature extraction module extracts the unique features from the biometric data captured by the sensor module. This module identifies the specific characteristics that are unique to an individual's biometric trait and generates a template that can be used for comparison and identification.

Matching module: The matching module compares the newly captured biometric data with the stored templates in the template storage module. This module calculates a score based on the similarity between the newly captured data and the stored template, and determines whether the individual is authenticated or identified.

Decision module: The decision module makes the final decision based on the score generated by the matching module. If the score is above a certain threshold, the individual is authenticated or identified. Otherwise, the individual is rejected.

1.4 Modes of operation of a biometric system :

There are two types of biometric recognition systems : those based on verification and those based on identification. Verification, also called authentication, consists of confirming or denying a person’s identity (am I who I claim to be ?) This is a one to one comparison ; the individual’s characteristics are compared to those presented in a reference record. As for identification, it makes it possible to establish the iden- tityof a person from a database, it is a one-to-many comparisons. Generally, biometric systems operate in three main modes : enrolment, authentication and identification. the whole process is being presented for more details [3]:

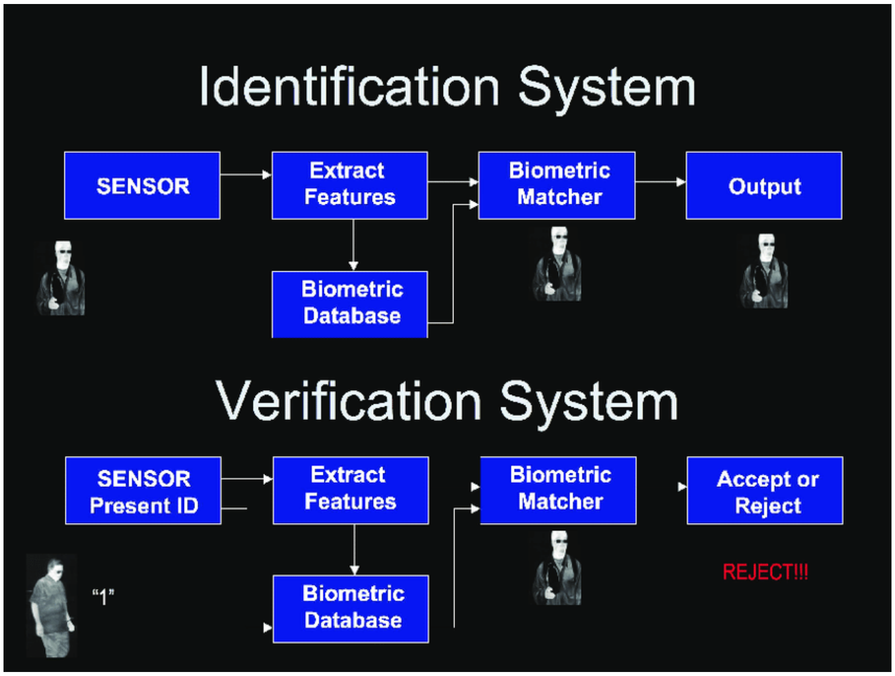

Figure 1.1- Biometric Identification vs. Verification [4].

Enrollment

The initial stage of any biometric system involves establishing a reference database and enrolling the user for the first time in the system.

Authentication

This particular step serves to authenticate an individual's identity. Essentially, the system verifies a person's identity by comparing the biometric data obtained with the individual's own stored biometric model in the database, employing a "one against one" comparison approach. The verification mode of a biometric system aims to answer the question, "Is this truly me?" Its purpose is to prevent multiple individuals from using the same identity.

Identification

This mode involves the recognition of individuals within a biometric system. The system performs a comparison between the identity of an unidentified person and the models of all individuals registered in the database, known as a 1:N match. The fundamental question being answered is, "Is this person familiar to the system?" If the person's identity does not match any of the identity models stored in the database, they will typically be rejected, indicating that they have not been enrolled by the system. Conversely, if there is a match, the person will be accepted [5].

1.5 Biometric modalities

Biometric modalities are robust, distinctive, and measurable physical characteristics that are difficult to change and impossible to steal or share.There are three biometric families [6]: morphological, biological and behavioral. Morphological modality is based on specific physical characteristics such as fingerprint, face, fingerprint, palm print, and retina, etc. The behavioral modality is based on the analysis of certain behaviors of people such as voice, signature, typing on the keyboard, etc. While the biological modality is based on the analysis of biological traces such as smell, saliva or DNA, etc.

Biological modality

This category is based on the analysis of biological characteristics of the person. It includes: smell, DNA, and physiological signals. Note that there are other biological modalities of biometric recognition that have been developed in recent years such as saliva, smell, blood type, hair and body hair, etc [7].

- **DNA**: DNA biometrics is a very reliable technique that uses genetic fingerprinting. This imprint is obtained following an analysis of biological tissues such as hair, blood, saliva. DNA fingerprint recognition is one of the most secure and accurate technologies. However, DNA analysis cannot, for the moment, be adapted to rapid recognition and it is expensive, since it requires specific analysis laboratories. Therefore, its use is limited to the recognition of family ties or criminals. DNA is not widely used for logical and physical access control [8].

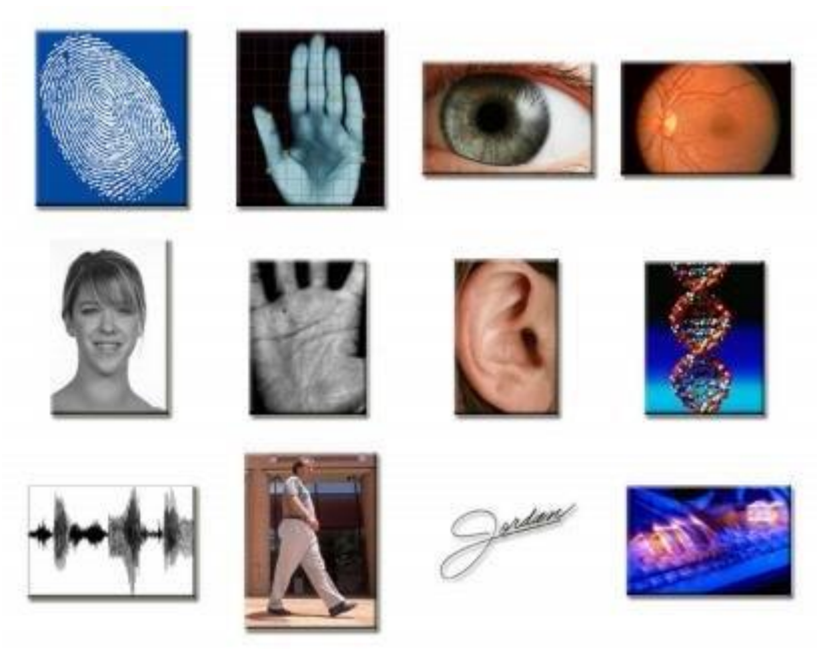

Figure 1.2- Different biometric modalities [2].

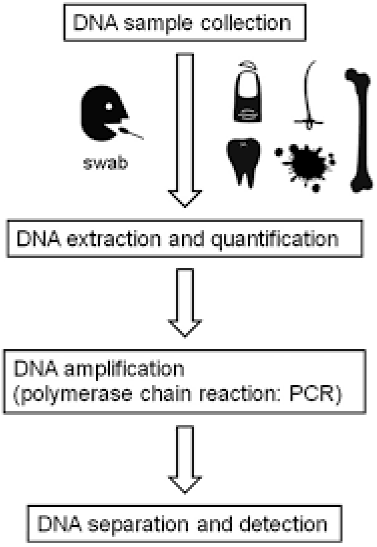
DNA sample collection
swab
DNA extraction and quantification
DNA amplification
(polymerase chain reaction: PCR)
DNA separation and detection

Figure 1.3- DNA [9].

Behavioral modality

Behavioral modality is based on the analysis of a person's physical behaviors such as signature, voice, typing style, and walking style, etc.

- **The signature**: this type of modality consists in measuring several specificities of the

  signature: speed, movement, pressure on the pencil and accelerations, etc. The device is generally associated with a graphic palette with a pen. The advantage of this modality is that it is very well accepted by the public. While its weak point is the reproduction of the signature by the same person. In addition, the nature of the signature depends on several factors such as stress, age and fatigue which hinder recognition [10].

Figure 1.4- Signature image.

- **Voice:** voice recognition is a technique for analyzing speech picked up by a microphone. It uses voice characteristics such as frequency, loudness and pitch to identify people. Its strong point is that it allows remote recognition, and is easy to implement with a simple microphone, as a speech acquisition device. However, it can be influenced by the noise, age or emotional state of the person [7].

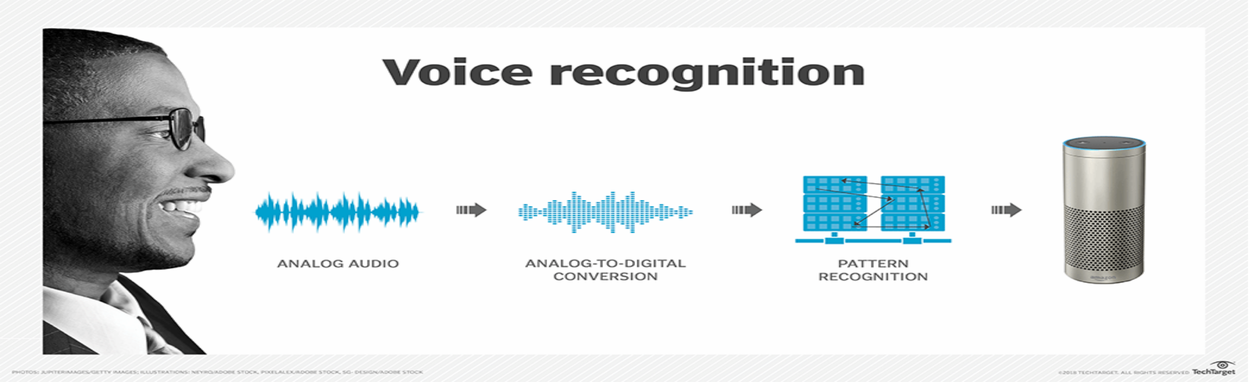

Figure 1.5– Voice recognition.

Morphological modality :

This category is based on the analysis of the particular and permanent physical characteristics of each person. These own physical traits are fingerprint, face, hand geometry, hand vein design, iris, retina, fingerprints finger joints. These elements have the advantage of being stable throughout the life of an individual and are not influenced by physiological factors such as stress or fatigue, from which the behavioral modality suffers [7].

- **Fingerprint:** this type of measurement uses the design represented by the ridges and furrows of the epidermis of the fingers. This drawing is unique and different for each individual. We extract the main characteristics (Extraction of the minutiae) such as the bifurcations of ridges, the "islands", the lines which disappear, etc [11].

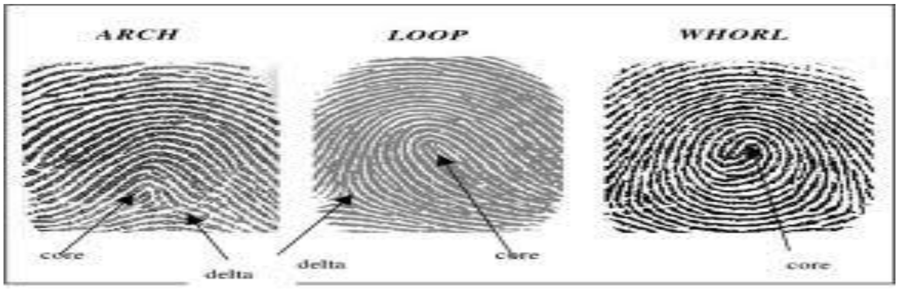

Figure 1.6- Representation of a fingerprint.

- **The retina:** it is the photosensitive film located at the back of the eye. This technique uses the patterns formed by the blood vessels of the retina unique to each individual and fairly stable over the person's lifetime[7].

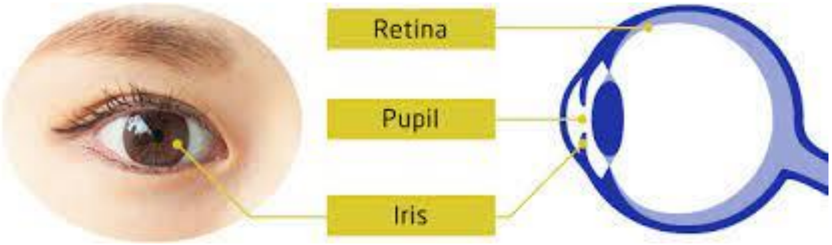

Figure 1.7– Recognition of the retina.

- **Impressions of the finger joints (FKP)** : it is a biometric technology based on the back surface of the finger, it contains distinctive features such as main lines, secondary lines and ridges, which can be extracted from the low resolution images

  The hand contains several fingers, for this, it is necessary to keep the information on each finger for precise recognition in the identification field [12].

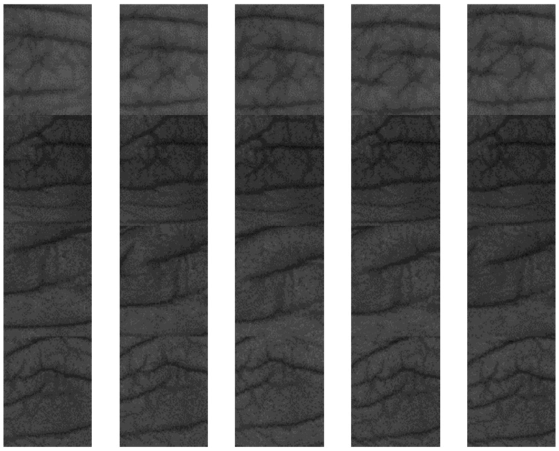

Figure 1.8- Biometric system based on finger joints.

Table I.1- Comparison between biometric modalities

Biometric Modality	Accuracy	User Acceptance	Cost	Security	False Acceptance Rate	False Rejection Rate
Fingerprint Recognition	High	High	Low	Medium	Low	Low
Face Recognition	Medium-High	High	Medium	Medium	Medium	Medium-High
Iris Scanning	High	Low	High	High	Low	Low
Voice Recognition	Medium	Medium	Low	Low	Medium	Medium-High
Hand Geometry	Medium	High	Medium	Medium	Medium	Medium
Signature Recognition	Medium	Medium	Low	Low	Medium	Medium
Gait Recognition	Low-Medium	Low	High	High	High	High

1.6 Criteria for evaluating biometric modalities:

Each biometric modality must satisfy certain conditions in order to be used as a valid biometric characteristic. These conditions are [13]:

Accuracy: Accuracy refers to the ability of the biometric modality to correctly identify or authenticate an individual. The accuracy of a biometric modality is typically measured in terms of false acceptance rate (FAR) and false rejection rate (FRR). A lower FAR and FRR indicates a more accurate biometric modality.

User Acceptance: User acceptance refers to how comfortable individuals are with using a particular biometric modality. This can depend on factors such as ease of use, privacy concerns, and cultural factors.

Cost: The cost of a biometric modality includes not only the cost of the hardware and software, but also the cost of installation, maintenance, and training. A more cost-effective biometric modality is generally preferred.

Security: Biometric modalities must be secure to prevent unauthorized access to sensitive information or areas. This can depend on factors such as the uniqueness of the biometric trait, the difficulty of spoofing or hacking the system, and the robustness of the encryption used to protect data.

Scalability: The ability of a biometric modality to scale up or down based on changing demands is an important consideration. A scalable biometric modality can be deployed in various settings and can accommodate different levels of usage.

Environmental Factors: Environmental factors such as lighting, temperature, and noise levels can affect the accuracy of certain biometric modalities. Evaluating the performance of a biometric modality under different environmental conditions is therefore important.

Interoperability: Biometric modalities should be able to interface with other systems and technologies to ensure seamless integration into existing workflows.

1.7 Unimodal and Multimodal Biometrics System

Biometric recognition systems employ either unimodal or multimodal biometrics. Unimodal biometrics rely on a single trait of an individual, such as finger vein, face, or iris. In contrast, multimodal biometrics combine multiple biometric modalities to enhance system security and accuracy. This approach typically involves using more than one biometric credential, such as a combination of finger vein and fingerprints, instead of relying on a single trait. By integrating multiple biometric features, multimodal systems can overcome limitations commonly faced by unimodal systems. Over the years, the utilization of multiple biometric features in combination has significantly reduced error rates.

Unimodal Biometric System

The unimodal biometric systems have many advantages, it has to face a large

number of problems like [14] :

- Noisy data
- Interclass similarities
- Non-universality
- Spoofing attacks

To solve this problem is to use a multimodal system which does not depend on one source of future extraction for the person.

Multimodal Biometric System

The limitations of unimodal biometrics can be overcome by incorporating multiple sources of information to establish a person's identity.

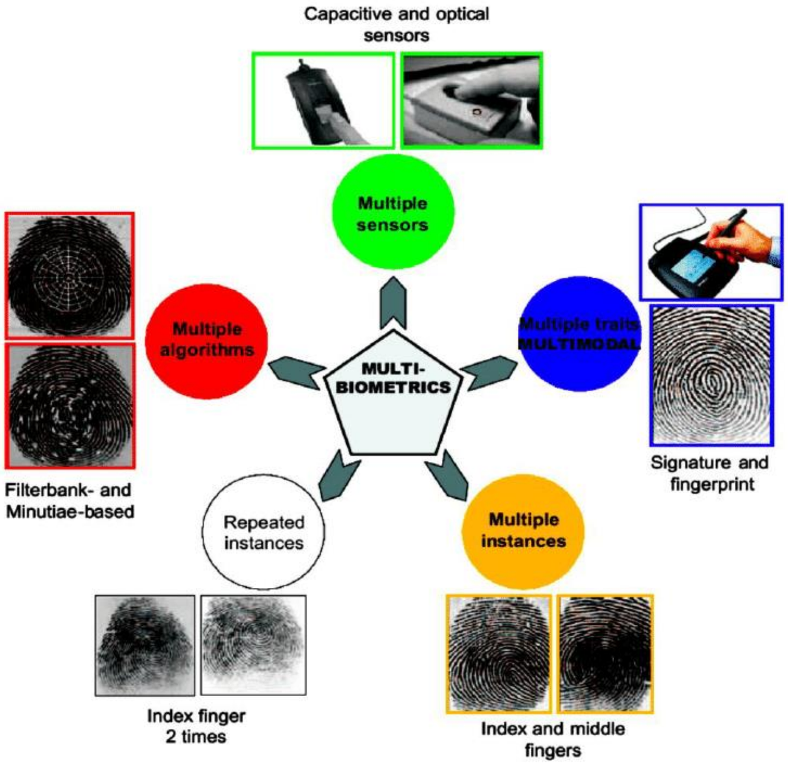

Figure 1.9– Different categories of the multimodal biometric system [15].

1.8 Machine learning

Machine learning is a field that utilizes computer technologies capable of learning from data and making predictions without explicit programming [17]. In the context of biometric comparisons, the challenge of "unclear comparison" arises due to the reduced accuracy of repeated biometric measurements. To overcome this challenge, biometric algorithms employ machine learning techniques such as neural networks, fuzzy logic, and evolutionary computation. Machine learning stands out for its ability to handle noise and solve intricate pattern recognition problems, as well as its adaptability and utilization of parallel computing architectures. These qualities enable it to effectively simulate complex biological features and generate precise mathematical models without heavy reliance on assumptions. Exploiting these characteristics, machine learning has demonstrated success in extracting and matching biometric information. However, the application of machine learning methods to vascular biometrics remains limited, with few studies conducted in this area.

1.9 Deep learning

In recent years, deep learning (DL) has gained prominence as a feasible choice for extensive applications, owing to notable advancements. These advancements encompass the abundance of data, the emergence of storage technologies capable of managing substantial data volumes, and the escalated computational power facilitating the processing of vast amounts of information [16]. Additionally, the availability of AI frameworks offered by platforms like Kaggle and Google Cloud Platform has democratized the development of AI, allowing individuals without a background in data science to delve into AI-driven solutions, even within the domain of cybersecurity.

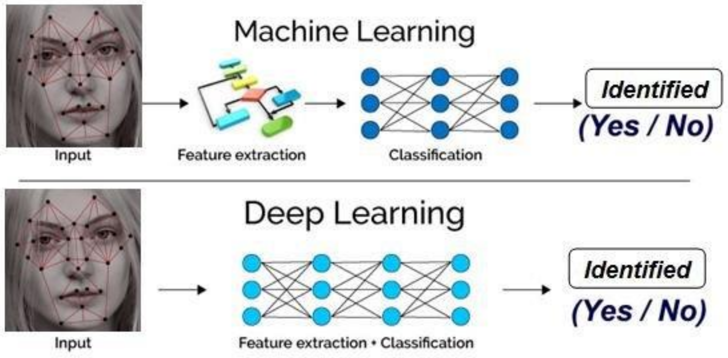

Figure 1.10- Key Demarcation Points in Deep Learning and Machine Learning [18]

1.10 Convolutional Neural Network

Definition

In the domain of deep learning, the convolutional neural network (CNN) stands out as a specialized form of deep neural networks predominantly used for visual image analysis. In contrast to conventional neural networks that rely heavily on matrix multiplications, CNNs employ a distinctive approach called convolution. This technique involves performing a mathematical operation between two functions to produce a third function that captures the transformation of one function by the other, ultimately reshaping it [19].

CNN architecture

The CNN architecture, is a specialized deep learning network specifically crafted for tasks related to image processing and analysis. It comprises a series of interconnected layers, each with a distinct role in the learning process. The essential components of a typical CNN architecture are as follows:

Convolutional Layers: These layers apply convolutions to the input data, extracting local features by utilizing filters or kernels across the image. The resulting output is known as feature maps.

Pooling Layers: Pooling layers downsample the feature maps, reducing their spatial dimensions while preserving the most significant information. This aids in reducing computational complexity and enhances the network's robustness to input variations.

Activation Functions: Activation functions introduce non-linearity to the network, enabling it to learn intricate patterns and relationships within the data. Popular activation functions include Rectified Linear Unit (ReLU) and sigmoid.

Fully Connected Layers: Fully connected layers establish connections between every neuron from the previous layer to the subsequent layer, similar to conventional neural networks. These layers perform high-level feature extraction and decision-making based on the features learned by earlier layers.

Output Layer: The final layer of the CNN architecture generates predictions or classifications based on the learned features. The choice of activation function in this layer depends on the problem at hand, such as softmax for multi-class classification or sigmoid for binary classification.

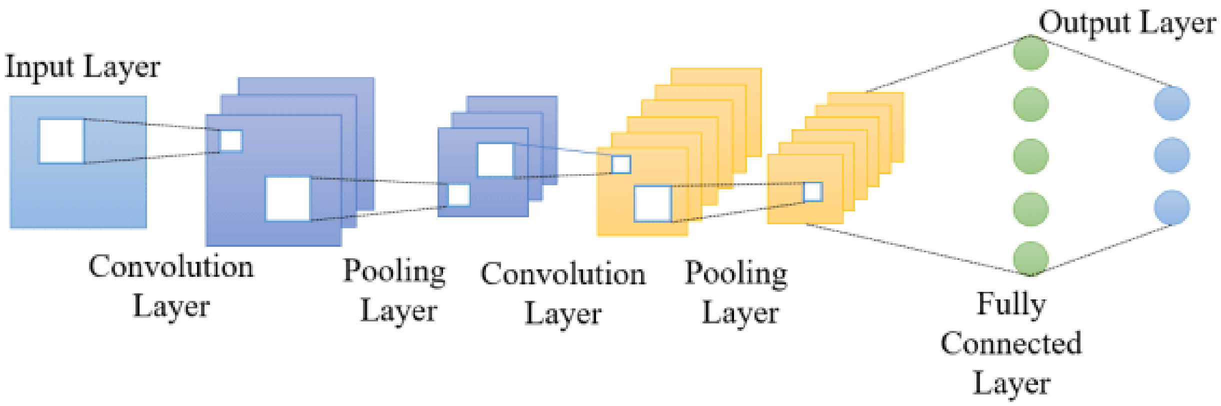

Figure 1.11- Basic architecture of CNN [20].

1.11 Conclusion

In the first section, we presented an overview of biometric recognition , followed by an explanation of internal structure of a biometric system and their operating modes, and we mentioned the the difference between unimodal and multimodal and we gave a simple explanation of some biometric techniques. The next chapter is devoted to the presentation of the different concepts related to deep features and convolutional neural networks (CNN).

CHAPTER 02: THE PROPOSED FKP RECOGNITION SYSTEM

2.1 Introduction

In this chapter, we discuss the state of the art of finger knuckle print recognition in the last years. Then, we propose our finger knuckle print recognition system and its components. A detail description of each part of our system is provided in order to give an idea about methods and techniques used in this work.

2.2 The FKP recognition state-of-art

Deep learning is a powerful form of machine learning that utilizes multiple layers of learning algorithms, enabling it to learn hierarchical representations and characteristics from data. As a result, deep learning has replaced traditional feature extraction methods in various domains, including computer vision, speech processing, and natural language processing. Biometrics is one such field that has benefited from the advancements in deep learning. Recent studies have demonstrated the effectiveness of deep learning models in finger knuckle print recognition (Fkp). For example, **M. Kumari, et al. (2019) [31]** proposed a finger knuckle print verification system based on deep learning features. The authors utilized a pre-trained convolutional neural network (CNN) as a feature extractor and achieved superior performance compared to traditional methods**.** **Z. Liu, et al. (2020) [32]** The authors introduced an enhanced finger knuckle print verification system that combined local derivative patterns and Gabor filters. This approach improved the recognition accuracy by effectively capturing the unique texture patterns present in finger knuckle prints. **L. Cao, et al. (2020) [33]** This research proposed a hybrid approach combining handcrafted features and deep neural networks for finger knuckle print recognition. The authors incorporated Gabor filters, local binary patterns (LBP), and histogram of oriented gradients (HOG) features along with a deep neural network model, achieving state-of-the-art performance. **X. Zeng, al. (2021) [34]** The authors developed a multi-scale finger knuckle print recognition system that utilized deep features. By considering different scales of the finger knuckle region, they achieved improved recognition accuracy compared to single-scale methods. The deep features were extracted using CNN. **Heidari and Chalechale (2020) [35]** the authors presented a unique FKP biometric system in which the feature extraction is a mix of the entropy-based pattern histogram (EPH) and a set of statistical texture characteristics (SSTF). The genetic algorithm (GA) was used to find the best characteristics among the retrieved features.

2.3 The proposed method

The Recognition System process consists of four main steps in Training : Preprocessing, extraction of features, Feature Fusion and classifiers. and in the test : Preprocessing, extraction of features and Final Decisions.

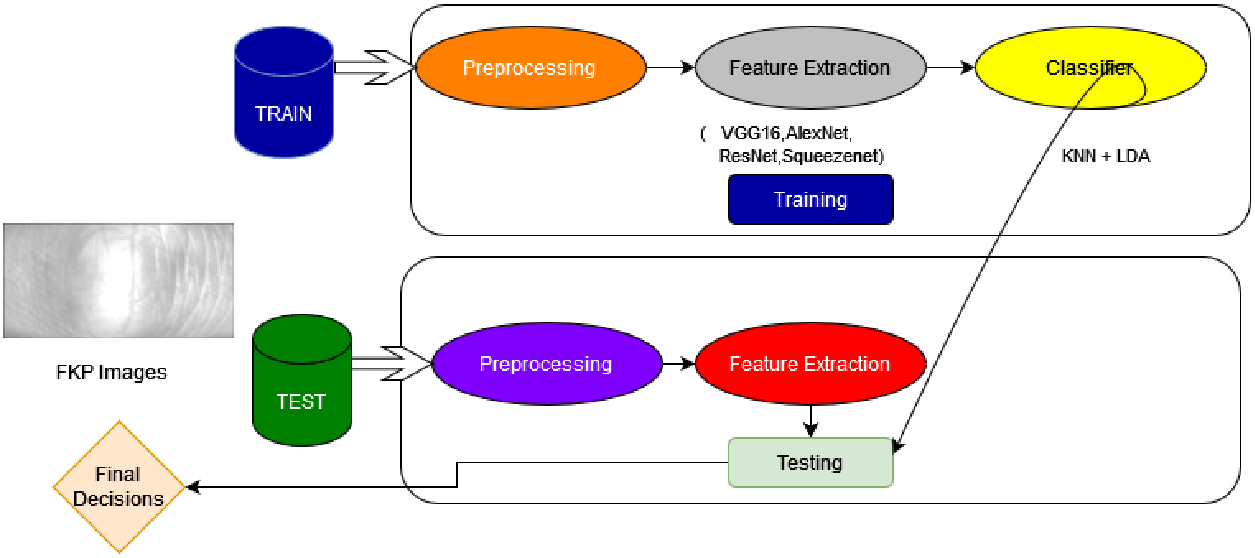

Figure 2.1- The proposed system framework.

Preprocessing

Preprocess the finger knuckle images to enhance their quality and remove any noise or artifacts. This involve techniques such as image cropping, resizing, and normalization.

Feature Extraction

Extract features from the finger knuckle print images using deep feature techniques. For this, we started a series of tests where we worked on four models of it (VGG16, ResNet50, AlexNet and SqueezeNet).

- **VGG16:** VGG16, the winning architecture of the 2014 ILSVR (ImageNet) competition [21], remains highly regarded in the field of vision models. What sets VGG16 apart is its emphasis on using 3x3 filter convolutional layers and consistently applying 2x2 filter max pool layers with the same padding. This architecture follows a consistent pattern of convolutions and max pooling layers throughout [22]. It concludes with 2 fully connected layers (FCs) and a SoftMax output. The "16" in VGG16 indicates the presence of 16 weight layers, making it a relatively large network with approximately 138 million parameters.

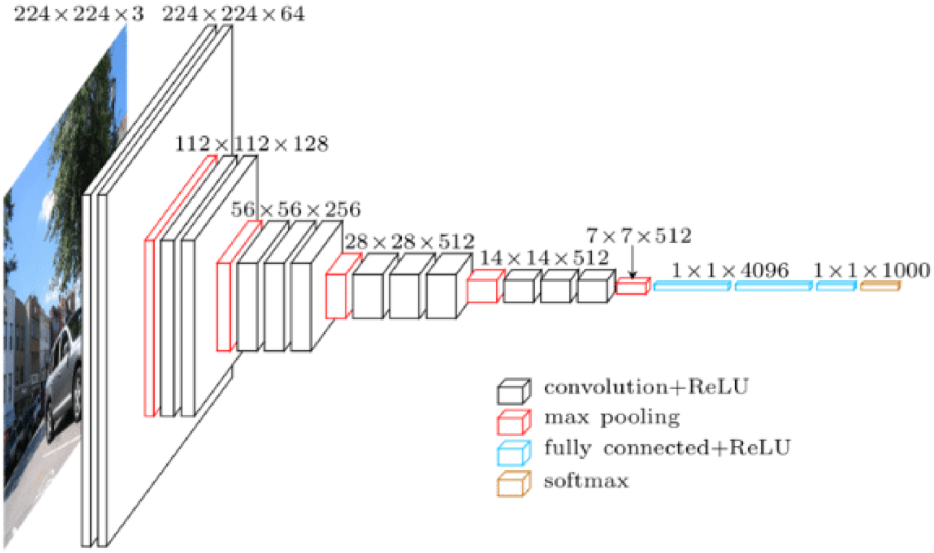

Figure 2.2- VGG16 architecture [23].

- **ResNet50:** The ResNet model is made up of small building blocks called the residual block. Each residual block is primarily made up of two to three convolution layers (this is dependent on the depth of the network) stacked together. The convolution layers are designed to learn and fit against the residual of the target function. The learned residual is then mapped back to the learned function through a skip connection that connects the input of the residual

  block to the output of the stacked convolution layers. By designing the neural network to learn and optimise on the residual instead of the original function, ResNet can learn the unknown original function more easily, thereby improving accuracy. We used the ResNet-50 architecture, which comprises 49 convolution layers organised into residual blocks and a fully connected layer for classification [25].

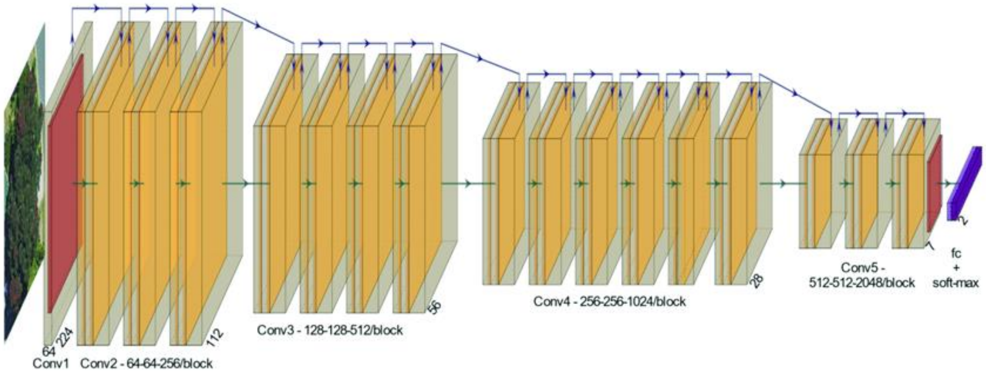

Figure 2.3- ResNet50 architecture [24]

- **Squeezenet:** as it is depicted in Figure II.6 [27], SqueezeNet begins with a standalone convolution layer (conv1), followed by 8 Fire modules (fire2-9), ending with a final conv layer (conv10). A Fire module is comprised of a squeeze convolution layer (which has only 1x1 filters), feeding into an expand layer that has a mix of 1x1 and 3x3 convolution filters. The number of filters per fire module are gradually increased from the beginning to the end of the network. SqueezeNet performs max-pooling with a stride of 2 after conv1, fire4, fire8, and conv10. It is also worth noting that in SqueezeNet there are not any fully -connected layers.

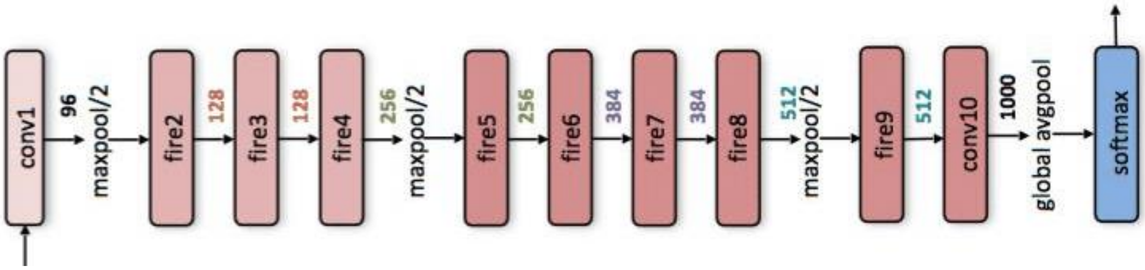

Figure 2.4- Squeezenet architecture [25].

- **AlexNet:** which was first proposed by Alex Krizhevsky et al. in the 2012 ImageNet Large Scale Visual Recognition Challenge (ILSVRC-2012), is a fundamental, simple, and effective CNN architecture, which is mainly composed of cascaded stages, namely, convolution layers, pooling layers, rectified linear unit (ReLU) layers and fully connected layers. Specifically, AlexNet is composed of five convolutional layers, the first layer, the second layer, the third layer and the fourth layer followed by the pooling layer, and the fifth layer followed by three fully-connected layers [29].

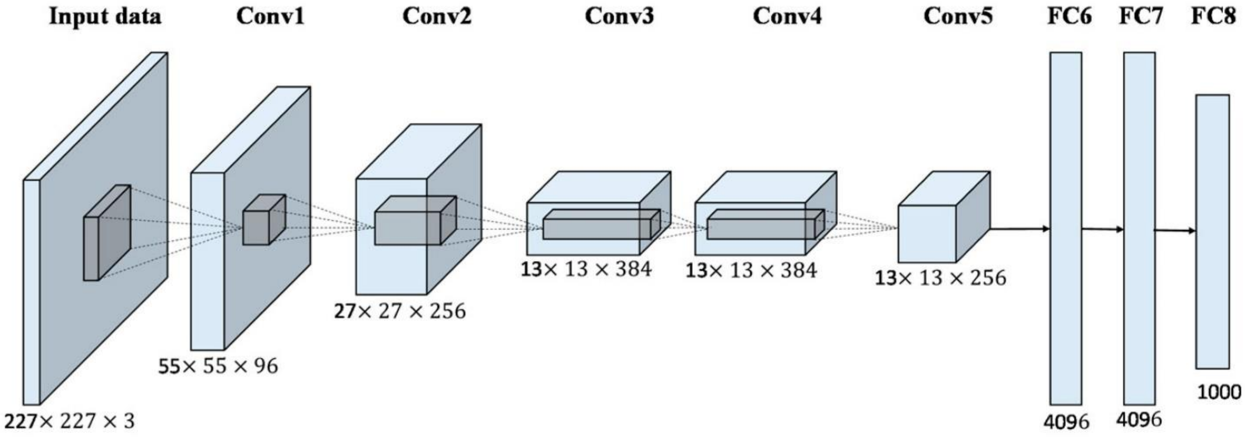

Figure 2.5- AlexNet architecture [26].

Classification

LDA: (Linear Discriminant Analysis) is a classification algorithm that aims to find a linear combination of features that maximally separates different classes in a dataset. LDA is a linear classifier that assigns data points to two different classes based on a linear category boundary (black line). The classifier has to be trained with labelled data (the class label is indicated by the color of the data points). LDA will find a category boundary, regardless of whether the data are well segregated by a linear boundary (A), or not (B). The quality of the classifier is measured by the fraction of correctly classified data points (0.95 for A versus 0.58 for B) [30].

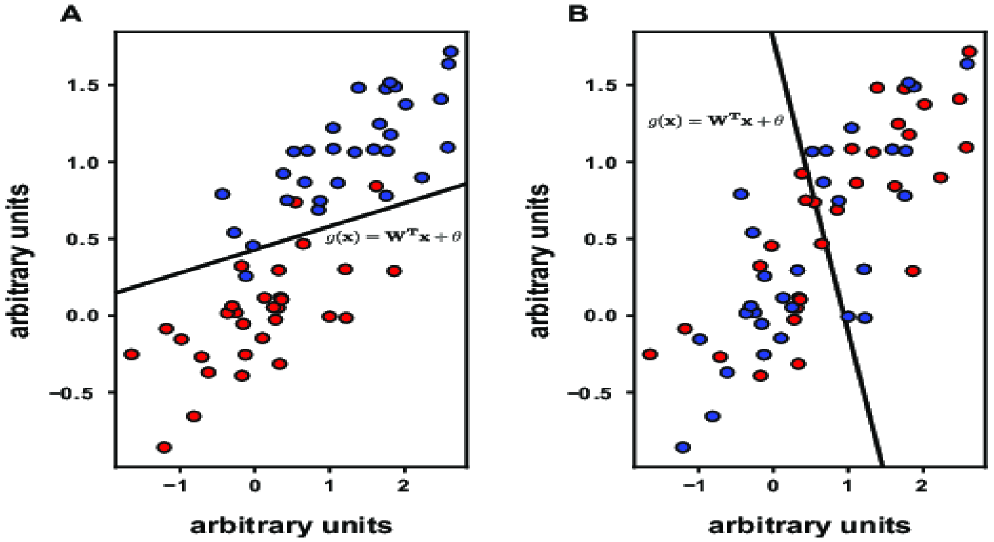

Figure 2.6- Illustration of linear discriminant analysis (LDA) [27].

K-Nearest Neighbor (KNN): KNN does not require any parameters for its working. Euclidean distance is used to measure the distance between neighbors. Figure 2.11 shows the basic principle behind the KNN classification algorithm, used to classify a new data instance into already observed classes based on its relative distance to either of the classes. The green squares depict the normal behavior class and red triangles show the abnormal behavior class, any newly observed unknown instance (blue hexagon) can now be classified based on the number of maximum nearest neighbors from either of the classes. Accordingly, this new instance is classified as a known class. k is the number of nearest neighbors used for classification [31].

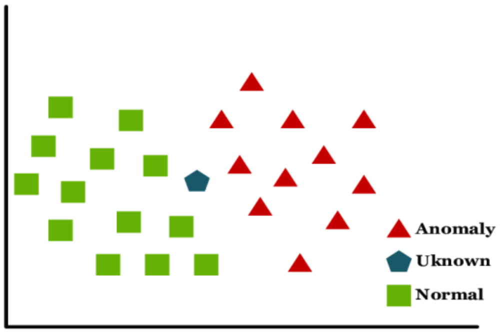

Figure 2.7- K-Nearest Neighbor (KNN) classification principle [28].

2.4 CONCLUSION

We have discussed in this chapter the state of the art of finger knuckle print recognition for deep feature, we have seen the preprossicng of our database and explained the different architectures of CNN. In the next chapter, we will report our different results with quantitative and qualitative discussions to bring out the strengths and weaknesses of our system.

Chapter 03 : RESULTS AND DISCUSSIONS

3.1 INTRODUCTION

In this chapter, we give a detailed description to our used database Then, we provided an explanation to the evaluation metrics that used in this work .we will report our different results with quantitative and qualitative discussions to bring out the strengths and weaknesses of our system.

3.2 Dataset descreption

To accomplish the study's objectives, particularly in the context of utilizing deep learning, we have chosen to utilize the Hong Kong Polytechnic University (PolyU) database. The PolyU FKP database comprises a total of 7920 images obtained from 165 individuals, consisting of 125 males and 40 females. Among these individuals, 143 subjects fall within the age range of 20 to 30 years, while the remaining individuals are between 30 to 50 years old. Each person in the database has contributed 48 distinct FKP images, with a specific distribution across the fingers. Specifically, all individuals have provided 12 images each for the Left Index Finger (LIF) and Left Middle Finger (LMF), as well as 12 images each for the Right Index Finger (RIF) and Right Middle Finger (RMF). Thus, the total number of images available for the Right Middle Finger (RMF), Right Index Finger (RIF), Left Index Finger (LIF), and Left Middle Finger (LMF) collectively amounts to 1980 images, provided by the 165 individuals [29].

3.3 EVALUATION METRICS

The evaluation of biometric systems is a major challenge in biometrics for several reasons. First, it allows researchers to better test and evaluate their systems with those in the literature. Consequently, in addition, it makes it possible to identify, for each system, the industrial applications based on these performances. In the literature, there are several metrics and several types of curves to define the performance of a biometric system, here are some of the most used [2]:

False Reject Rate (FRR)

This rate determines the probability that a system will not recognize a person who should normally have been recognized. It is a ratio between the number of people legitimate persons whose access was denied and the total number of legitimate persons whomanifested [11].

$$\text{FRR} = \frac{\boldsymbol{number\ of\ rejected\ customers}}{\boldsymbol{total\ number\ of\ customer\ accesses}} \times \mathbf{100}$$

False Accept Rate (FAR)

This rate determines the probability that a system will recognize a person who normally should not have been recognized. It is a ratio between the number of people who were accepted when they should not have been and the total number of unauthorized people who tried to be accepted [3].

$$\text{FAR} = \frac{\boldsymbol{number\ of\ accpeted\ imposters}}{\boldsymbol{total\ number\ of\ imposter\ accesses}} \times \mathbf{100}$$

Equal Error Rate (EER)

This rate is calculated from the first two criteria and constitutes a point of measurement of current performance. This point corresponds to where FRR = FAR, it is the best compromise between false rejections and false acceptances [11].

$$\text{EER} = \frac{\boldsymbol{number\ of\ false\ acceptances\ +\ number\ of\ false\ rejections}}{\boldsymbol{total\ number\ of\ accesses}} \times \mathbf{100}$$

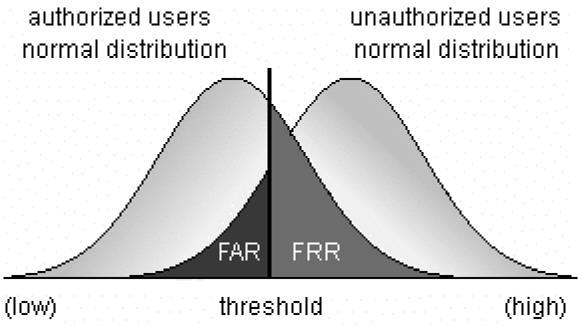

Figure 3.1- Illustration of FRR and FAR.

ROC Curve (Receiver Operating Characteristics)

The performance of a biometric system can be presented graphically using the Receiver Operating Characteristic (ROC) curve [33]. This curve represents FRR values as a function of FAR. This is obtained by calculating the torque (FAR, FRR) for all the values of the test thresholds. This differs from the smallest value obtained at a higher value. This curve can be broken down into three zones: high security zone, compromise zone and low security zone [30].

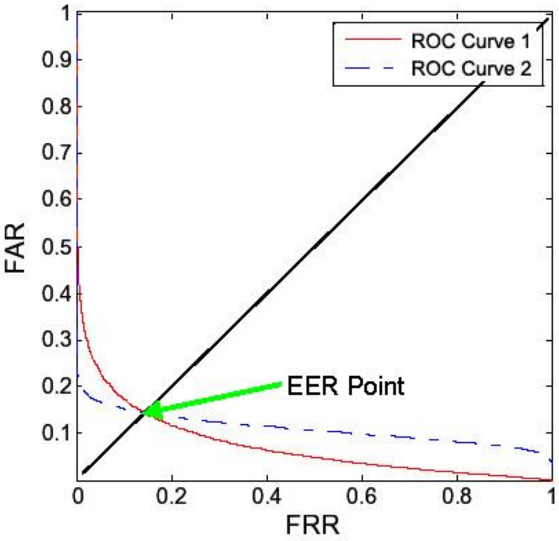

FIGURE 3.2– ROC curve.

Curve of cumulative scores (Cumulative Match Characteristic or CMC)

This curve (see figure I.15) gives the percentage of people recognized according to a variable called rank [35].

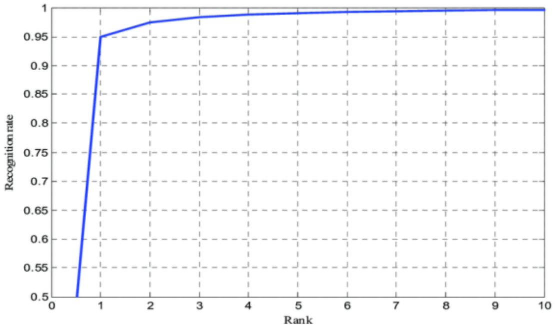

FIGURE 3.3– CMC curve.

3.4 RESULTS

Experiment 1 concerning LIF modality:

Deep features	Identification rank-1%	EER%	Verification vr@1% FAR%	Verification vr@0,1% FAR%	Verification vr@0.01% FAR%
AlexNet	94.89%	1.64%	98.10%	95.67%	91.95%
ResNet50	89.18%	2.60%	95.84%	87.79%	79.13%
Squeezenet	92.12%	3.03%	95.76%	91.72%	84.34%
VGG16	92.90%	2.01%	96.88%	92.90%	85.54%

Table 3.1: results for differents deep features for LIF modality

The table 3.1 illustrates the results of applying four deep learning models on the left index fingers, in this table we note that: All results are good with a small error value also indicate that the performance of AlexNet is better than ResNet50, Squeezenet and VGG16.

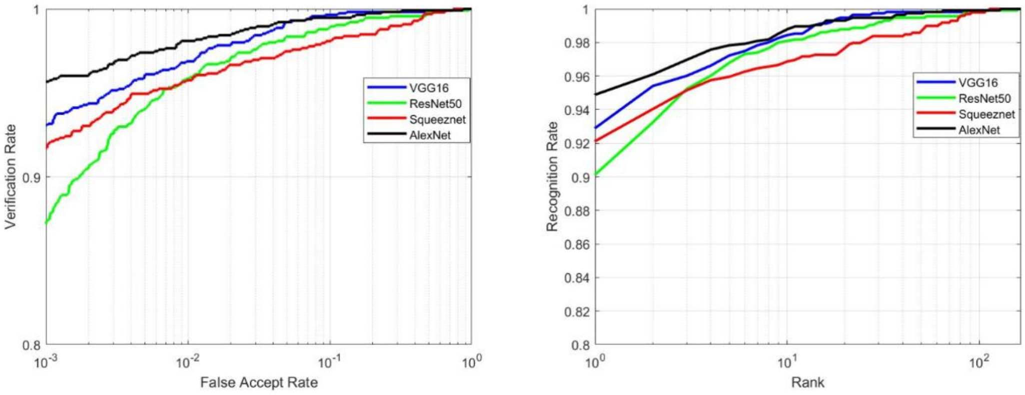

Figure 3.4-ROC curve and CMC curve of the LIF Modality

In the ROC curve we notice that the alexnet is the best method for the LIF modality because the surface of the alexnet is bigger and the verification rate is closed to 1 wich indicate a good result.

In the CMC curve we notice that the alexnet is the best method for the LIF modality because the surface of the alexnet is bigger and the recognition rate is closed to 1 wich indicate a good result.

Experiment 2 concerning RIF:

Deep features	Identification rank-1%	EER%	Verification vr@ 1% FAR%	Verification vr@0.1% FAR%	Verification vr@0.01% FAR%
AlexNet	93.16%	2.34%	96.71%	94.46%	88.83%
ResNet50	87.97%	4.76%	92.64%	85.80%	77.84%
Squeezenet	89.96%	2.69%	96.02%	91.08%	84.50%
VGG16	93.42%	2.51%	96.88%	93.59%	86.49%

Table 3.2: results for differents deep features used for RIF modality.

The table 3.2 illustrates the results of applying four deep learning models on the right index fingers, in this table we note that: All results are good with a small error value also indicate that the performance of VGG16 is better than ResNet50, Squeezenet and AlexNet

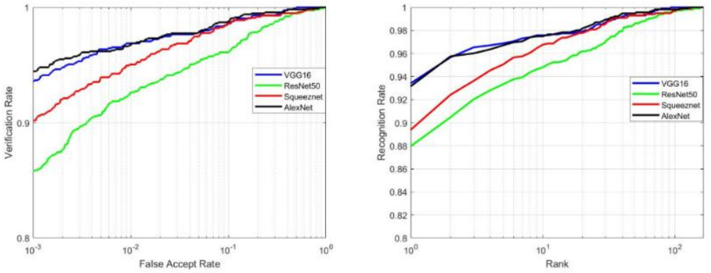

Figure 3.5-ROC curve and CMC curve of the RIF Modality

In the ROC curve we notice that the alexnet is the best method for the LIF modality because the surface of the alexnet is bigger and the verification rate is closed to 1 wich indicate a good result.

In the CMC curve we notice that the vgg16 is the best method for the LIF modality because the surface of the alexnet is bigger and the recognition rate is closed to 1 wich indicate a good result.

Experiment 3 concerning LMF:

Deep features	Identification rank-1%	EER%	Verification vr@1% FAR%	Verification vr@0,1% FAR%	Verification vr@0.01% FAR%
AlexNet	96.02%	1.56%	98.18%	96.36%	92.03%
ResNet50	91.60%	2.08%	96.54%	90.74%	78.79%
Squeezenet	94.37%	2.69%	96.54%	94.11%	88.40%
VGG16	94.20%	2.25%	96.97%	93.94%	90.04%

Table 3.3: results for differents deep features used for RIF modality.

The table 3.3 illustrates the results of applying four deep learning models on the left middle fingers, in this table we note that: All results are good with a small error value also indicate that the performance of AlexNet is better than ResNet50, Squeezenet and VGG16.

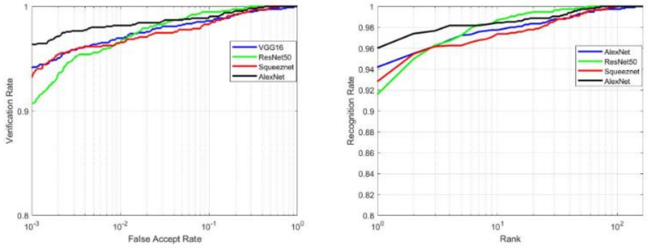

Figure 3.6-ROC curve and CMC curve of the LMF Modality

In the ROC curve we notice that the alexnet is the best method for the LIF modality because the surface of the alexnet is bigger and the verification rate is closed to 1 wich indicate a good result.

In the CMC curve we notice that the alexnet is the best method for the LIF modality because the surface of the alexnet is bigger and the recognition rate is closed to 1 wich indicate a good result.

Experiment 4 concerning RMF:

Deep features	Identification rank-1%	EER%	Verification vr@1% FAR%	Verification vr@0.1% FAR%	Verification vr@0.01% FAR%
alexnet	94.98%	1.28%	98.44%	95.24%	92.81%
resnet	91.34%	3.21%	95.24%	90.74%	85.02%
squizznet	92.99%	2.94%	96.10%	93.59%	89.35%
Vgg16	95.41%	1.37%	98.01%	95.93%	92.38%

Table 3.4: : results for differents deep features used for RIF modality.

The table 3.4 illustrates the results of applying four deep learning models on the left middle fingers, in this table we note that: All results are good with a small error value also indicate that the performance of VGG16 is better than ResNet50, Squeezenet and AlexNet.

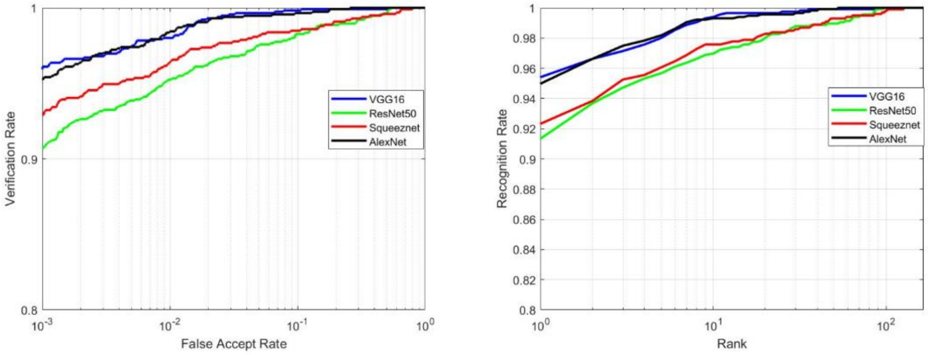

Figure 3.7-ROC curve and CMC curve of the RMF Modality

In the ROC curve we notice that the vgg16 is the best method for the LIF modality because the surface of the alexnet is bigger and the verification rate is closed to 1 wich indicate a good result.

In the CMC curve we notice that the vgg16 is the best method for the LIF modality because the surface of the alexnet is bigger and the recognition rate is closed to 1 wich indicate a good result.

After the applying of the four deep features modules on the four fkp madlities we notice that the best modules are the AlexNet and the VGG16 and we notice that the ResNet50 always give the least accuracy and in the future in order to obtain more accurate results we propose the method of fusion between the diffrent four modalities

3.5 CONCLUSION

We have discussed in this chapter our used database ,and seen the criteria that evaluate our work In this chapter, we presented some tests carried out on the different parameters used in our finger knuckle print recognition system with 4 different modalities VGG16, ResNet50, AlexNet and squizznet. using KNN and LDA as classifier.

General Conclusion

The main objective of this graduation thesis is to investigate a biometric system that utilizes deep learning techniques for accurate identification and classification of individuals based on their finger knuckles. Precision in recognition is crucial, and this biometric technology is known for its strong security features. The uniqueness of biometric characteristics makes it highly improbable for others to possess the same features, even in the case of identical twins. Our focus was on enhancing the accuracy of identification and classification in the finger knuckle biometric system (FKP) through the implementation of four methods: AlexNet, ResNet50, VGG16, and Squeezenet.

Experimental findings reveal that the the best methods are the vgg16 and the alexnet with high accuracy from the resnet50 and sqeeznet. These methods have yielded a favorable accuracy rate, which is particularly significant as it enhances the reliability of our system and enables us to achieve our initial goal of extracting finger knuckle features and effectively classifying them.

References

[1] Wang, Patrick & Yanushkevich, Svetlana. (2007). Biometric technologies and applications. Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, AIA 2007. 249-254.

[2] Morizet, Nicolas. (2009). Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris.

[3] El-Abed, 2011 El-Abed, M. (2011). Evaluation de système biométrique PhD thesis, Université de Caen.

[4] Byrd, Kenneth & Szu, Harold & Chouikha, Mohamed. (2009). Implications of the advanced mini-max (AMM) classifier on non-cooperative standoff biometrics. Proceedings of SPIE - The International Society for Optical Engineering. 7343. 10.1117/12.820832.

[5] Sabhanayagam et al, 2018 Sabhanayagam, T., Venkatesan, V. P., and Senthamaraikannan, K. (2018). A comprehensive survey on various biometric systems. International Journal of Applied Engineering Research, 13(5) :2276–2297.

[6] C. Guerrier and L.A.Cornelie, 2003 Les aspects juridiques de la biométrie. Document analyse commission accès à informations.

[7] Takwa Chihaoui. 2018. Système d'identification de personnes basé sur la rétine. Traitement du signal et de l'image [eess.SP]. Université Paris-Est; Université de Tunis El Manar, Français. NNT : 2018PESC1145. tel-02085887

[8] Hashiyada M. 2004 Development of biometric DNA ink for authentication security. Tohoku J Exp Med ;204(2):109-17. doi: 10.1620/tjem.204.109. PMID: 15383691.

[9] Masaki Hashiyada, 2011, DNA biometrics, , DOI: 10.5772/18139

[10] D. Muramatsu and T. Matsumoto. 2007, Effectiveness of pen pressure, azimuth, and altitude features for online signature verification. In International Conference on Biometrics (ICB’07), volume 4642, pp. 503-512.

[11] Aldjia BOUCETTA, 2019 , “Approches évolutionnaires multi-biométriques pour l’identification des personnes”, Thèse de doctorat en Informatique, Faculté des mathématiques et d’informatique, Université Batna 2.

[12] L. MENSSOURA, 2013 , “identification des visages humains par réseaux de nuerons“, mémoire de magister, université de Batna.

[13] S. Prabhakar, S. Pankanti, and A. K. Jain. 2003, “Biometric recognition Security and privacy concerns “, IEEE Security and Privacy, 1 : pp. 33-42.

[14] Sanjekar, P. and Patil, J. (2013). An overview of multimodal biometrics. Signal & Image Processing, 4(1) :57.

[15] Mohamed, Soltane. (2012). MULTI-MODAL BIOMETRIC AUTHENTICATIONS: CONCEPT ISSUES AND APPLICATIONS STRATEGIES. http://www.sersc.org/journals/IJAST/vol48/3.pdf. 3. 23-60.

[16] [Goodfellow et al., 2016] Goodfellow, I., Bengio, Y., and Courville, A. (2016). Deep learning. MIT press.

[17] [Bakshi and Bakshi, 2018] Bakshi, K. and Bakshi, K. (2018). Considerations for artificial intelligence and machine learning : Approaches and use cases. In 2018 IEEE Aerospace Conference, pages 1–9. IEEE.

[18] Najm, Hayder & Ansaf, Hayder & Hassen, Oday. (2019). 西南交通大学学报 AN EFFECTIVE IMPLEMENTATION OF FACE RECOGNITION USING DEEP

CONVOLUTIONAL NETWORK. Xinan Jiaotong Daxue Xuebao/Journal of Southwest Jiaotong University. 54. 10.35741/issn.0258-2724.54.5.29.

[19] Li, Zewen & Liu, Fan & Yang, Wenjie & Peng, Shouheng & Zhou, Jun. (2021). A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. IEEE Transactions on Neural Networks and Learning Systems. PP. 1-21. 10.1109/TNNLS.2021.3084827.

[20] Gu, Hao & Wang, Yu & Hong, Sheng & Gui, Guan. (2019). Blind Channel Identification Aided Generalized Automatic Modulation Recognition Based on Deep Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2934354.

[21] [Simonyan and Zisserman, 2014] Simonyan, K. and Zisserman, A. (2014). Very

deep convolutional networks for large-scale image recognition. arXiv preprint arXiv :1409.1556.

[22] [Rezende et al., 2018] Rezende, E., Ruppert, G., Carvalho, T., Theophilo, A., Ramos, F., and Geus, P. d. (2018). Malicious software classification using vgg16 deep neural network's bottleneck features. In Information Technology-New Generations, pages 51– 59. Springer.

[23] Sugata, T & Yang, C. (2017). Leaf App: Leaf recognition with deep convolutional neural networks. IOP Conference Series: Materials Science and Engineering. 273. 012004. 10.1088/17 899X/273/1/012004.

[24] Pearse, Grant & Watt, Michael & Soewarto, Julia & Tan, Alan. (2021). Deep Learning and Phenology Enhance Large-Scale Tree Species Classification in Aerial Imagery during a Biosecurity Response. Remote Sensing. 13. 1789. 10.3390/rs13091789.

[25] Fragoulis, Nikos & Pothos, Vasileios & Kastaniotis, Dimitrios & Theodorakopoulos, Ilias. (2016). A fast, embedded implementation of a Convolutional Neural Network for Image Recognition. 10.13140/RG.2.1.1778.9681.

[26] Han, Xiaobing & Zhong, Yanfei & Liqin, Cao & Zhang, Liangpei. (2017). Pre-Trained AlexNet Architecture with Pyramid Pooling and Supervision for High Spatial Resolution Remote Sensing Image Scene Classification. Remote Sensing. 9. 848. 10.3390/rs9080848.

[27] Azizi, Amir & Pusch, Roland & Koenen, Charlotte & Klatt, Sebastian & Bröcker, Franziska & Thiele, Samuel & Kellermann, Janosch & Güntürkün, Onur & Cheng, Sen. (2018). Emerging

category representation in the visual forebrain hierarchy of pigeons (Columba livia). Behavioural Brain Research. 356. 10.1016/j.bbr.2018.05.014.

[28] Ashraf, Javed & Moustafa, Nour & Khurshid, Hasnat & Debie, Essam & Haider, Waqas & Wahab, Abdul. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics. 9. 10.3390/electronics9071177.

[29] Attia, Abdelouahab & Moussaoui, Abdelouahab & Mourad, Chaa & Chahir, Youssef. (2018). Finger-Knuckle-Print Recognition System based on Features-Level Fusion of Real and Imaginary Images. ICTACT Journal on Image and Video Processing. 8. 10.21917/ijivp.2018.0252.

[30] S. Boudjelial, 2014 , " détection et identification d'individu par méthode biométrique "

UMMTO.

[31] M. Kumari, et al. (2019) "Finger-Knuckle-Print Verification Using Deep Learning Features"

[32] "Enhanced Finger-Knuckle-Print Verification System Based on Local Derivative Patterns and Gabor Filters".

[33] L. Cao, et al. (2020) "Finger-Knuckle-Print Recognition Using Hybrid Feature Extraction and Deep Neural Networks".

[34] X. Zeng, et al. (2021) "Multi-Scale Finger-Knuckle-Print Recognition Based on Deep Features" .

[35] HEIDARI, Hadis & Chalechale, Abdolah. (2020). A new biometric identity recognition system based on a combination of superior features in finger knuckle print images. TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES. 28. 238-252. 10.3906/elk-1906-12.