Ministry of Higher Education and Scientific Research

University of Kasdi Merbah Ouargla

Faculty of New Information Technologies and Communication

Department of Electronics and Telecommunications

Master Thesis In: Academic Master

Domain: Science and Technology

Field: Telecommunication

Speciality: Telecommunication Systems

Presented by

Khennag Houria

Amrane ghania

Theme

Biometric Identification System Using Hand Dorsal Related Trait

CHARGUI Abdelhakim	MCP	Ouargla University	President
KORICHI Maarouf	MCA	Ouargla University	Supervisor
BENCHAABAN Abdrezzak	MCA	Ouargla University	Examiner

2023/2024

ACKNOWLEDGMENT

First of all, we thank God, our Creator, who gave us the strength and courage to accomplish this humble work.

After that, we extend our sincere thanks to our supervisor,

Dr.Korichi Maarouf,for his continuous support, comments, and valuable guidance during the preparation of this memorandum. We also thank all members of the arbitration committee **Dr.Charguei Abdelhakim** and **Dr.Benchaaban Abdrezzk** for accepting Terrace, reading this work, and examining our humble thesis

Finally, our sincere thanks to everyone who helped us with encouragement and support, which did not stop throughout the preparation of our work.

Dedication

I humbly dedicate this work to the most important person in my life, my dear mother**, Om Elkhir**, the source of my strength and inspiration, and to the soul of my father **Abd Elkader**in heaven, who never left my heart, and to the entire **Khennag** family, from my brothers to grandchildren, for their prayers and support for me.

To everyone who taught me and guided me over the years, and to some of his teachers who have never left my memory, and to **M.Korichi** which guided me to offer the last station of my study. and to everyone who believes that science and knowledge are the key to progress and success, we would like to present this research to you, me and my beautiful colleague**Ghania**, hoping that it will contribute to knowledge and benefit.

THANK YOU.

KHENNAG HOURIA

Dedication

To the one whom God has crowned with awe and reverence, to the one whose name I carry with all pride... My dear father, **Mebarek**. To the beacon of love every day of the year, to my angel in life, to the smile of life and the secret of existence...my beloved mother, **Fatima.** To my brothers **Omar** and **Haythem** and to **my other half**.

To **Mr. korichi Maarouf**, who contributed greatly to this work, such as guiding the research ship until it docked in this picture.

To my colleague **Houria**, who overcame the difficulties in order to reach one goal To everyone who supported me in my life journey.

AMRANE GHANIA

CONTENTS

Chapter 3:Experimental Results and Discussion

List of Figures

List of tables

Acronyms

CNN Convolution Neural Network

CMC Cumulative Match Curve

DNA Deoxyde Nucleic Acide

EER Equal Error Rate

FAR False Acceptance Rate

FFR False Rejection Rate

IIT Indian Institute of Technologies

MAX Maximum

MIN Minimum

PCA Principal Component Analysis

ROI Rate of information

ROR Rank One Recognition

RPR Rank of Perfect Recognition

SUM Sum of partitions

SVM Support Vector Machine

UBS Unimodal Biometric System

VGG Visual Geometry Group

Biometrics is considered one of the most effective alternatives to ensure security based on physiological characteristics such as: (face, fingerprint, iris), behavioral characteristics such as: (voice, gait, signature), or biological features (such as saliva and ADN) that are unique to each individual.

In recent years, the dorsal hand which is used in the areas of identity verification, has gained great popularity as it is considered an effective and secure means of identifying the user and authenticating it for use on a daily basis by workers and engineers. However, we face the problem of protecting some user information, so it will be necessary to provide a security system capable of recognizing Identity is reliable.

Through this study, the possibility of using deep learning techniques using a CNN (Convolution Neural Network) algorithm to extract features and match them with SVM (Support Vector Machine) technology and classify them will be reviewed to develop a fast and effective system capable of identifying with high accuracy the user's identity using the dorsal hand.

Our work presented in this study consists of three chapters:

- The first chapter, in which we will talk about the concepts of biometrics and a general overview of its various types and methods used in the field of information security to maintain the security and comfort of users.
- In the second chapter, we will address the architecture of the dorsal hand identification system, which includes explaining the method of features extraction from images of dorsal handprints based on deep learning and evaluating the performance of the CNN algorithm for its high ability to process images and extract their features, then to achieve matching between the database and the extracted features of the person's dorsal hand. Using the SVM algorithm, which is an effective method for classifying biometric data
- The third chapter explains the experimental results by identifying users through dorsal handprints, especially the second knucklewe discussed it to determine the extent of this proposed system and its reliability.
- Finally, we will end with a general conclusion that captures what we discussed in this study.

CHAPTER

1

General Information of Biometric

1.1 Introduction

The world at the present time has become a small village thanks to the development of technology and information, due to the close distances between individuals and the speed of its services. Moreover, it is currently being used electronically through smart devices, but despite this, at the same time, these technological developments are a major problem represented in protectinthisinformation,which has become a source of concern for many professionals and consumers. Therefore, it is necessary to have a comprehensive security and protection system capable of identifying and verifying the user's identity.

The biometrics system is one of the most successful solutions that have proven its security efficiency. It is a rapidly developing technology for identifying a person. This system is also essentially a system for identifying the biological characteristics of an individual. The most common in physiological biometrics are scanning processes and iris and face and hand geometry (structure and Hand shape and fingerprints...), Or behavioral characteristics (gait, voice, signature, keystroke dynamics, etc.), Or biological characteristics such as DNA that distinguish each person from another.[1]

In addition, we will highlight the definition and importance of this system in various industries and its potential applications in enhancing the biometric authentication process.

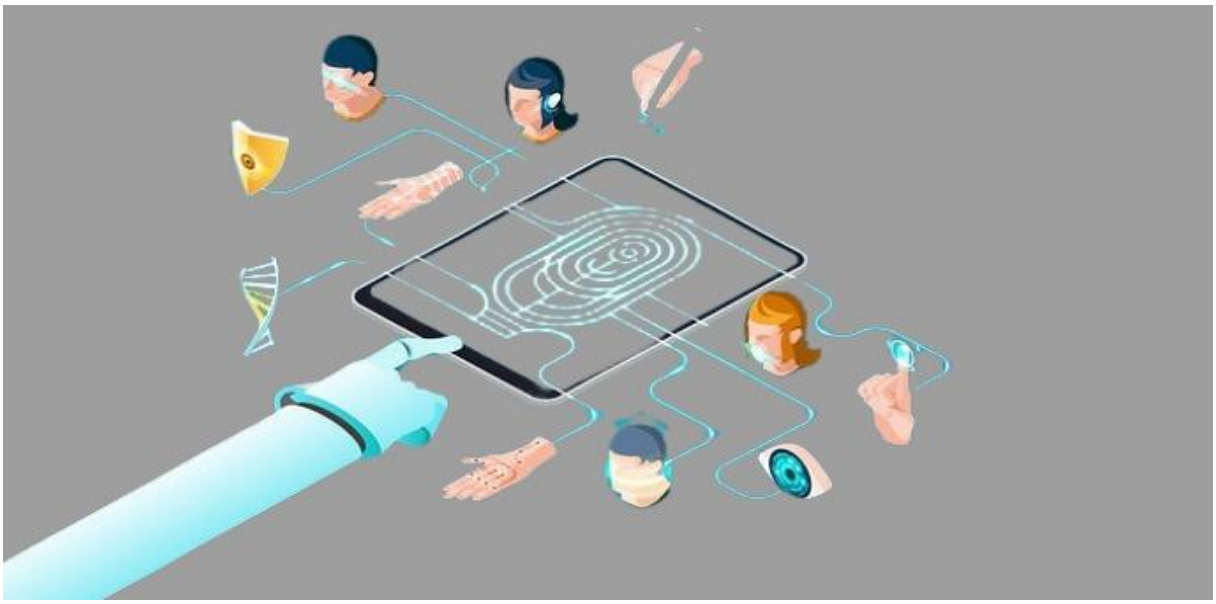

Figure 1.1: The biometrics System

1.2 Information Security Methods

Information security is a means of protecting information from unauthorized access and manipulation by anyone other than the user, with the growing need for effective biometric identification methods.

This chapter aims to give an overview of the methods used in the field of information security, first exploring traditional methods and how they came to be and are used and secondly involving biometrics-based methods.

1.2.1 Traditional Methods

Traditional authentication methods provide two traditional methods for determining an individual's personal identity, the knowledge-based method and the possession-based method, including the use of passwords, security questions, and unique authentication codes. They are easy to use for users familiar with these methods and do not require learning new technologies. It is widely available and commonly used across online platforms, making it easily adoptable and accessible by most users.

However, it faces security challenges, as attackers can exploit passwords and security questions. The need for users to manage multiple passwords can make their experience inconvenient. Additionally, human errors can lead to account closures and frustration, making these methods less than ideal in some cases. [2]

1.2.2 Biometric-Based Methods

Biometric-based authentication methods rely on unique physical or behavioral characteristics, such as fingerprints, facial recognition, or voice recognition, to verify a user's identity. Biometric authentication compares data for the person's characteristics to that person's biometric "template" to determine resemblance.

The reference model is first stored, and the data stored is then compared to the person's biometric data to be authenticated. [3]

These methods offer enhanced security compared to traditional authentication methods because biometric features are difficult to replicate or fake. They also provide a more convenient user experience, as users don't need to remember passwords or security questions. However, biometric systems may face challenges such as accuracy issues, privacy concerns regarding the storage and use of biometric data, and potential vulnerabilities to spoofing attacks. Despite these challenges, biometric authentication continues to gain popularity due to its combination of security and convenience.

1.3 Biometric System general architecture

1.3.1 Definition

Biometrics systems have had a major impact on the practices of identifying an individual's personal identity, through the significant change in the ways in which people are identified and the time taken to verify the identification process, which now takes only a few seconds.This is due to fraudsters trying to steal a person's saved data through other platforms

Biometrics is taken from the Greek language bios meaning life, and Merton orMetrikos means measurement. (The old meaning of biometrics referred to apply statistical and mathematical methods to analyze data in biological sciences. now the term also refers to techniques for identifying individuals through biological characteristics present on the body, such as fingerprints, the iris and retina, the voice, and the signature to distinguish someone from the rest of the people.[4]

-This is what the picture below shows:

Figure1.2: Taxonomy of biometric modalities.

1.3.2 Biometric Traits

Biometric traits are unique characteristics of individuals that can be measured and used for personal identification or verification. Biometric traits are utilized in various fields such as security, identity management, information technology, and many other applications that require accurate and secure individual recognition.

This section discusses some examples of different biometric modalities which are based either on biological, behavioral or morphological analysis.[5]

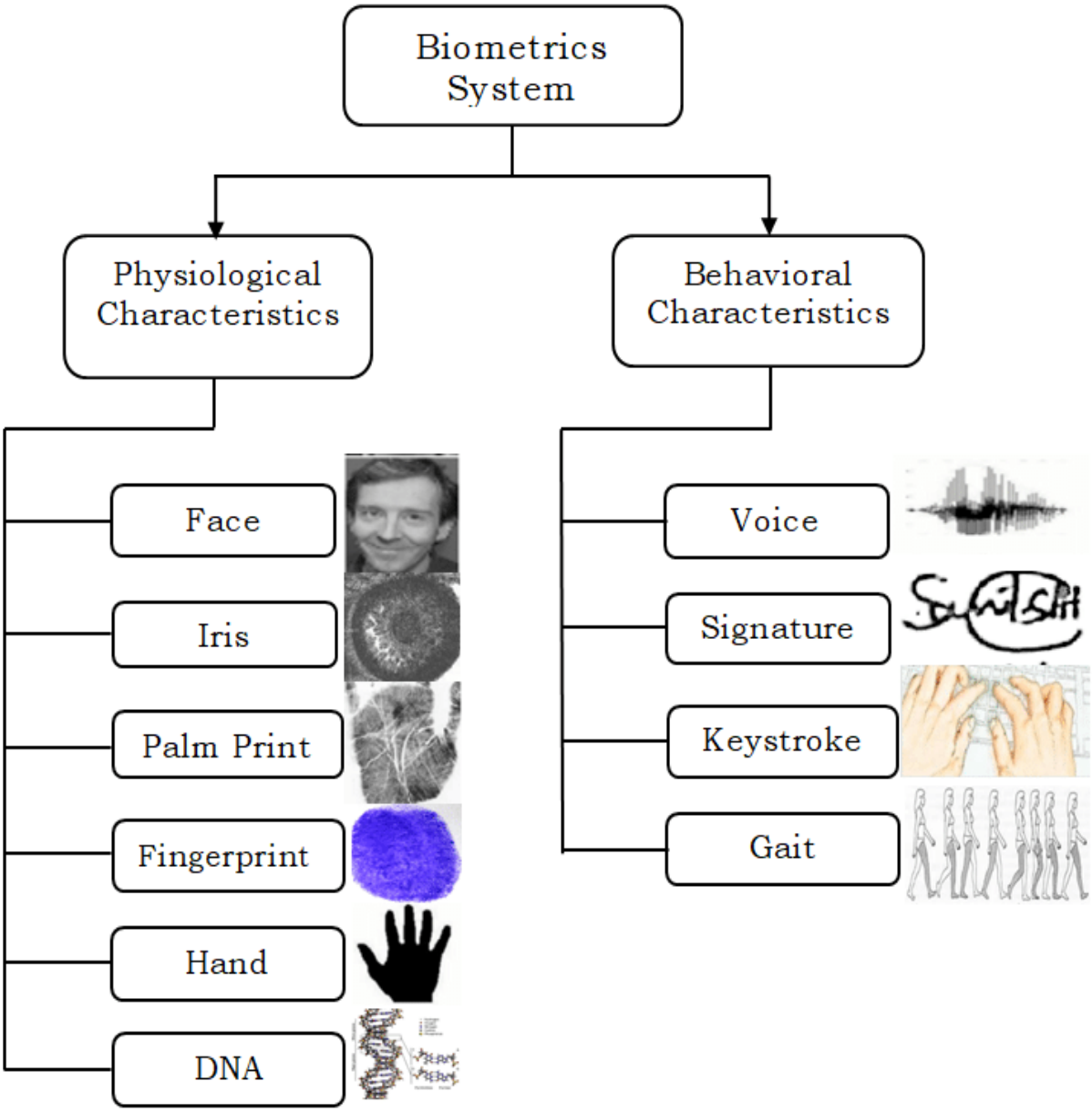

Figure 1.3: Examples of biometric characteristics.

- **Face**

Using static or video images of the face facilitates recognition, with modern approaches often relying indirectly on the locations, shapes, and spatial relationships of facial landmarks such as the eyes, nose, lips, and chin. Signal processing techniques based on localized filter responses on the images have largely replaced earlier methods relying on representing the face as a weighted combination of canonical faces. Recognition can be effective when employing canonical poses and simple backgrounds, but challenges arise when illumination and angle change, along with the potential for facial appearance alterations over time between enrollment and recognition attempts.

- **Fingerprints**

Fingerprints, the patterns of ridges and valleys on the "friction ridge" surfaces of fingers, have been utilized in forensic applications for over a century. These ridges are formed during fetal development, and even identical twins do not share the same fingerprints. The performance of current fingerprint-based recognition systems, especially those using prints from multiple fingers, is quite robust. Whether a single print or multiple prints (one from each finger) are used affects recognition accuracy, with multiple prints providing additional valuable information in large-scale systems. However, the computational intensity of large-scale fingerprint recognition systems, particularly when searching for matches among millions of references, presents a challenge.

- **Hand Geometry**

Hand geometry refers to the study of the shape of the human hand, palm size, and the lengths and widths of the fingers. Using these characteristics for identification is relatively simple and easy to use, yet it does not offer the same level of distinctiveness in large populations, typically used for verification rather than identification. Furthermore, since the devices used to capture this information must be at least hand-sized, they are often too large for devices like laptops.

- **Palm Print**

Palm prints combine some of the features of fingerprints and hand geometry. Human palms contain ridges and valleys, similar to fingerprints, but are much larger, requiring larger image

capture or scanning hardware. Palm prints, like fingerprints, have particular applications in the forensic community, as latent palm prints can often be found at crime scenes.

- **Iris**

The iris, the circular-colored membrane surrounding the eye's pupil, is complex enough to be useful for recognition. Systems utilizing this modality have shown promising performance. While early systems required significant user cooperation, modern systems are becoming increasingly user-friendly. However, iris-based systems face challenges with high False Non-Match Rates (FNMRs), partly due to the belief that the iris may change over time, though these changes over a lifetime have not been well-characterized.

- **Voice**

Voice recognition directly combines biological and behavioral characteristics. An individual's voice is based on physical aspects of the body, such as the mouth, nose, lips, vocal cords, etc., and can be influenced by age, emotional state, native language, and medical conditions. The quality of the recording device and ambient noise also affect recognition rates.

- **Signature**

Person’s signature tends to evolve over time and can be heavily influenced by various factors including physical conditions and emotional state. Despite being relatively easy to forge, signatures have long been accepted as a method of recognition.

- **Gait**

Gait, or the way a person walks, holds potential for human recognition from a distance and potentially over time. Laboratory-based gait recognition systems rely on image processing to detect the human silhouette and associated spatiotemporal attributes. Factors such as footwear choice, walking surface, and clothing can affect gait. However, gait recognition systems are still in the developmental stage.

- **Keystroke**

Keystroke dynamics, hypothesized to be distinctive to individuals, have a tradition of identifying Morse code operators by their unique patterns. These dynamics, influenced by

factors like emotional state, posture, and keyboard type, are being explored as a biometric trait.

1.3.3 Unimodal Biometric System Architecture

Presently, a variety of biometric modalities are applied to perform human identification or user verification. Unimodal biometric systems (UBS) is a technique which guarantees authentication information by processing distinctive characteristic sequences and these are fetched out from individuals.[6]

Unimodal biometric systems: unimodal biometrics or unimoetrics system designed base on a signal identifier, such as face, fingerprint, iris, plan print, etc. This type of system is useful when single biometrics evidence is available and design complexity is found to be less than that of other type of biometric system.

1.3.4 Limitation of Unimodalbiometric system

Unimodal is used in many applications; some of the main applications are border control and voter id issuance. In unimodal biometrics, theoretically it might be very proficient but in reality, it has various numbers of challenges when enrolling large number of people. The unimodal systems are not suitable for all applications; this is the major issue with the unimodal biometrics. Therefore, multimodal biometrics is used to overcome the limits of unimodal biometrics. Limits of unimodal biometrics are follows: The biometric trait uses susceptibility to remove noisy or bad data. The biometric technology uses the captured biometric data. And due to imperfect acquisition conditions, the biometric data might be distorted. By using facial recognition method, the limitations can be seen in applications. With the illumination conditions and facial expressions using these, facial images might affect the quality of the facial features. Example of fingerprint recognition method is that it leads to false database matching because the scanner is not able to read fingerprints clearly. An imposter leads to falsely accepted and enrolled person leads to incorrectly rejected. For elderly and young children, fingerprint images are not able to capture properly due to faded fingerprints or underdeveloped fingerprints ridges. And for groups of population it is not compatible. unimodal system is susceptible to inter class similarities for large population. For identical twins facial recognition method may not work correctly. Inaccurate matching is the major issue in the recognition method for identical twins, so camera cannot distinguish between the two subjects. By using uniondale biometrics, the data can be forged or imitated

due to spoof attacks. Using rubber fingerprints person information can be easily spoofed and it is possible in the fingerprint recognition systems [7]

1.4 Multimodal biometric system

1.4.1 Architecture of a biometric system

The generic architecture of a biometric system consists of five main modules as depicted in figure Storage module: It is used to store biometric individuals' templates.

- Capture module: This component involves specialized sensors or devices that capturebiometric data from individuals. Examples include fingerprint scanners, iris scanners, facial recognition cameras, voice recorders, etc.
- Matching module: It is used to compare the extracted biometric raw data to one or more previously stored biometric templates. The module therefore determines the degree of similarity (or of divergence) between two biometric vectors.
- Decision module: It is used to determine if the returned index of similarity is sufficient to determine the identity of an individual.

Capture module: It consists of capturing the biometric raw data in order to extract a numerical representation. This representation is then used for enrollment, verification or identification.

- Signal processing module: It allows the reduction of the extracted numerical representation in order to optimize the quantity of data to store during the enrollment phase, or to facilitate the processing time during the verification and identification phases this module can have a quality test to control the captured biometric data.

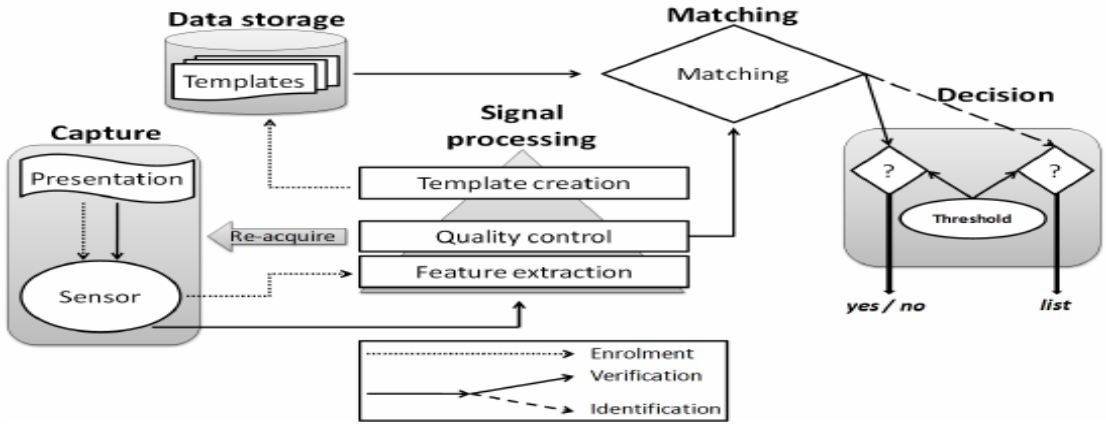

Figure 1.4: Generic architecture of a biometric system

1.4.2 Fusion level

Fusion levels in multibiometric, two or more biometric trait is used in biometric systems and also decision channels used more than one. Biometric fusion is used widely in the industry. In biometrics system, implementations of multibiometric can be done by using levels of fusion. To address number of issues in the biometrics, fusion is used. Some of the issues are robustness, applicability, accuracy, efficiency and universality. To increase robustness of the multibiometric, various levels of fusion are used for fusing the biometrics traits. Four types of fusions are available they are as follows: sensor level, feature level, matching score level and decision level. The block diagram of fusion levels in a multibiometric as shown in figure.[7]

- **Sensor level**

  Multi-Sensors In this category of sensor level fusion, multiple samples of a single biometric modality are obtained using multiple sensors and the information is combined such that the fused multi-sensor information improves the recognition performance

- **Feature level**

  for feature vectors. To select useful features, reduction combining feature vectors and later classifications are applied algorithms are used to form composite feature vector by biometric trait; separately feature vectors are extracted,Inextracted separately from each biometric trait.The fusion channels are first processed after which the feature vectors are feature level fusion, signals coming from different biometric techniques are used in feature level. Compared to matching Signals are processed first which are coming from different scoring.

  Method, feature level contains richer information of biometric traits in the feature level. And later from each biometrics and therefore good recognition results are obtained from feature level fusion and also when features of different.

- **Matching**
- **decision level**

As the name suggests, decision fusion aims at combining the decisions taken by different classifiers to achieve a common consensus that is better than the individual decisions of the classifiers, SousingDecisional Each biometric feature is pre-classified separately The biometric attribute is captured first and the features are extracted Either accept or reject based on the extracted features. By Combining the outputs of the different attributes and the final classification of Biometrics are done.

- **score level fusion**

Summethod, maxmethod, weighted sum method, adaptive method.

- **Decision level fusion**

Logical ‘and’, Logical‘or’, Bayesian fusion.

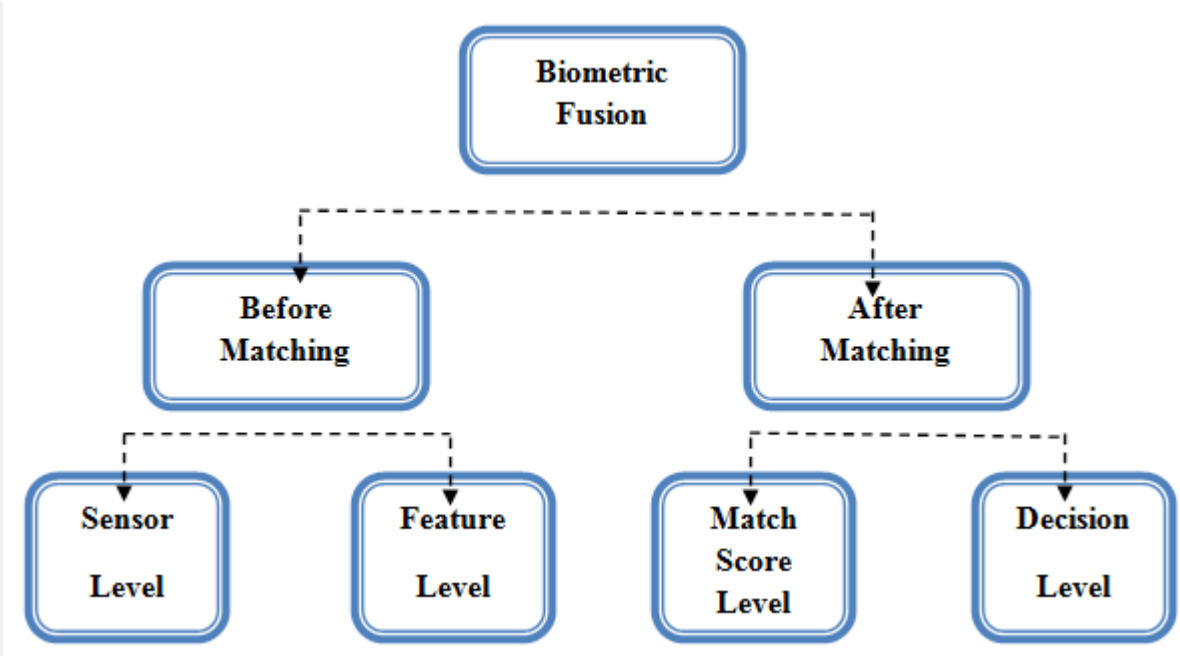

Figure 1.5:type of fusion level

1.5 Performance of a biometric system

The performance of a biometric system is determined by its ability to accurately identify individuals based on unique biological or behavioral characteristics. Key factors in evaluating performance include False Rejection Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER), recognition speed, scalability, robustness to environmental changes, and resistance to spoofing attacks. Evaluating these factors helps assess the system's reliability, security, and usability in various applications such as access control, identification, and authentication.[8]

Here we explain how to determine the performance, we need to clearly define three main criteria (FRR, FAR and EER) :

False Rejection Rate (FRR): This refers to the rate at which the system incorrectly rejects genuine users who should be granted access. In other words, it measures the probability that the system fails to recognize an authorized user.

False Acceptance Rate (FAR): This is the rate at which the system incorrectly accepts unauthorized users who should be denied access. It measures the probability that the system incorrectly identifies an impostor as a legitimate user.

Equal Error Rate (EER): This is a point on the ROC (Receiver Operating Characteristic) curve where the rates of false rejection and false acceptance are equal. Essentially, it represents the point at which the system's performance is optimal, balancing false rejection and false acceptance errors.

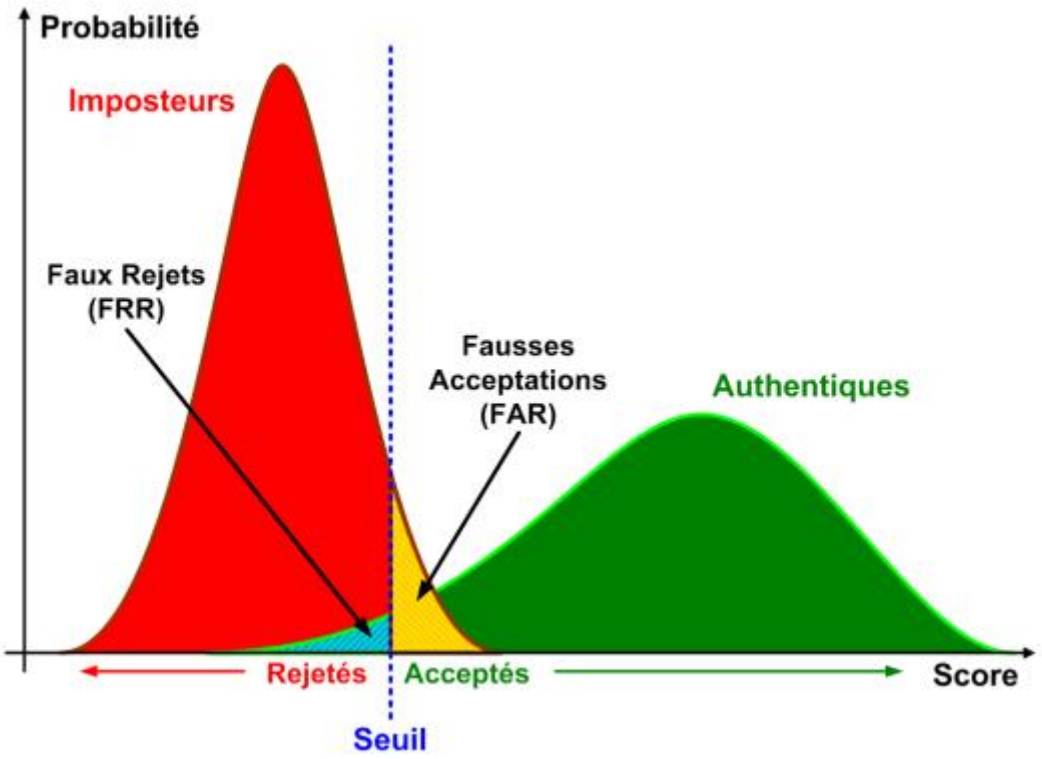

Figure 1.6: Illustration of FRR and FAR.

Right Rejection Rate (ROR): It measures the system's ability to correctly reject false identities, meaning it recognizes and rejects unauthorized individuals.

Right Acceptance Rate (RPA): It measures the system's ability to correctly recognize and accept authorized individuals.

Receiver Operating Characteristic (ROC): curve is a graphical plot that illustrates the performance of a binary classifier system as its discrimination threshold is varied. It plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various threshold settings. The area under the ROC curve (AUC-ROC) is often used as a metric to evaluate the overall performance of the classifier.

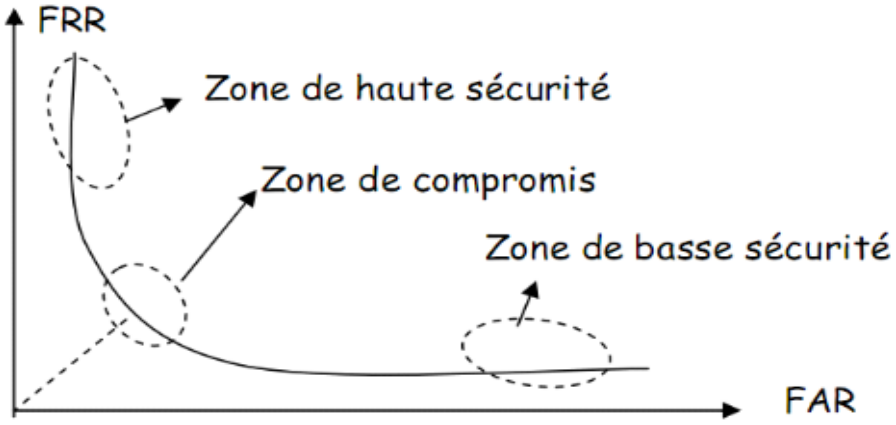

Figure 1.7: ROC Curve

Cumulative Match Characteristic (CMC):curve is a plot that shows the cumulative probability of correctly recognizing an individual in a ranked list of candidates. It is commonly used in biometric systems to evaluate the performance of matching algorithms. The CMC curve typically plots the rank (or position) on the x-axis and the recognition rate (or cumulative match rate) on the y-axis.

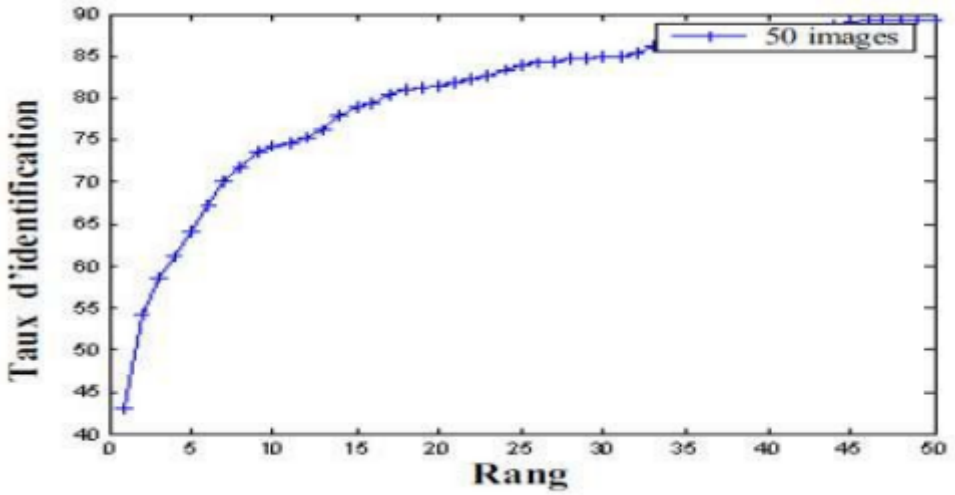

Figure 1.8: CMC Curve

1.6 Conclusion

In this chapter, we mainly give a general overview of the biometric system, so that we will review the most important points and concepts that were addressed by examining the concept of biometrics and the general structure of the biometric system and its forms, as well as the performance of its work and do not forget the security methods for preserving information,Security and comfort of users of this technology.

CHAPTER

2

Proposed biometric identification system using hand dorsal modality

2.1 Introduction

In light of recent developments in the field of technology and information security, biometric recognition technologies have become an essential tool for securing data and identifying individuals accurately and reliably.

In this chapter, a biometric identification system was proposed using the back of the hand, which is one of the promising biometric methods that use the structure of the hand and its unique feature to distinguish individuals (fingerprints, veins, skin grains, wrinkles, colors, lines, etc.).

This technology is used because it is considered an innovative and effective technology to verify the user's personal identity accurately and securely. This technology finds widespread use in many fields such as government buildings and companies, as well as its use in access control technologies and electronic payment systems.

2.2 Architecture of proposed biometric identification system using hand

The dorsal hand is a potential biometric method to achieve accurate recognition. The proposed system consists of several main components that work in harmony to achieve biometric recognition of the dorsal hand position.

These components include modules for feature extraction and biometric matching, as well as database management and then identification of the person (user interface control).

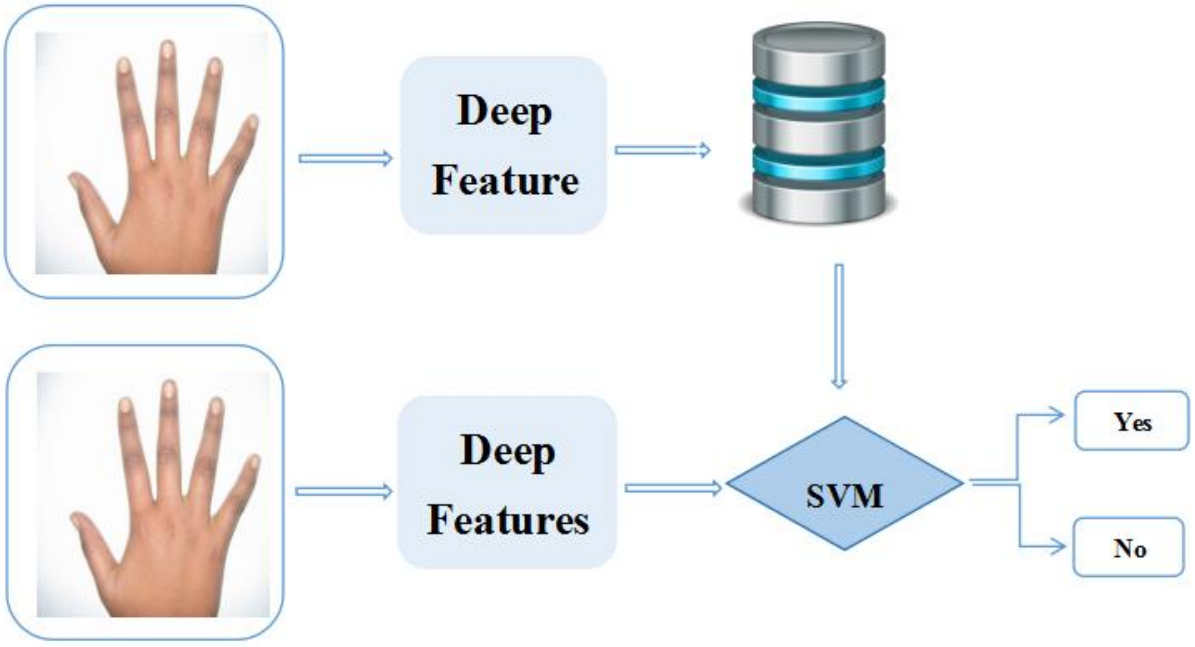

Figure 2.1: Architecture of proposed biometric using dorsal hand

2.2.1 Preprocessing

The main goal of the preprocessing unit is to extract the back of the hand. We use the concept of ROI so that the focus is on that area for the purpose of identifying the user by extracting the biometric features of the individual. This area usually includes visible vein patterns, wrinkles, and other unique features.

We obtained an image of the dorsal hand of a volunteer's right hand using an phone mobile phone camera without touching the hand. As an example, as shown in Image 2.1

Figure2.2 : Automated segmentation of region of instars

We identify in this **Figure2.2**the four main points of interest to determine the ROI bounding rectangle. We use techniques to define an ideal rectangle that fully shows the hand information, and then we crop it to reduce the image size to a certain size, for example [128 x 128]. Improving the quality of the ROI requires adjusting the lighting to ensure equal distribution. As well as improving contrast to improve the clarity of details in the area of interest, then correcting noise and adjusting color if this image suffers from color imbalance or some blemishes.

2.2.2 Features extraction

Feature extraction is a machinelearningandsignalprocessingtechniquethat reduces theamount ofprocessingresources by identifyingkeyfeatures of datawithoutlosingimportant information. Theprocess of featureextraction is represented by theability of thealgorithm to determinetheform in whichinformation is stored in the computer. When we input an image, it is analyzed in pixels andeachpixel is assigned a specificvalue, eventhough it is a largeamount of data. Data is requiredwith multiple features, many of whichmay be redundant. Thentherearedifferentmethods for extractingfeatures, such as: LDA and PCA, chosenbased on thedatatypeanddesired goals.

2.2.2. Machine learning

Machine learning is a branch of artificial intelligence, and it works to develop techniques that allow systems to learn from data and improve their performance over time, as it uses algorithms and mathematical models to analyze that data and extract patterns. This development takes place in four basic steps, which are: First / selection and preparation Training data set. This is done by knowing how to solve the problem for which it was designed. Secondly, choosing algorithms to run on the data set, depending on the size of the data and the type of problem. Thirdly, training the algorithms, which is a process of repetition? The variables are run through the algorithms and the results are compared with those. Whichis produced and followed by the fourth step, which is to use the model and improve it based on the problem that was solved. The model is used on new data.

2.2.2. Transfer learning

It is a strategy in machine learning, based on using knowledge gained from a specific task and applying it to another similar or simply related task. Transferring knowledge has several benefits, such as saving training time (accelerating the training process), improving performance, and not needing a lot of data because the model has been trained in advance, thus reducing the need for large data sets. When we first train a basic network on a dataset, we reuse the features we learned back to the second network for use in the dataset, and this is useful in the field of data science.

Transfer learning using CNN is done by choosing a pre-trained model that suits the task or data set, or includes common options such as ResNet or Vgg. The model is downloaded and customized, then the data is prepared, the model is trained, followed by evaluation and selection.

2.2.2.Deep learning

It is considered one of the branches of artificial intelligence, which relies on the use of artificial neural networks because it contains algorithms capable of simulating the structure of the human brain, as it consists of hundreds of layers, and each of them interprets information from the layer that precedes it, in order to understand and analyze data automatically.

Then there is CNN (Convolution Neural Network) It is a technology within the field of deep learning, or in other words we will say that CNN is a specific type of deep neural network, which in turn means a model designed specifically for image processing and computer vision. The CNN network consists of adversarial layers, starting with (Convolution layer), which learns patterns and local processing using an iterative recognition technique (Receptive

Field).Followed by a layer that reduces dimensions (Correction layer),andis called (Pooling) and latent layers (Hider Layer) that work to extract advanced features and a higher representation of the image. Thanks to these layers, deep neural networks can effectively recognize details within the image and classify it in a distinctive way.[10]

2.2.3 Features matching

Feature matching is a process that consists of comparing and matching features between two different sets of data in order to determine the extent of similarity and difference between them.SVMtechnology is used in machine learning to solve data classification problems, including linear and non-linear ones...

SVM is an algorithm that takes data as input and outputs the best line that separates these categories and classifies them accurately. You need SVM to classify the manual dorsal data set by reducing the problem of multi-class classification to multiple binary categories and processing them.[11]

2.3 Tied rank normalization

It is a technique that we usually use in some predictive models and statistics based on converting a set of values into points by returning to their original order. This technique is usually used in statistical models or predictive models.The main goal of the linked arrangement is to unify the distribution is to data and make it homogeneous with each other, and so is its purpose the reduce the variance and negative impact of the impulsive features within each graph.[12]

Linked ordering is used if there are some repeated values in the data, or in other words, when repeating values are discovered in a data set, linked ordering is applied to deal with the repeated values, and when there is a tie in the data, there will be a large change in the values and variance, resulting in Difficult to understand data accurately. In Abakhir, this method improves the accuracy and reliability of data analysis and interpretation.

2.4 Conclusion

In conclusion, the proposed biometrics system using the virtual hand showed many advantages, including the use of network models pre-trained using the features found on the virtual hand (Machine Learning, Transfer Learning, Deep Learning) and then matching them with the associated rank normalization technique to extract the features using SVM. Or to perform the classification task, this system has the potential to become the most important technology in the field of biometric authentication.

CHAPTER

3

Experimental Results and Discussion

3.1 Introduction

Our project aims to identify different people based on the experimental study and discussion related to the application of the dorsal hand fingerprint, based on image pre-processing, feature extraction (deep learning and CNN algorithm), and matching(SVM) to enhance the vision of the unique patterns and features of dorsal hand.

We collected images of the dorsal hand from a data set of 500 different people using non-contact hand imaging. Images were taken of the right hand of the volunteers, where we provided explanations of our method as described in chapter 2.

In this chapter, as we said previously and conclusions based on identifying people through the details of the dorsal hand, based on the best methods of assembly and classification.

3.2 Why hand dorsal modality

We chose the dorsal hand as one of the means of biological verification due to its multiple uses. The latter is characterized by many unique features and patterns, including two main features: which characterized the dorsal part of the hand (using ROI technique), and the veins, which are the most important part of the hand because they contain many identificationinformation, it also distributes vital vessels under the skin, wrinkles and folds that are difficult to imitate.

As for the security aspect, it is distinguished by its individuality, which means that each individual has his own fingerprint, different from others. It is easy to access the user's fingerprint and is not affected by it over time.

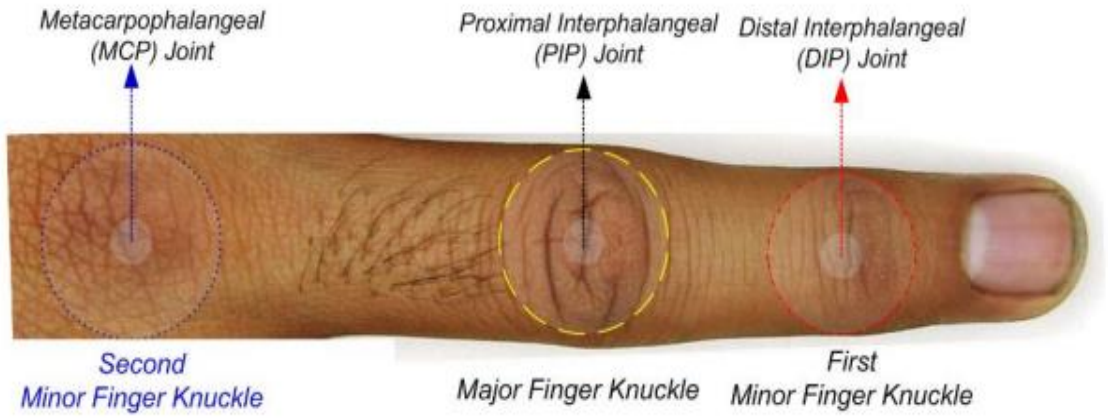

Figure 3.1: Sample finger dorsal to illustrate in finger knuckle and second minor finger knuckle patterns investigated.

3.3 Database description

The database is an advanced system capable of organizing.And storing classifying a large and diverse set of information based on the ITT campus and theuniversity Hong Kong Polytechnic campus during the period 2006-2015. In this study, we used a database containing dorsal handprints consisting of at least 500 (Male and Female) participants of different ages. Each participant in the group has 13 modality, they are divided into 5 images [3 of which are trait and 2 of which we used as a test].

Through the dorsal part of the hand, which we changed its size, 3 parts of the finger joint (or what is known as the interdigital joint), and a major finger knuckle which is the most important part of the hand and first minor finger knuckle as shown in the previous picture. All this data is saved and organized into folders to make it easy to link them to the original images folder for ease of use.

3.4 Database separation

After we collected the dataset of participants' dorsal handprints, we had to organize and separate the database with the goal of dividing it into groups separate from the other datasets, i.e. the subgroups include the dorsal fingerprints of different individuals and categories. This is done by collecting dorsal fingerprint data and then dividing it into subgroups, placing each branch in a specific group. After division, two groups are selected, one for training and the other for testing. These groups that we have identified must be diverse and balanced to achieve the best results.

The main purpose of data segregation is to allow only authorized individuals to review and access the database, as well as the ability to accurately and secureleperform identification models on individuals in various circumstances.

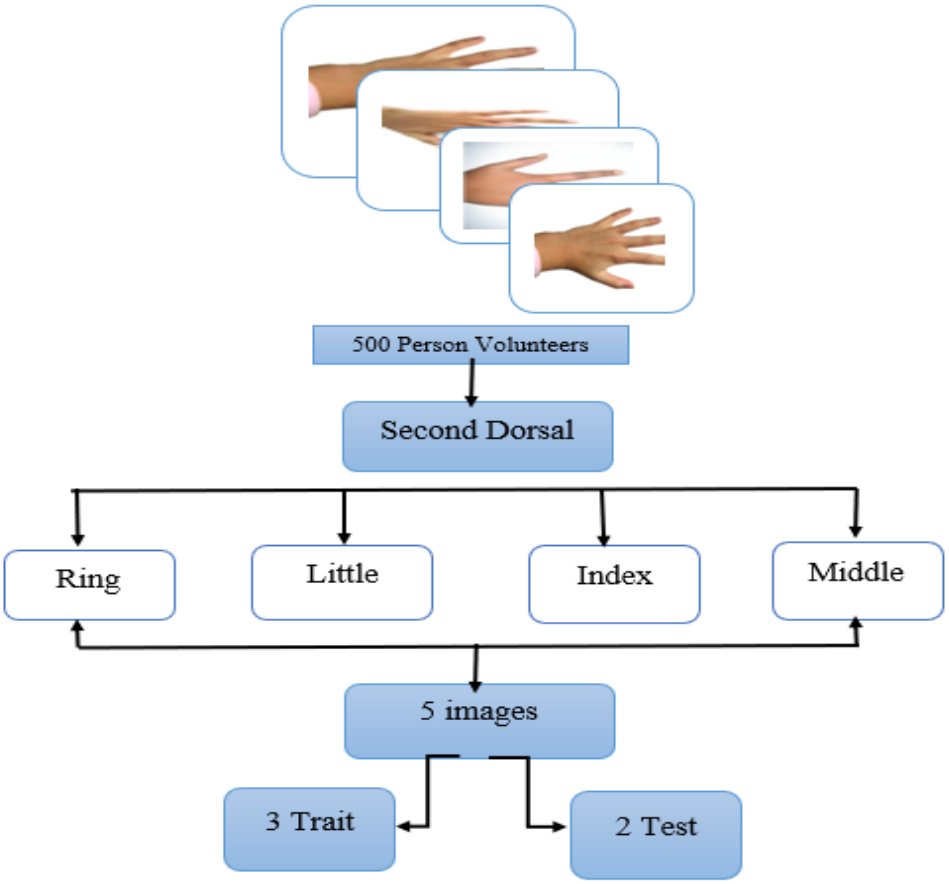

Figure 3.2: Database separation

3.5 Assessment protocol

We will evaluate the performance of the proposed method by taking 500 different people's hands. As we mentioned previously, we took the four categories (the center of the back, the first joint, the main joint, and the second joint). Since each of the four categories has 4 fingers (index, middle, ring, and pinky), we will evaluate the work of the verification system we proposed using only the main joint and track its value in this system.

In order to activate and implement this project, we present the hardware and software environments for this work.

3.5.1 Hardware environment

We will provide a set of equipment from **HP ProDesk 600 G3 SFF** workstation computer equipped with the following characteristics:

- **Processor:**Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz 3.41GHz
- **System Type:**64-bit operating system, x64-based processor

3.5.2 Software environment

MATLAB. They added several useful features that made experimenting easier.

As a result, we decided to use MATLAB for our experiment. In summary, the environment we used for our experiment is:

- The software tool used by our system is MATLAB R2023b.
- The operatingsystem used to run our software is windows 10.

3.6 Experimental results and discussion

In this section we will explain the unimodal and multimodal systems at stake. To train and test transfer learning architectures using our data. Using the AlexNet, Vgg16, Vgg19 models. Here will compare their effectiveness in dealing with the biometric identification task:

- Equal Error Rate (EER)
- T0 (threshold)
- Recognition Rate (ROR)
- RankPerfect Recognition (RPR).

a. Unimodal test result

For Alexnet

Trait	Open set		Closed Set	
	EER	T0	ROR	RPR
Index	2.6070	0.7330	87.9000	424
Middle	1.5992	0.7100	92.8000	311
Ring	2.1972	0.7320	89.7000	265
Little	1.7703	0.7190	90.7000	448

Table 3.1: Unimodal test result for alexent

For Vgg16

Trait	Open set		Closed Set	
	EER	T0	ROR	RPR
Index	3.4076	0.6920	81.8000	366
Middle	2.5770	0.7050	85.2000	257
Ring	2.5065	0.6940	83.6000	303
Little	2.1974	0.6860	86.2000	319

Table 3.2: Unimodal test result for Vgg16

For Vgg19

Trait	Open set		Closed Set	
	EER	T0	ROR	RPR
Index	2.8885	0.7240	81.8000	314
Middle	3.0078	0.6940	85.4000	343
Ring	2.7344	0.6780	84.2000	248
Little	2.7055	0.6710	86.7000	222

Table 3.3: Unimodal test result for Vgg19

Discussion

After analyzing **Table 3.1**forAlexnet, we notice that the "**middle**" finger achieves between results for this system compared to the other fingers for the system **EER=1.5992** and **ROR=92.8%,** After we analyze **Table 3.2** and **Table 3.3** for (**Vgg16** and **Vgg19),** we notice that the "**little**" finger achieved the best performance for both cases at the values for Vgg16 (**EER=2.1974** and **ROR=86.2000**), and for Vgg19 (**ERR=2.7055** and **ROR=86.7000**).After comparing which fingers perform best for recognition, in this **Figure 3.3**shows the results of the unimode test for the open set, and Figure 3.4 shows the proposed system based on determining the closed set. Offers for all fingers, wiche shows that **Alexnet** is the best model.

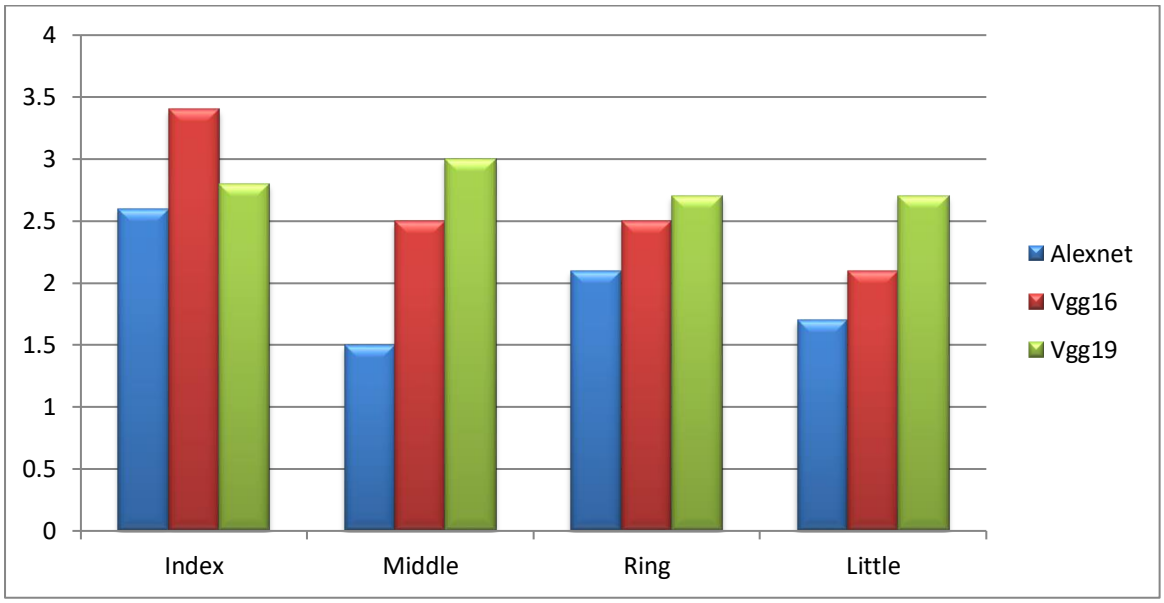

Figure 3.3: Unimodal test results for open set identification mode

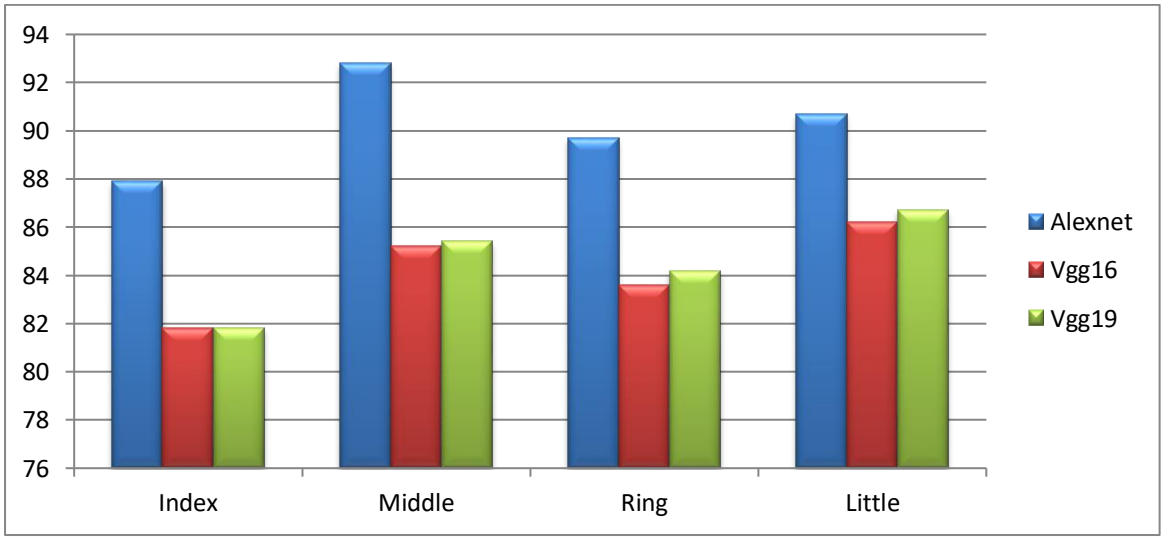

Figure 3.4: Unimodal test results for closed set identification mode

b. Multimodal test result

The results we presented indicate the performance of a multimodal system using fusion methods ″**Min**,″ ″**Max**″ and ″**Sum**″ and ″**Wsum**″. The system will evaluate the attributes at the ″second″ level in terms of **EER**, **T0**, **ROR**and**RPR.**

1) Multi-Traits

For Alexnet

- **Open set identification mode**

Trait	SUM		Min		Max		W SUM	
	EER	T0	EER	T0	EER	T0	EER	T0
SecondAll	0.7003	0.7230	1.4985	0.7570	1.3013	0.7010	0.6973	0.7220

Table 3.4: Open set based multimodal test result(for alexent)

- **Closed set**

Trait	SUM		Min		Max		W SUM	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
Second All	96.5000	381	93.7000	377	93.8000	230	96.5000	377

Table 3.5: Closedset based multimodale test result (for alexenet)

For Vgg16

- **Open set**

Trait	SUM		Min		Max		W SUM	
	EER	T0	EER	T0	EER	T0	EER	T0
Second All	1.0010	0.6660	2.2088	0.7150	1.6957	0.6950	1.0999	0.6570

Table 3.6: Open set based multimodal test result (for Vgg16)

- **Closed set**

Trait	SUM		Min		Max		W SUM	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
Second All	96.3000	209	91.8000	306	90.9000	374	96.2000	195

Table 3.7: Closed set based multimodal test result (for Vgg16)

For Vgg19

- **Open set**

Trait	SUM		Min		Max		W SUM	
	EER	T0	EER	T0	EER	T0	EER	T0
Second All	1.1258	0.6620	2.0044	0.7310	1.7982	0.6790	1.1025	0.6630

Table 3.8: Open set based multimodal test result (for Vgg19)

- **Closed set**

Trait	SUM		Min		Max		W SUM	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
Second All	96.2000	220	90.8000	293	91.0000	364	96.1000	216

Table 3.9: Closed set based multimodal test result (for Vgg19)

Discussion

Based on the provided tables,and after analyzing**Table 3.4**for alexnet, it gave the value of the SUM **(EER=0.7003** and **ROR=96.5%).**

The tables **Table 3.5** and**Table 3.6** for vgg16, gave the value of the SUM**(EER=1.010**and **ROR=96.3)**.

At vgg19, it gave the total value **(EER = 1.1258** and **ROR = 96.2)**. Here we notice that **alexnet** gave the best rating compared to the percentage values of **vgg19** and **vgg16**, when EER is closest to **0** and when **ROR** is closest to **100%.**

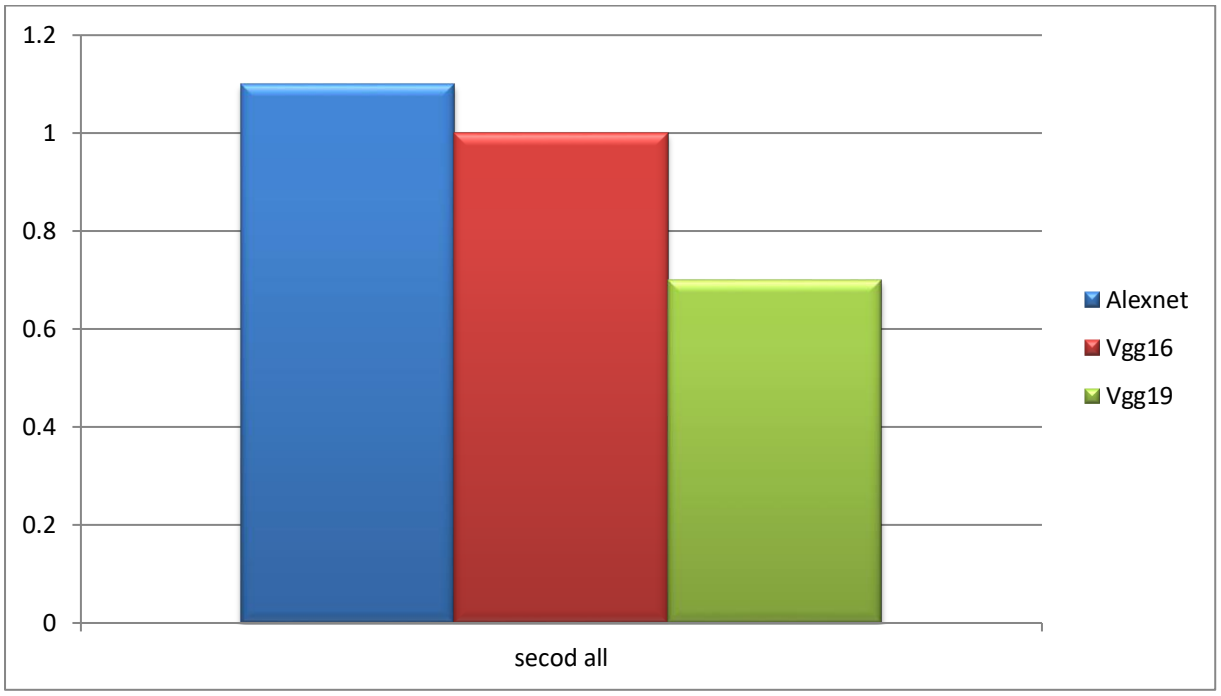

Figure 3.5: multi-trait test results for open set identifies mode

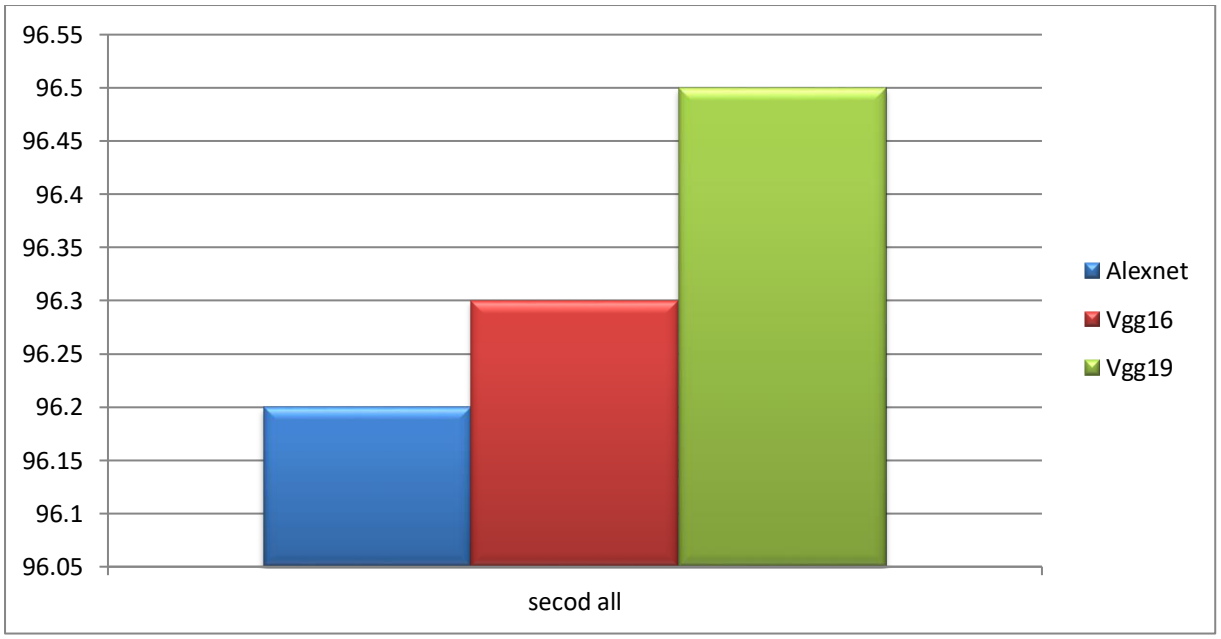

Figure 3.6: multi-trait test results for closed set identifies mode

2) Multi-algorithm

- **Open set**

Trait	SUM		Min		Max		W SUM	
	EER	T0	EER	T0	EER	T0	EER	T0
Index	2.1077	0.6930	2.7571	0.7470	2.5023	0.6950	1.9980	0.6980
Middle	1.5918	0.6750	2.2977	0.7180	1.8927	0.6790	1.5045	0.6760
Ring	1.8016	0.6750	2.5021	0.7340	1.9786	0.6800	1.7352	0.6770
Little	1.3005	0.6710	1.1917	0.7160	1.6042	0.6730	1.2991	0.6730

Table 3.10: Open set based multi-algorithm test result

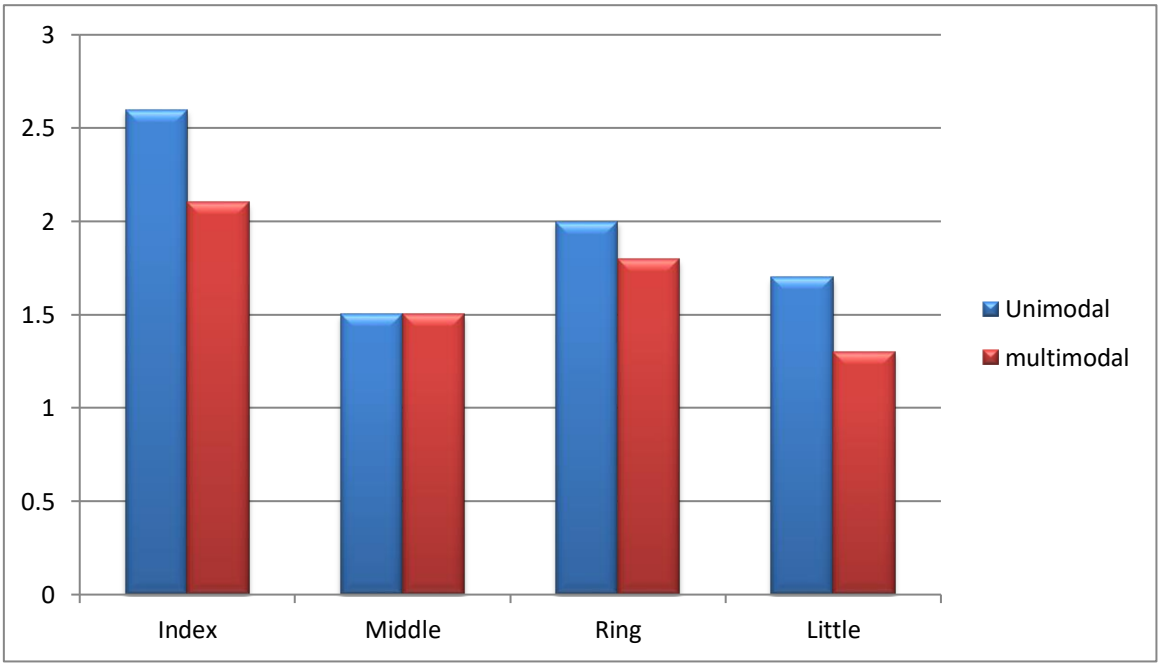

Figure 3.7: Multimodal VS unimodal test results: a comparison open set performance

- **Closed set**

Trait	SUM		Min		Max		W SUM	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR

Index	91.8000	322	2.7571	340	87.7000	361	91.7000	329
Middle	92.6000	328	89.9000	342	89.8000	299	93.1000	350
Ring	93.5000	184	88.0000	237	90.000	259	93.5000	182
Little	93.9000	372	91.1000	299	91.3000	352	93.9000	267

Table 3.11: Closed set based multi-algorithm test result

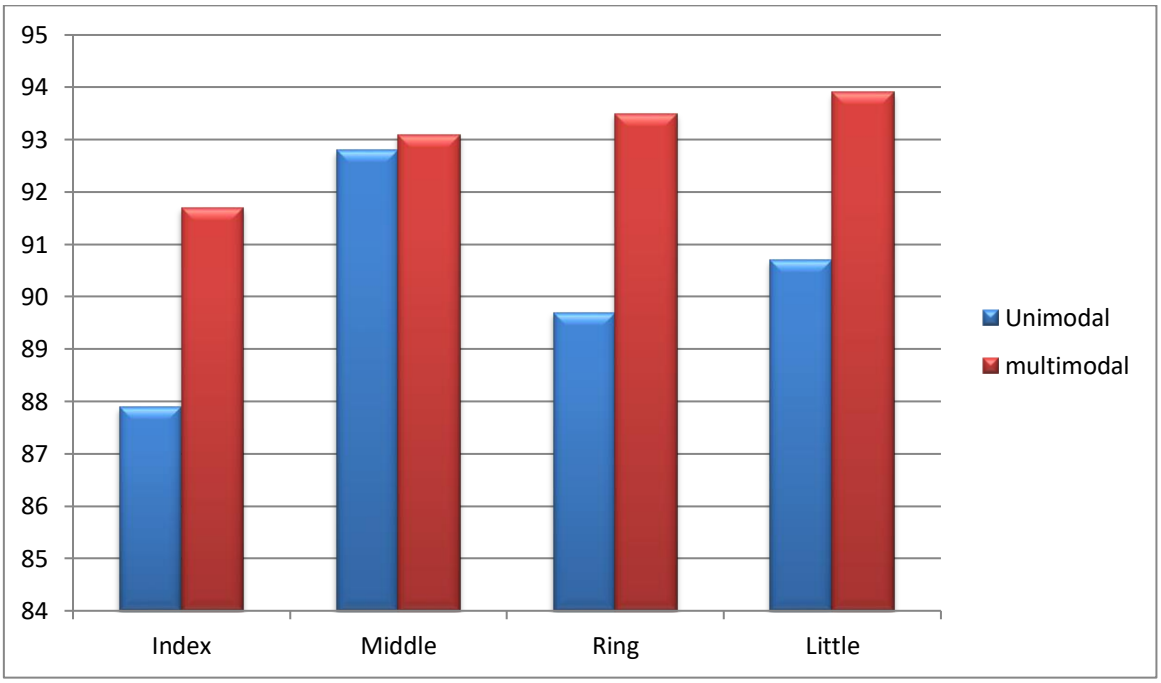

Figure 3.8: Multimodal VS unimodal test results: a comparison closed set performance

Discussion

To achieve better performance than the possibility of improving this system by using integration or merging of information from some images of the dorsal hand, we tested the best group capable of improving the accuracy of the system.

In the case of the open group**Table 3.10**, we notice that the performance and efficiency of the system has improved significantly. as this group works on Reducing the **EER** ratio **(EER=1.3005)** when the existing fusion rule is used compared to the best performance in the case of a single-media system **EER=1.5992**.

In the case of the group being closed at **SUMTable 3.11**, we notice that the system performance has improved better by **93%.**

A performance comparison is drawn between the unimodal and multimodal presentations for agents in the open and closed modes, where we notice an improvement in the performance of the multimodal compared to the unimodal. This is evidence that the multimodal has enhanced the algorithms and methods to perform much better recognition.

3.7 Conclusion

In this chapter we examined biometric features of the back of the hand using a database from theUniversity of Hong Kong containing 500 volunteers. In our study, we focused on the secondfinger joint, which in turn contains 4 dorsal image classes(Middle,Index,Ring,Litlle).

We conclude from the study that we conducted that Alexnet gave the best performance rating, asthe Equal error rate EER=0.7003% and the recognition rate is ROR=96.5% compared to vgg16and vgg19.

General Conclusion

With the recent development that the world is witnessing, researchers have become interested inidentifying people's identity based on biometrics through their physical and behavioralcharacteristics.

In our research, we relied on the dorsal hand, as it is considered one of the most accurate methodsfor identifying a person.The results obtained in this research were conducted using the dorsal hand database from HongKong Polytechnic University for 500 people using non-contact manual photography, whichconsists of 4 categories of dorsal images.

Our goal in this research is to provide a methodology to improve the performance of biometricdorsal hand identification using alexnet and vgg 16 and vgg 19 as feature generators. These features are then sent to train a classifier in order to build a model capable of distinguishingbetween people.

Finally, we note that the experimental results of combining lead to better results with individualncharacteristics, and we expect this work to be a useful starting point for new and combined approaches ground for a wide range of benefits in other biometrics and dorsal hand identification.

Bibliographie

[1] Bhatia, Renu."Biometrics and face recognition techniques." International Journal of Advanced

Research in Computer Science and Software Engineering 3.5 (2013).

[2] Juliana munoz, Biometric authentication vs traditionel methodes: pros and cons, 6 april 2023.

[3] Giesing,Ilse(Compiler).(2003).Biometrics.-University of Pretoria.-pp.49-76 And (Raab and Mason).(2003).p.83

[4] Millett, L. I., & Pato, J. N. (Eds.). (2010). Biometric recognition: Challenges and opportunities.National Research Council (US) WhitherBiometricsCommittee.

[5] Ajay Kumar, Zhihuan Xu Kwong, "Personal identification using minor knuckle patterns from palm dorsal surface," IEEE Trans. Info. Forensics & Security, vol. 11, no. 10, pp.2338-2348, October 2016

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

[7] BOUHAFS, Khaoula and TARFAIA, Mouna. *Toward Effective Person Recognition Using Hand Dorsal modality Sustained*. Master thesis. university of ouargla,2022.

[8] Ghayoumi, Mehdi. "A review of multimodal biometric systems: Fusion methods and their applications." 2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS). IEEE, 2015

[9] R. P.WILDES, "A system for automated iris recognition ". Proc. of 2ndIEEE Work-shop on Applications of Computer Vision, pp. 121-128, Décembre 1994.

[10] M. BAHAZ and M. HAMZA."Palmprint And Palmvein Recognition Based On Deep

Lerning ". Mémoire de master .Université Ouargla 2018.

[11] S. J. PAN and Q. YANG."A survey on transfer learning. IEEE Transactions on

Knowledge and Data Engineering". 22(10), 1345–1359. 2010.

[12] Annapoorna Shetty, Shravya Shetty K, Krithika K"A Review on Asymmetric Cryptography–RSA and El Gamal Algorithm," International Journal of Innovative Research in Computer and Communication Engineering, ISSN, pp.2320-9801, 2014.

[13] Mohammed Adnane BAHAZ & Mahdi Abdurrahman HAMZA, "Palmprint and Palm veinRecognition Based on Deep Lerning", master memory, KASDI MERBEH UNIVERSITY 2018/2019.

[14] Jisha Nair.RanjithaKumari."A Review on Biometric Cryptosystems. RVS College of Arts & Science", Sulur, Tamil Nadu, India. International Journal of Latest Trends in Engineering and technology (IJLTET)].

[15] M.KORICHI. "Biometrics and Information Security for a Secure Person Identification".

Thesis Doctoral, KASDI MERBEH UNIVERSITY, OURGLA, 2019.

الملخص

في ظل التطور التكنولوجي السريع أصبح النظام البيومتري مكانا بارزا للعديد من التطبيقات الحيوية نظرا للحاجة المتزايدة لوسائل فعالة وآمنة للتحقق من هوية المستخدمين.

في هذه الأطروحة، تم اقتراح نظام للتعرف على اليد الظهرية يعتمد على تحديد القياسات الحيوية القادرة على التمييز بين الأفراداعتمادا على حرم جامعة **هونغ كونغ**. ولذلك استخدمنا برنامج التعلم العميق المعتمد على خوارزمية (**CNN**) لدقة التصنيف، ثم تقنية المطابقة باستخدام (**SVM**). يقوم بجمع وتحليل البيانات بناء على قاعدة البيانات المعروفة في هذا المجال لاختبار مدى فعالية النظام.

تهدف هذه الدراسة إلى تعزيز أمان وثقة نظام التعرف البيومتري من خلال تقنيات متطورة وحديثة.

الكلماتالمفتاحية: المقاييسالحيويه , اليدالظهريه،نظامالتعرفالبيومتري،التعليمالعميق،SVM,CNN, تجميع.

ABSTRACT

In light of the rapid technological development, the biometric system has become a prominent place for many vital applications due to the increasing need for effective and secure means of verifying the identity of users.

In this thesis, a dorsal hand recognition system was proposed that is based on identifying biometrics capable of distinguishing between individuals depending on the university of **Hong Kong** campus. Therefore, we used a deep learning program based on the (**CNN**) algorithm for classification accuracy, then the matching technique using (**SVM**). Collects and analyzes data based on the well-known database in this field to test the effectiveness of the system.

This study aims to enhance the security and confidence of the biometric identification system through advanced and modern technologies.

Keywords: Biometrics, dorsal hand, biometric recognition system, deep learning, CNN, SVM , clustering.

Résumé

À la lumière du développement technologique rapide, le système biométrique est devenu une place importante pour de nombreuses applications vitales en raison du besoin croissant de moyens efficaces et sécurisés pour vérifier l'identité des utilisateurs.

Dans cette thèse, un système de reconnaissance de la main dorsale a été proposé, basé sur l'identification biométrique capable de distinguer les individus selon la campus de l'universite de **Hong Kong**. Par conséquent, nous avons utilisé un programme d'apprentissage profond basé sur l'algorithme (**CNN**) pour la précision de la classification, puis la technique d'appariement utilisant (**SVM**). Recueille et analyse des données basées sur la base de données bien connue dans ce domaine pour tester l'efficacité du système.

Cette étude vise à améliorer la sécurité et la confiance du système d'identification biométrique grâce à des technologies avancées et modernes.

Mots clés : Biométrie, main dorsale, système de reconnaissance biométrique, deeplearning, CNN, SVM, clustering.