N^o d'ordre :.../.....

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF KASDI MERBAH OUARGLA

FACULTY OF NEW INFORMATION AND COMMUNICATION TECHNOLOGIES

THESIS

Thesis submitted in partial fulfillment of the requirements for the degree of

2nd Cycle LMD Master

In : Telecommunications Systems

By : **FEHDI OUSSAMA and BENABDALLAH MOHAMED.**

Thesis

Biometric Images Processing and Recognition

Publicly sustained on : 23/06/2024 before the jury composed of:

Name and Surname	*Title*	*Affiliation*	*Quality*
K. BENSID	*MCB*	*Univ. K. M. Ouargla*	*President*
R. CHELAOUA	*MCB*	*Univ. K. M. Ouargla*	*Thesis Director*
A. CHERGUI	*MCB*	*Univ. K. M. Ouargla*	*Examiner*


بسم الله الرحمن الرحيم


وقل رب زدني علما


صدق الله العظيم

Dedication

I DEDICATE THIS PROJECT TO ALLAH, MY SOURCE OF INSPIRATION, WISDOM, KNOWLEDGE AND UNDERSTANDING, THE SOURCE OF MY STRENGTH THROUGHOUT THIS PROGRAM.

TO MY PARENTS WHO HAVE PROVIDED ME WITH THEIR ENCOURAGEMENT, LOVE AND UNDERSTANDING.

TO BELOVED PEOPLE WHO HAVE MEANT AND CONTINUE TO MEAN SO MUCH TO ME. ALTHOUGH THEY ARE NO LONGER OF THIS WORLD, THEIR MEMORIES CONTINUE TO REGULATE MY LIFE.

TO MY DEARLY LOVED ONE, DJELAILIA.

TO ALL MY FRIENDS AND TEACHERS IN EVERY INSTITUTION I DID STUDY AT.

TO ALL WHO WERE THERE FOR ME, THANK YOU FOR YOUR HELP AND ENCOURAGEMENT.

BENABDALLAH MOHAMED

Dedication

TO MY DEAR PARENTS, FOR ALL THEIR SACRIFICES, THEIR LOVE, THEIR TENDERNESS, THEIR SUPPORT AND THEIR PRAYERS THROUGHOUT MY STUDIES, TO MY DEAR SISTERS SARA AND AMINA FOR THEIR PERMANENT ENCOURAGEMENT AND MORAL SUPPORT, TO MY DEAR BROTHERS ILYES AND ADNAN, FOR THEIR SUPPORT AND ENCOURAGEMENT,
TO ALL MY FAMILY AND FRIENDS(RACHID,RABEH,ABDELDJALIL,YOUSEF,IKHLAS) FOR THEIR SUPPORT THROUGHOUT MY UNIVERSITY CAREER,
MAY THIS WORK BE THE FULFILLMENT OF YOUR SO-CALLED WISHES, AND ESCAPE FROM YOUR UNFAILING SUPPORT.

FEHDI OUSSAMA

First and foremost, we are extremely grateful to our supervisor, Dr. ***Rachid CHELAOUA*** *for his invaluable advice, continuous support, and patience during us study. His immense knowledge and plentiful experience have encouraged us in all the time of our academic research and daily life.*

We also extend our sincere thanks to the members of the jury: Dr. ***BENSID Khaled*** *and Dr.* ***CHERGUI ABDELHAKIM*** *for their acceptance to evaluate this work.*

Finally, we would like to express our gratitude to all teachers in the electronics department of University Kasdi Merbah Ouargla for their help and advice, without forgetting all colleagues and friends.

Résumé

La reconnaissance de l'empreinte palmaire est une méthode biométrique physiologique utilisée pour reconnaître une personne. Elle se compose de diverses caractéristiques telles que la texture, les statistiques et la géométrie. Ces caractéristiques sont utilisées séparément ou par la combinaison de deux ou plusieurs caractéristiques pour une reconnaissance rapide et correcte. Cette technologie est utile dans divers domaines tels que la sécurité, le contrôle d'accès aux bâtiments, les applications de paiement sécurisé.

Dans cette thèse, nous présentons le système biométrique proposé, où l'apprentissage profond AlexNet est appliqué au système biométrique de reconnaissance d'empreintes palmaires. Ainsi, nous nous basons sur 2D-DWT comme méthode de fusion d'images et expliquons leurs structures. Pour une évaluation plus complète, nous avons modifié les paramètres et les variables de notre réseau neuronal afin de sélectionner la meilleure combinaison. Sur la base des résultats, nous avons obtenu d'excellents taux de précision, qui donnent un aperçu de la performance du système de reconnaissance proposé.

Mots clés: Palmprint, AlexNet, 2D-DWT, feature fusion.

Abstract

Palm print recognition is physiological biometric method used for recognition of person. It consists of various features like texture, statistical, geometry features. Which are used separately or by the combination of two or more features for quick and correct recognition purpose. This technology is beneficial in various fields such as security, access control to buildings, secure payment applications.

In this thesis, presents the proposed biometric system, where the deep learning AlexNet is applied on palm-print recognition biometric system. Thus, we based on 2D-DWT as image fusion method and explain their structures. For more comprehensive evaluation, we changed parameters and variable of our neural network to selected best combination. Based on the results, excellent accuracy rates war achieved, that provide an overview of the performance of the proposed recognition system.

Keywords: Palmprint, AlexNet, 2D-DWT, feature fusion.

Contents

List of Figures

List of Tables

Abbreviations

CNN	:	Convolutional Neural Networks	DWT	:	Discrete Wavelet Transform
FA	:	False Acceptation	FAR	:	False Acceptance Rate
FR	:	False Rejection	FRR	:	False Rejection Rate
EER	:	Equal Error Rate	EM	:	Expectation-Maximization
GAR	:	Genuine Acceptance Rate	CPU	:	Central Processing Units
PIN	:	Personal Identification Number	PLM	:	Palmprint
NIR	:	Near Infra-Red	NIST	:	National Institute of Standards Technology
PCA	:	Principal Component Analysis	PCANET	:	Principal Component Analysis Networks
PIN	:	Personal Identification Number	PLM	:	Palmprint
RBF	:	Radial Basis Function	RBM	:	Restricted Boltzmann Machine
RFT	:	Random Forest Transform	ROC	:	Receiver Operating Curve
ROI	:	Region Of Interest	ROR	:	Rank One Recognition
RPR	:	Rank of Perfect Recognition	SVM	:	Support Vector Machine
TA	:	True Acceptance	TR	:	True Rejection

Chapter 1

INTRODUCTION

HUMAN identification leads to trust that is essential for the proper functioning of society. It has been identifying humans based on their face, appearance, or gait for thousands of years [1]. In the era of technology, biometric authentication is a process for identifying and giving the permission in the specific system for the real user or object. In this process, mainly we use three types methodology. One of this based on the knowledge that is password or PIN, it is widely used last few decades. The second methodology is based on the possession such as a smart card, badge, document and key. Biometric proofing approach is another one, which gains more attention nowadays [2].

Biometrics security offers a natural and reliable solution to certain aspects of identity management by utilizing automated schemes to recognize individuals based on their inherent anatomical and/or behavioral characteristics. By using biometrics it is possible to establish an identity based on "Who you are?", rather than by "What you know or possess?" [3]. Biometrics characteristics are often classed in two main categories [4]:

- **Physiological biometrics:** Features notably identified through the five senses and processed by finite calculable differences. Including things like hair and eye color, teeth, facial features, DNA, fingerprints or hand-prints, etc.
- **Behavioral biometrics:** Based on the manner in which people conduct themselves, such as writing style, walking rhythm, typing speed, and so forth.

For these characteristics to be used for sustained identification encryption purposes, they must be reliable, unique, collectable, convenient, long term, universal, and acceptable. A primary motivation for using biometrics is to easily and repeatedly recognize an individual. The supremacy of a biometric is that it doesn't change. It's very exhausting to forge or fake. In some cases, it is next to impossible. Biometric provides a very strong access control

security solution satisfying authentication, confidentiality, integrity, and non-repudiation [5].

Biometric is being increasingly used today to carry out person recognition in a large number of civilian applications (national ID card, e-passport and smart cards). Depending on the use case and criticality, some systems use biometrics as one of the ways of authentication, and other systems use it as mandatory.

The rest of the thesis is organized as follows. In the Chapter 2, the focus was on biometric systems by discussing the units of biometric systems. Covering biometric system settings and multimedia biometric systems, while also reviewing biometric fusion before matching and after matching. In addition, this chapter provides a look at the evaluation and performance curves and the different error rates that exist.

In the Chapter 3, the proposed methodology for a biometric system based on 2D palmprint technology is explained. With a rationale for using deep learning methods and architectures, which can be used on smart biometric applications. In addition to clarifying all the different operations of the proposed system in more detail.

In the Chapter 4, experiments on the efficiency of the proposed biometric system were carried out. To show the biometric system evaluation. In addition to presenting the results obtained from systems and comparing them. Through the obtained experimental results and research, interpretations and evaluations of our proposed biometric systems are provided.

In the Chapter 5, the thesis is summarized with a comprehensive conclusion including its contribution and concluding remarks are provided. Potential future directions for this research are also discussed.

Chapter 2

BIOMETRICS SYSTEMS OVERVIEW

2.1 Introduction

BIOMETRIC is a dual combination of technological and scientific authentication methods majorly based on human biology and extensively used in information assurance [6]. Biometric is a measurement and statistical test for the representation of unique intellectual and behavioral individuals. This technique is mainly used for identification and access control or to identify persons who are being monitored. The fundamental principle of biometric verification is that every person can be determined correctly via his-her inner physical or behavioral characteristics. The term 'biometrics' is derived from the Greek word 'metric' which means to measure and 'Bio' means life.

Hence, Through biometrics authentication of identification can be made secure by accessing human biological or behavioral information [7] such as retina , DNA, plam-print, voice, gait, etc [8]. which are the common biometrics. Biometrics is unique and as every human acquires these characteristics uniquely, so these are the most reliable methods to authenticate any identification securely. Fig. 2.1 depicts various types of biometrics.

2.2 Biometric Systems

Biometric system can be dened as the automatic recognition of a persons using distinguishing features. It is basically a pattern recognition system that can recognize a person by extracting a biometric features from the acquired data of users, and comparing this feature set against the templates feature set, witch are previously stored in the database. Then, the individual can be identied based on result of match [3].

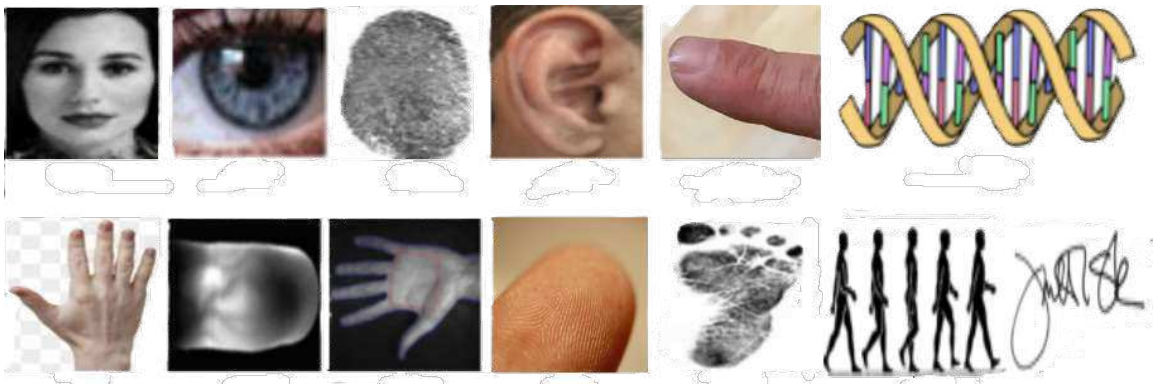

FIGURE 2.1: Various types of biometrics.

2.3 Biometric Systems Modules

Every biometric system consist of five basic modules. Modules are mainly used for converting the acquired image into some useful information and stored as a template [9]. The block diagram of biometric system is shown in Fig. 2.2.

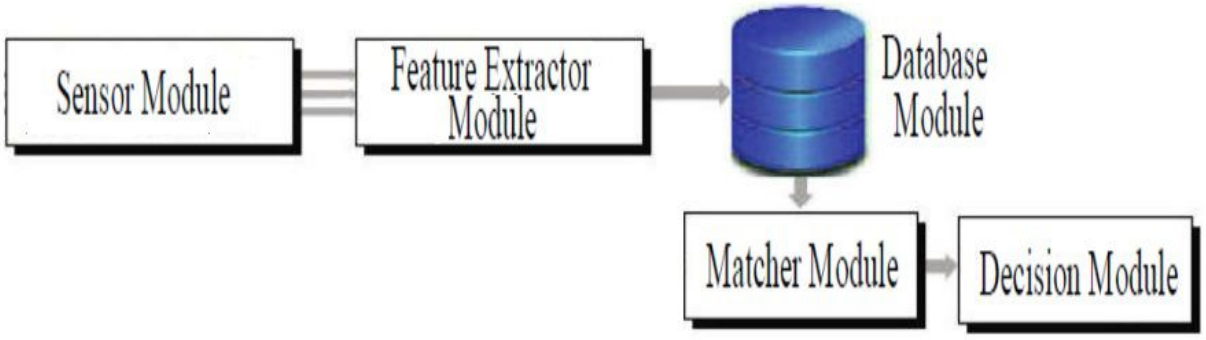

FIGURE 2.2: Biometric System Modules.

The description of modules are as follows [10]:

Sensor Module: sensor module in biometric system is used for capturing biometric data(palmprint, face etc.) and after scanning convert it into digital form.

Feature extractor module: the feature extractor module in a biometric system operate on data sent by the sensor module. As its name indicates, module extract feature set and store it in a compact representation called template database.

Database module: is important component for system, where the templates are being stored then retrieved to authentication process [11].

Matcher module: this module compare feature set received from feature extractor module with templates stored in database. Matching result are generated when all comparisons are done. This result is used for identification and verification of an user.

Decision module: this module accept or reject the user after comparing matching score with predefined security threshold value, if matching score is higher than predefined security threshold value, it will accept the user otherwise reject it.

2.4 Biometric System Modes

Depending on the application context, a biometric system may operate either in identification mode or verification mode. Before the system can be put into these modes, a system database must be created through to process of enrolment.

Enrolment is the process where the users initial biometric samples are collected, assessed, processed, and stored for use in a biometric system as shown in Fig. 2.3 If users are experiencing problems with a biometric system then they have to re-enroll to gather higher quality data.

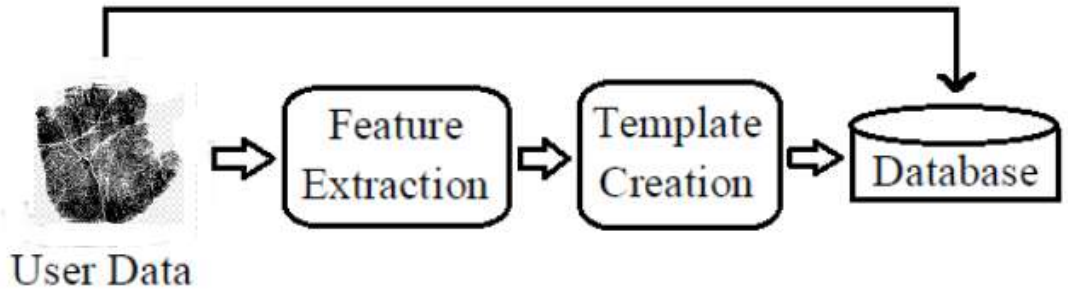

FIGURE 2.3: Enrolment Process in Biometric System.

Biometric systems use two modes. These are identification and verification (authentication) modes:

2.4.1 Verification mode

It refers to 1:1 matching, Verification is also known as authentication, the user claims an identity and system verifies whether the claim is genuine or not. Sample given by individual is matched with only one template i.e. stored template of that person only. As only one

matching is performed so verification process is very fast and accurate [12]. The procedure of verification mode is given in Fig. 2.4.

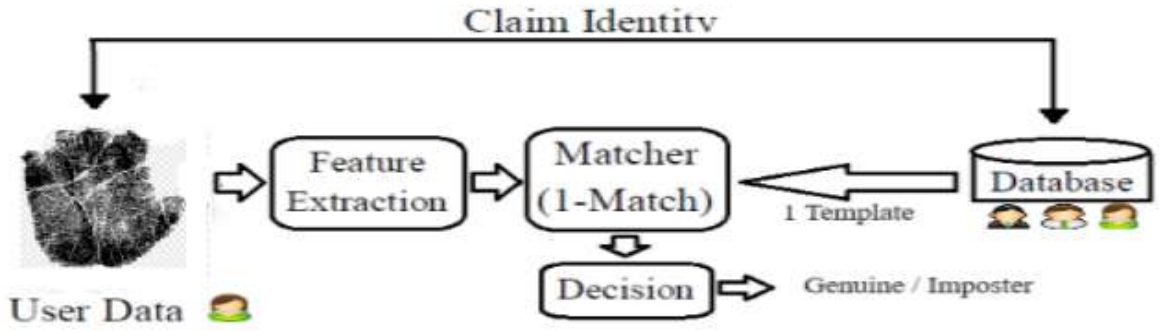

FIGURE 2.4: Verification Process in Biometric System.

2.4.2 Idenfication mode

It refers to 1: N matching where "N is total number stored templates in database". In this situation user does not know his identity, he is simply presenting his biometrics for matching with whole database. Users data is matched with all the templates to identify with which template it has highest similarity [12]. Fig. 2.5 illustrates the identification concept.

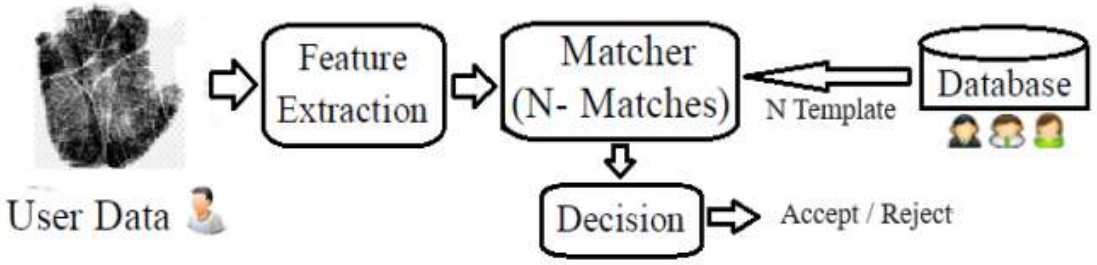

FIGURE 2.5: Identification Process in Biometric System.

2.5 Multimodal Biometric Systems

Authentication systems setup with one biometric modality may not be sufficient for the pertinent application in terms of properties such as universality, acceptability etc [13]. Application that is known as biometric system can be classified into two different types:

Unimodal Biometric System: the unimodal biometric system employs single biometric trait (either physical or behavior trait) to identify the user.

Multimodal Biometric System: a biometric system that consolidates the information from multiple sources is known as multimodal biometric system.

Multimodal biometrics is a system that combines the results obtained from several biometric characteristics for personal identification purposes. Multimodal biometric systems are more reliable because many independent biometric modalities are used. The use of a multiple number of biometric modalities can result in a highly accurate and secure biometric identification system, as a unimodal biometric system may not provide accurate identification due to its non-universal nature. For example, as few people may have worn, cut or unrecognizable fingerprints, fingerprint biometrics can produce erroneous results.

In multimodal biometric systems, the failure of one technology may not seriously affect individual identification, as other technologies can be used successfully. As a result, identity theft can be considerably minimized, improving the efficiency of the overall system. The reduction in the failure rate to register for multimodal assessment is very significant, and is one of the major benefits of this system.The block diagram of general multimodal biometrics is shown in Fig. 2.6.

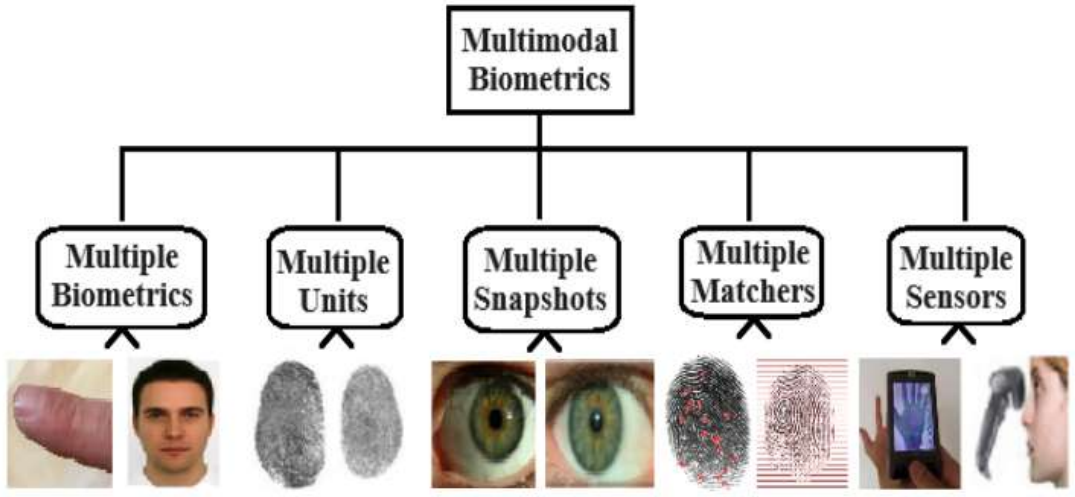

FIGURE 2.6: Block diagram of general multimodal biometrics.

Some of the limitations imposed by unimodal biometrics can be overcome by including multiple source of information for establishing identity of person[14]. The multimodal biometric system offers a number of advantages over the unimodal biometric system, as listed below:

- Offers a substantial improvement in the matching accuracy as compared to that of unimodal system.
- Capable of addressing the non-universality issue.
- Multimodal biometric systems are less sensitive to imposter attacks.
- Insensitive to the noise on the sensed data.
- Help in continuous monitoring or tracking the person in situation when a single biometric trait is not enough[15].

2.6 Review of Biometric Fusion

In a biometric system, the amount of available information gets compressed as one progresses along the various modules of the system [16]. Based on the type of information available in a certain module, different levels of fusion can be defined. Biometric fusion constitutes multiple types of biometric data for improving the performance of biometric systems. A perfect biometric should be unique, universal, and permanent over time that is easy to measure. No single biometric can fulfills all these requirements simultaneously. Therefore combination of several complementary biometrics can provide higher recognition [17].

From levels of fusion, multi-biometrics is classified into two broad categories: fusion before matching and fusion after matching Fig. 2.7 [18].

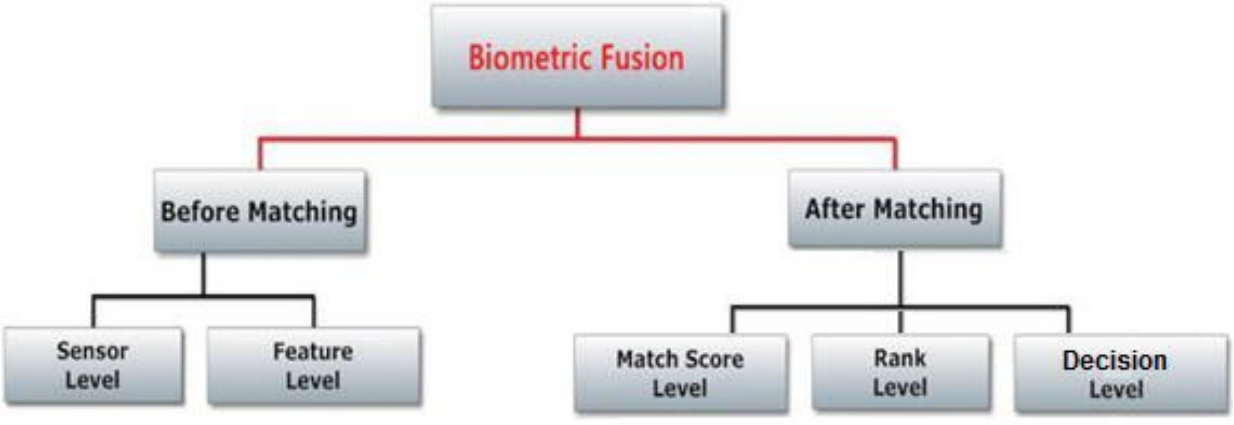

FIGURE 2.7: Biometric fusion levels, Fusion before or after matching.

2.6.1 Fusion Before Matching

Fusion before matching may be performed at the level of sensors or features. When done at the sensor level, the fusion procedure merges data from different sensors, usually concerning the same biometric trait. This approach is not too common, although it does got used in some hybrid systems [19]. In these cases, there is often competition with other approaches in order to improve the Equal Error Rate "EER". EER is one of the main indicators of robustness in biometric systems: the value where the false positive rate equals the false negative rate.When fusion is done at the level of features, different features are extracted via different techniques. They are then processed in order to produce a new feature array. Examples of this approach using neural networks can be found in [20, 21].

2.6.2 Fusion After Matching

Fusion after matching can be carried out at the score level, rank level or decision level. Match Score level fusion, with score level fusion, different algorithms produce individual scores, possibly based on different biometric traits. These scores are combined to obtain the final score. Rank level fusion means the classifiers rank the classes, with higher rank implying a better match, and the rankings are combined to obtain the final rank [22]. Decision level fusion is the latest possible stage. After feature extraction, matching and recognition, each biometric subsystem gives a response as to the authenticity of the subject. The final decision combines the individual response, usually by means of logical or Boolean operators. The most common contemporary use of decision level fusion is in crypto-systems [23].

2.7 Performance Evaluation

Different metrics can be used to rate the performance of a biometric factor, solution or application. The performance of biometric systems is an important issue in high-security applications. In fact, the system must match the characteristic of the person to be recognized against the whole set of characteristics stored in the database, thus deciding if one of these is sufficiently similar to the one considered. Where, the matching between the stored template and the template constructed generates a confidence score to check if they're a genuine user or an impostor.

2.7.1 Error Rates

The degree of similarity between two biometric feature sets is indicated by a similarity score. A similarity match score is known as a genuine or authentic score if it is a result of

matching two samples of the same biometric trait of a user. It is known as an impostor score if it involves comparing two biometric samples originating from different users. An impostor score that exceeds the threshold results in a False Accept Rate (FAR), while a genuine score that falls below the threshold results in a False Reject Rate (FRR) [24, 25]. Therefore,

$$FAR = \sum t = TmaxTFA(t) \sum t = 0 \infty AI(t) \tag{2.1}$$

$$FRR = \sum t = TTRA(t) \backslash \sum t = 0 \infty AG(t) \tag{2.2}$$

The Genuine Accept Rate (GAR) or True Accept Rate (TAR) is defined as the fraction of genuine scores that exceed the threshold [25]. Therefore,

$$GAR(\eta) = p(s \geq \eta \mid \omega 1) = 1 - FRR(\eta) \Rrightarrow GAR = 1 - FRR \tag{2.3}$$

Equal Error Rate (EER) is the rate where both accept and reject error rates are equal. EER is also called Crossover Error Rate (CER) with lowest EER are most accurate [25]. Therefore,

$$FRR = FAR \tag{2.4}$$

2.8 Conclusion

Biometric technologies are now able to achieve fast, easy-to-use authentication with high precision. Biometric technologies will benefit many areas.

Any efficient biometric system depends on the accuracy rate and it's higher performance. The degree of accuracy defined by a plenty of methods from measures of error rate such as false rejection rate and false acceptance rate.

Here, we covered architecture of a biometric system to achieve the objective of recognition in both enrolment and test. Also, we have discussed an advantages and necessity of

multimodal systems compared to unimodal biometric systems, as well as the different scenarios involved in multimodal biometric system development. In this context, the biometrics information fusion plays a key role for biometrics system improvement. Vast majority of works focus score level fusion, this is because of the richness of information.

Chapter 3

PROPOSED BIOMETRICS RECOGNITION

3.1 Introduction

With the development of network and information technology, the society has put forward higher and higher requirements for the security of information systems. Biometric recognition technology has gradually become one of the important methods to enhance the security and stability of information systems.

Palmprint recognition has recently become an interest study in image processing, artificial intelligence, and pattern recognition area. Several biometric applications have recently included deep learning techniques for identification. A variety of patterns are being used to train the deep network. Once the deep learning model has learned the dataset's unique characteristics, it can be incorporated to identify similar patterns. In this chapter, we will proposed 2D palmprint recognition system based on deep learning techniques, especially AlexNet.

3.2 Proposed Recognition

Various types of biometrics systems have been successfully developed. As a new emerging characteristic, 2D palmprint has many advantages, for example, easy to collect, small noise interference, and user-friendly [26, 27]. In addition, 2D palmprint is a two-dimensional biometric feature with many concavity and convexity patterns. The principal lines, wrinkles,

and minutiae palmprint have led to very good anti-counterfeiting performance in recognitions. Therefore, 2D palmprint recognition technology has been widely studied.

However, hand pose variations, rotations, translations, complicated backgrounds are the common problems in contactless palmprint recognition. To solve these problems, this thesis proposes a palmprint recognition approach based the convolutional neural network (CNN), which consists of three main parts, namely, image preprocessing, CNN feature extraction and matching. In Fig. 3.1, we show the block-diagram of the proposed biometric system based on 2D palmprint images. For train phase, we perform a preprocessing step to ensure the size and dimensions necessary to run our algorithm. After that, the feature will be as a training data used to create models based on AlexNet processing. In the test phase, the features are extracted from tested image, then are matched with models to make decision.

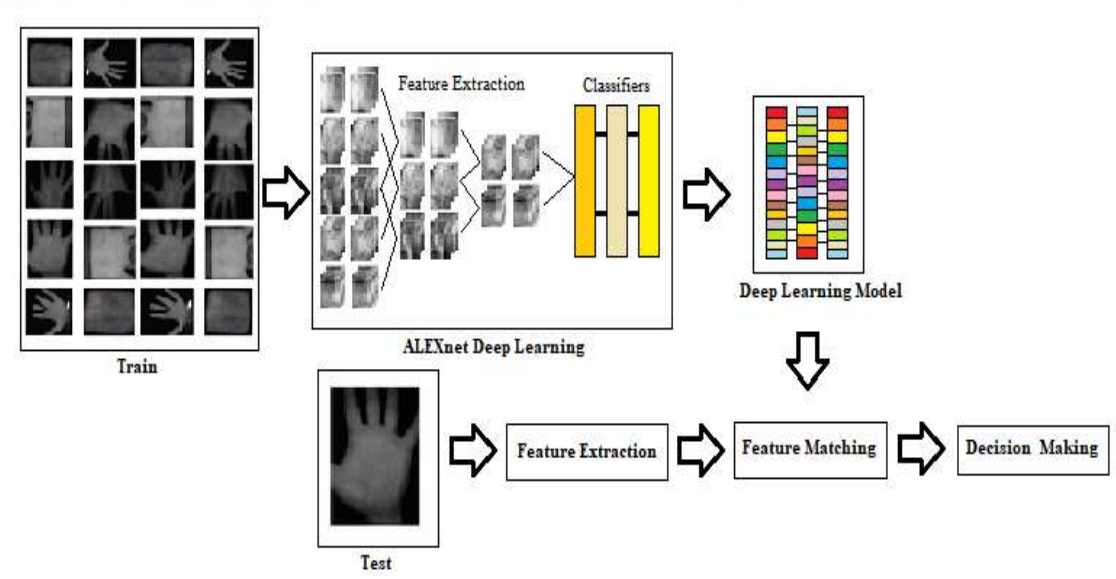

FIGURE 3.1: Block-diagram of the proposed biometric system.

3.3 Our Contribution

Palmprint attracts more and more scholars' attention due to its advantages. Compared with other biological features, palmprint is easier to obtain rich personal information due to its larger surface area. But, palmprint recognition presents a number of complex challenges, primarily due to reduced pattern quality, variations in focal length, nonlinear deformation

and computational complexity [28].

A 2D palmprint biometric system employs 2D imaging device to acquire surfaces of human palm. Extracted features from this data include depth and curvature of palm lines and wrinkles on the palm surface. Therefore, in this work, our aim is to using the 2D palmprint as a distinctive biometric for recognition, which refers to the distinct pattern present on the palm. As, we aim to apply deep learning techniques for our proposed recognition due to its high efficiency in classification problems.

3.4 AlexNet:Deep Neural Network

Convolutional Neural Network is the widely used deep learning framework which was inspired by the visual cortex of animals . Initially it had been widely used for object recognition tasks but now it is being examined in other domains as well like object tracking, pose estimation, text detection and recognition, visual saliency detection, action recognition, scene labeling and many more [9].

Neural networks can be visualized as a collection of neurons arranged as an acyclic graph. The main difference from a neural network is that a hidden layer neuron is only connected to a subset of neurons in the previous layer. Because of this sparse connectivity it is capable to learn features implicitly. The deep architecture of the network results in hierarchical feature extraction [30].

3.4.1 AlexNet Architecture

The architecture of AlexNet comprises five convolutional layers, three fully connected layers, and one SoftMax output layer. The input is an RGB image of size 227×227×3, and the output is the probability of the image belonging to one of the 1000 object categories. The Fig. 3.2 below shows the various layers of the AlexNet architecture [31].

Convolutional Layers (Conv1-Conv5): There are five convolutional layers in the AlexNet architecture. These layers apply filters that slide across the images to detect features. The first convolutional layer uses a filter of size 11×11 to capture broader, low-level features like edges and textures. The filter size in the subsequent convolutional layers is less (15×5 or 3×3) as they focus on specific details within prominent features [32].

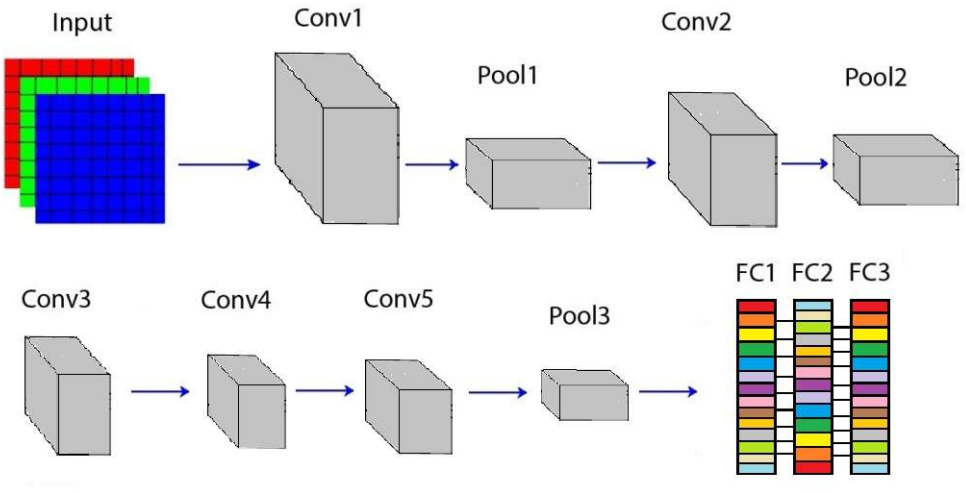

FIGURE 3.2: The various layers of the AlexNet architecture.

Pooling Layers (Pool1-Pool3): The Max pooling layer helps to reduce the spatial dimensions of the data while retaining important features. There are three max-pooling layers in the AlexNet, which have a filter of size 3×3 with a stride of 2.

Normalization Layer (Norm1 and Norm2): In the AlexNet architecture, two local response normalization layers (LRN) are used after the first and second convolutional layers to normalize the outputs. It helps the AlexNet network to learn better and differentiate between essential features in the image while avoiding less relevant activations.

Fully Connected Layers: There are three fully connected dense layers in the AlexNet network, and they are responsible for learning high-level features from the output of the previous convolutional and max-pooling layers. The first two dense layers have 4096 neurons each, while the third dense layer has 1000 neurons corresponding to the 1000 classes in the ImageNet dataset [32].

AlexNet's convolutional layers learn features such as edges, textures, and shapes to distinguish between classes. The fully connected layers then analyze these learned features and make predictions.

3.4.2 AlexNet Feature extraction

AlexNet consists of eight layers, five convolution layers and three fully-connected layers. Each convolution layer convolves the set of input feature maps with a set of weight filters resulting in a set of output feature maps. The fully connected layers, what every output

is a function of all the inputs. CNN is a deep learning framework made with expression, speed, and modularity in mind. Therefore, we used the CNN deep learning framework which provides the AlexNet for extracting the palmprint feature. The AlexNet architecture for palmprint feature extraction is depicted in Fig. 3.3.

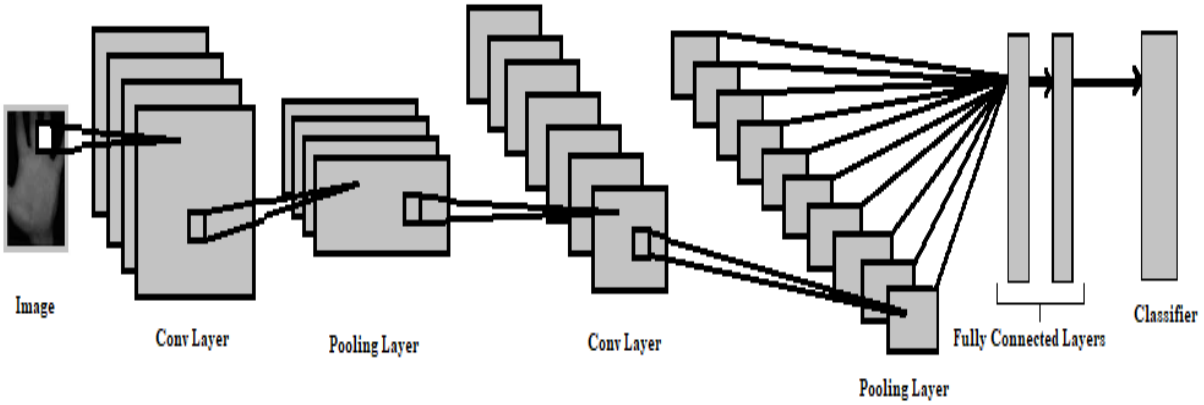

FIGURE 3.3: The AlexNet architecture for palmprint feature extraction.

3.4.3 AlexNet Classification

Classification is the process of determining in which class/label a particular data belongs to. So, after extraction of image features using Alexnet, a classifier is required to decide the corresponding label for every test images. For this, a multiclass Support Vector Machine has been used. Binary classification is the simplest one in which an image is classified into one of the two classes. Multiclass classification is comparatively harder than binary classification because the classifier has to learn to find a number of hyperplanes. There are different approaches to multiclass classification problem [27].

3.5 Feature Fusion

Depending on the type of data fusion can be classified into two major groups, fusion before matching (fusion pre-classification) can take place either at the image level or at the feature level. And Fusion after matching (fusion post-classification) can be divided into two: score levels or at the decision level.

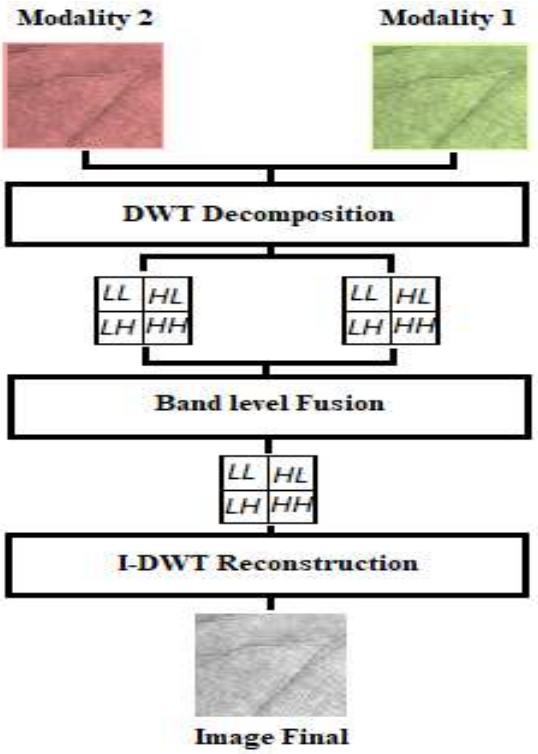

FIGURE 3.4: Image level fusion by DWT.

The raw biometric data represented the richest source of information although it is expected to be contaminated by noise. For image level fusion, we based on Discrete Wavelet Transform (DWT) [33]. Where, the idea of this transform is decomposing a signal to different resolutions. The decomposition of image performs by two filter into sub-bands high-pass and HA low-pass LA. The reconstruction of the image also called synthesis, it requires the use two filters (HS, LS). Image Fusion based on DWT decomposition (Approximation, Horizontal detail, detail Vertical, Diagonal detail) presents in Fig. 3.4. Suppose M1 and M2 are two images, the fusion steps are [33]:

1. DWT (M1) = [A1, V1, H1, D1] and DWT (M2) = [A2, V2, H2, D2].
2. The averages of all sub bands is: [A, G, H, D] = ([A1, V1, H1, D1] + [A2, V2, H2, D2]) / 2.
3. In the end apply the inverse DWT on the results obtained: M = IDWT ([A, V, H, D]).
4. The image M is the fusion of two pictures M1 and M2.

3.6 Conclusion

The proposed system based on 2D palmprint identification is having several advantages. In this chapter, we presented the methodology of proposed biometric system and gave detail of the various modules in this system; beginning by the implementation of AlexNet method to extract the features from palmprint trait, then how classified of these feature vectors to create stored models in database. Furthermore, the proposed method has been successfully implemented for our authentication system based on deep learning descriptors. This eligibility can be confirmed further after reviewing the results in the next chapter.

Chapter 4

EXPERIMENTATIONS AND RESULTS

4.1 Introduction

Assessing the performance of biometric recognition technologies is critical in information security field. Palmprint biometric is most used because it's high recognition accuracy rates. Since each individual's palmprint is unique, it can be strongly relied upon to achieve accurate discrimination between individuals. However, there are challenges that need to be addressed such as environmental complexities and lighting effects. Dealing with these difficulties requires the appropriate use of data processing techniques and advanced algorithms.

In this chapter, we are going to evaluate palmprint recognition based on AlexNet by using MATLAB software. The multiple experiments and deep analyze of results will give an idea about the proposed system and its point of strength based on the obtained performance.

4.2 Database

The development of an identification biometrics systems involves the use of a database to evaluate its performance. During these last years, several databases have been developed to evaluate the algorithms of biometric recognition. The Biometric Research center at Hong Kong Polytechnic University has developed a real time multis pectral palmprint capture device which can capture palmprint images, and has used it to construct a large scale multis pectral palmprint database. Thus, we have adopted it in our proposed system and for that

our experiment tests were performed using the PolyU Palmprint Database [34].

The combined Palmprint database from 150 different subjects, including 95 men and 55 women. They collected samples in two separate sessions. This database also provides many samples in different age groups to support studies. Such images are made publicly available for all the subjects and can be easily identified using the names of respective images/folders in the database [34].

4.3 Parameters Selection

AlexNet parameter selection refers to the process of determining the appropriate values for the parameters used in the CNN transformation. The process of CNN parameter selection depends on the specific application and performance require-ments. The process of parameter selection may involve conducting experiments and tests to evaluate the performance of different parameters and selecting the values that produce the best results.

4.3.1 Selection of Mini Batch Size

Mini batch size use to create, pre-processing, and manage mini-batches of data for training using custom training loops, or convert data to a different precision, or apply a custom function to pre-processing your data.

Firstly, to determine the 'mini batch size' configurations in our approach, we describe the sub-results related to the proposed Mini Batch Size configuration parameter. When using different numbers of configurations such as $10, 20, 30, and 40$ for each test. With save of default parameters: "Epochs equal 6 and Initial Learn Rate equal 1e-4". In Table. 4.1, we present the test results of our palmprint recognition systems.

From this Table. 4.1, it is evident that the set of four configurations for mini batch size provides better results in terms of GAR. In this case, the 20 size of mini batch size for AlexNet that can achieve a GAR of 99.98% at a time T = 48min 34s. Additionally, from this table, we can observe that the configuration of 10 that offer a GAR of 99.67% at a time T = 78min 0s. Furthermore, using the configuration of 30 that offer a GAR of 98.22% at a

NUMBERS	EER(%)	GAR(%)	Training Time
10	0.33	99.67	78min 0s
20	0.02	99.98	48min 34s
30	1.78	98.22	26min 4s
40	2.33	97.67	18min 27s

TABLE 4.1: Results of different mini batch size parameters.

time T = 26min 4s. Finally, using the configuration of 40 for AlexNet that yields a GAR of 97.67% at a time T = 18min 27s. The curves for the four AlexNet configurations of mini batch size are shown in Fig. 4.1, where the Accuracy (GAR) is plotted against the Iteration (epochs).

Therefore, the system can achieve the best accuracy with the configuration of 20 mini batch size for AlexNet compared to the other configurations, which produces an GAR of 99.98% with an EER of 0.02%.

4.3.2 Selection of Epochs

An epochs is defined as the number of times an algorithm visits the data set .In other words, epoch is one backward and one forward pass for all the training.

Secondly, to select the number of epochs, this subsection describes a results of the proposed epochs number parameter. When, we using a different probability of numbers as "1, 6, 11 and 16" of each test, with save of other default parameters: "mini batch size equal to 10 and Initial Learn Rate equal to 1e-4". Thus, Table. 4.2 present the test results of the epochs parameter for our systems.

NUMBERS	EER(%)	GAR(%)	Training Time
1	5.22	94.78	13min 1s
6	0.33	99.67	78min 0s
11	0.22	99.78	153min 53s
16	0.02	99.98	1808min 18s

TABLE 4.2: Results of different epochs number parameters.

From this Table. 4.2, it is evident that the set of four configurations for epochs provides better results in terms of GAR. In this case, the 16 number of epochs for AlexNet that

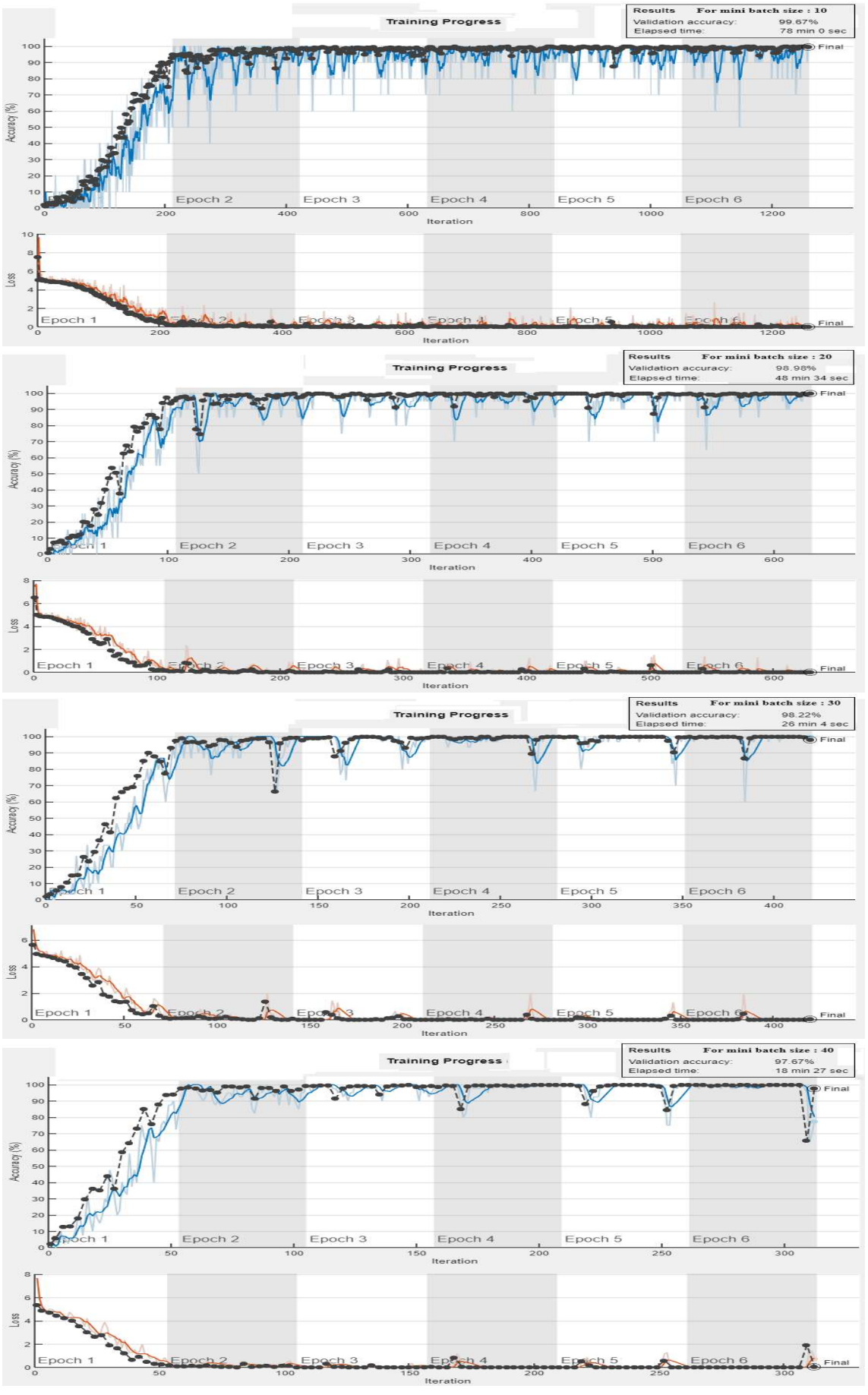

FIGURE 4.1: The results of AlexNet for different mini batch size parameters.

can achieve a GAR of 99.98% at a time T = 1808min 18s. Additionally, from this table, we can observe that the configuration of 1 that offer a GAR of 94.78% at a time T = 13min 1s. Furthermore, using the configuration of 6 that offer a GAR of 99.67% at a time T = 78min 0s. Finally, using the configuration of 11 that yields a GAR equal to 99.78% at a time T = 153min 53s. The curves of the four cases of AlexNet epochs configurations are shown in Fig. 4.2, where the Accuracy (GAR) is plotted against the Iteration (epochs).

Therefore, test results indicate that the system can achieve the best accuracy with the configuration of 16 epochs for AlexNet compared to the other configurations, But compared with the time rates, it takes a very large amount of time (1808min 18s), so we will skip it for 11 epochs due to the very small difference in GAR, with a huge difference in time of 153min 53 for 11 epochs.

4.3.3 Selection of Initial Learning Rate

Initial learning rate used for training, specified as a positive scalar. If the learning rate is too low, then training can take a long time. If the learning rate is too high, then training might reach a sub-optimal result or diverge.

Thirdly, to select the last parameter (the learning rate), this subsection describes a results of the proposed parameter. When, we using a different learning time of rates as "1e-1, 1e-2, 1e-4 and 1e-6", with also save of other default parameters: "Epochs equal to 6 and mini batch size equal to 10". Thus, Table. 4.3 present the test results of the learning rate parameter for our recognition systems.

NUMBERS	EER(%)	GAR(%)	Training Time
$1e-1$	33	67	74min 10s
$1e-2$	33	67	73min 38s
$1e-4$	0.33	99.67	78min 0s
$1e-6$	7.11	92.89	74min 20s

TABLE 4.3: Results of different Initial learn rate number parameters.

From this Table. 4.3, it is evident that the set of four configurations for Initial learning rate provides better results in terms of GAR. In this case, the rate of 1e-4 of Initial learning rate for AlexNet that can achieve a GAR of 99.67% at a time T = 78min 0s. Additionally, from this table, we can observe that the configuration of rate 1e-1 and 1e-2 for AlexNet

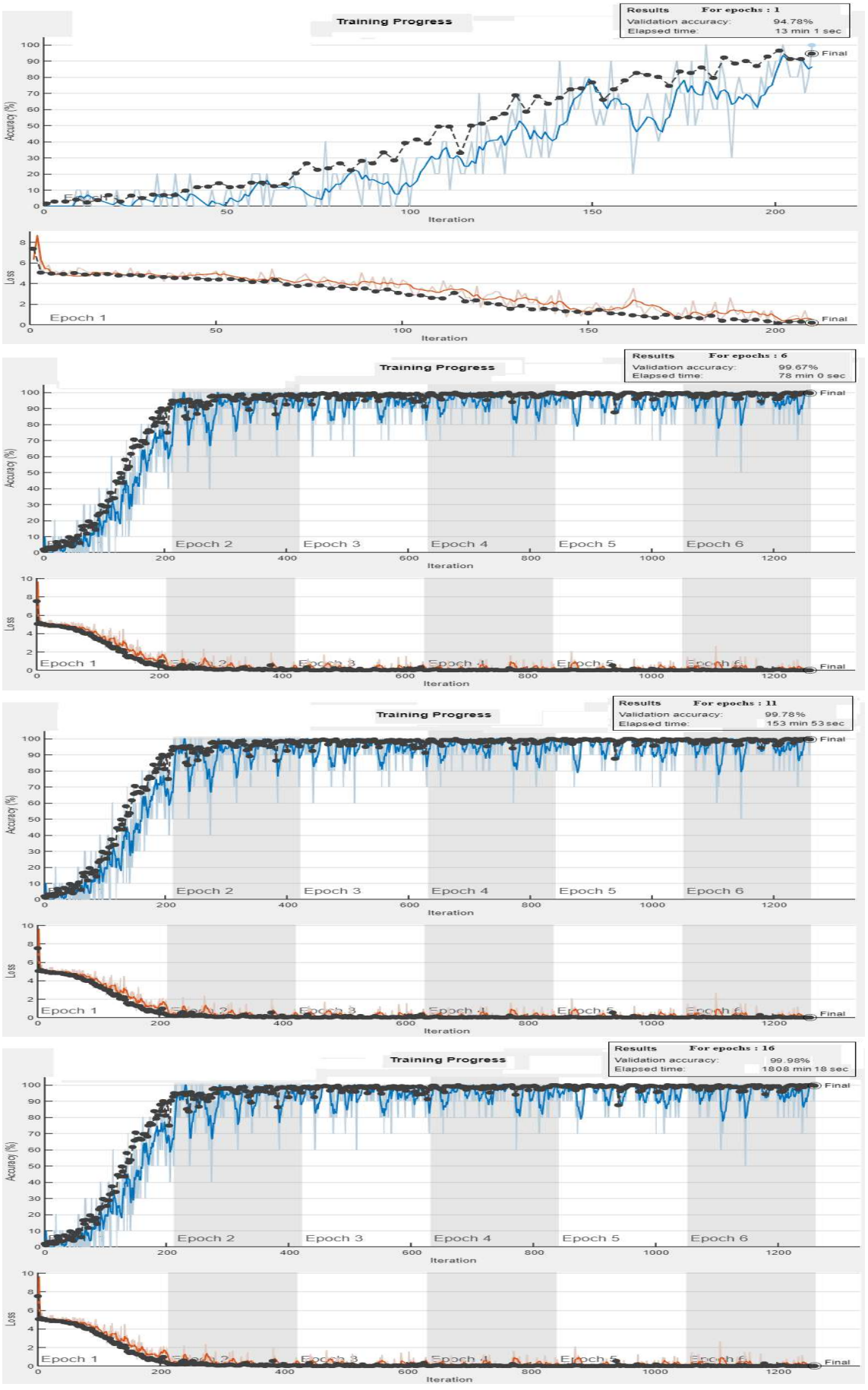

FIGURE 4.2: The results of AlexNet for different epochs parameters.

that offer the same result, a GAR equal to 67% at a a time T = 74min 10s / 73min 38s, respectively . Finally, using the configuration of rate 1e-6 for AlexNet that yields a GAR equal to 92.89% at a time T = 74min 20s. The curves of the best learning rate configurations are shown in Fig. 4.3, where the accuracy (GAR) is plotted against the Iteration (epochs).

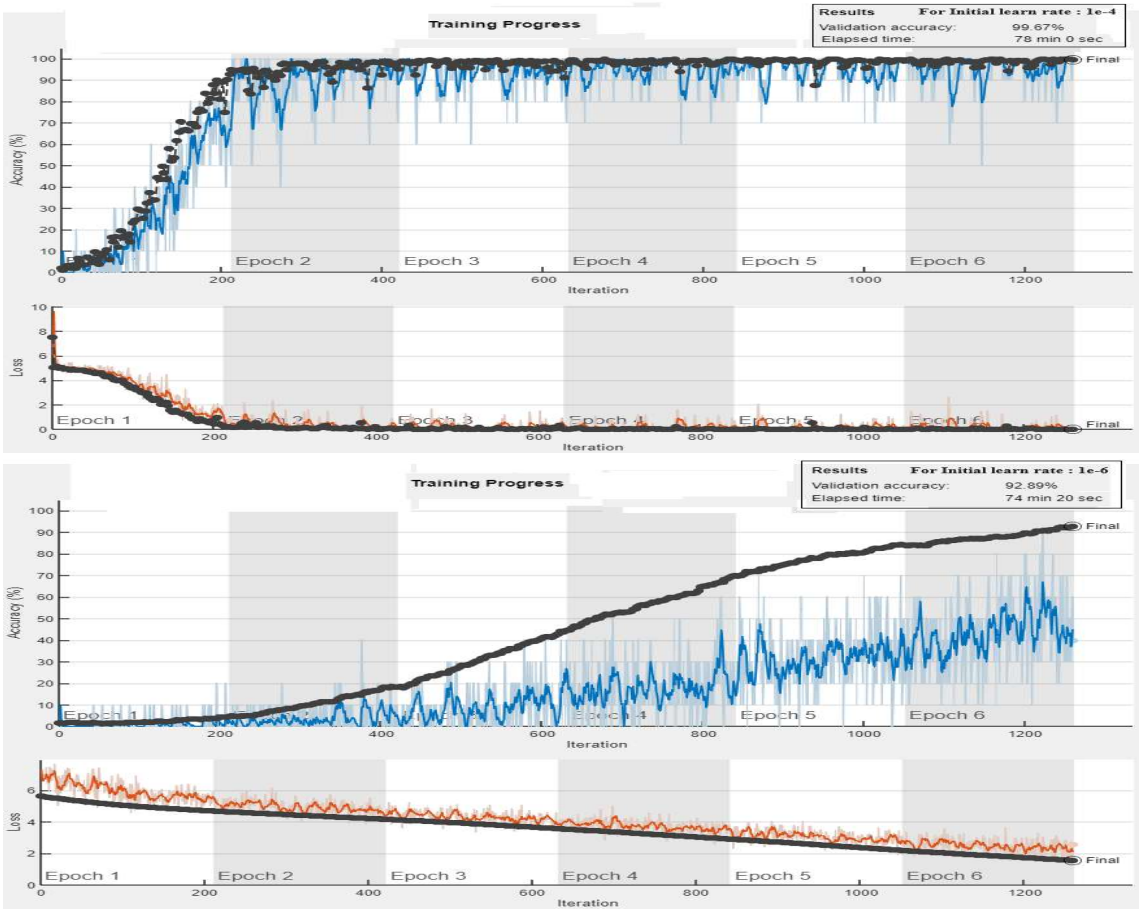

FIGURE 4.3: The results of AlexNet for different Initial learn rate number parameters.

Therefore, the system can achieve the best accuracy with the configuration of 1e-4 Initial learning rate of AlexNet compared to the other configurations, which produces a GAR equal to 99.67% with an EER equal to 0.33%.

4.4 Biometric System Evaluation

Depending on the preceding results, the AlexNet algorithm can be set to the following parameters: the mini batch size equal to 20, the epochs number are 11, also the initial learning rate is (1e-4). Therefore, we have decided to choose these parameters in the rest of test study.

4.4.1 Obtained Results of Unimodal Systems

In unimodal biometrics, theoretically it might be very proficient but in reality it has various numbers of challenges when enrolling large number of people. For unimodal system, we will use the parameters we have already determined for the accuracy of its results, which is a GAR equal to 97.69% with an EER equal to 2.31% at a Time equal to 107min 1s. The accuracy results of unimodal systems based on AlexNet described in Fig. 4.4.

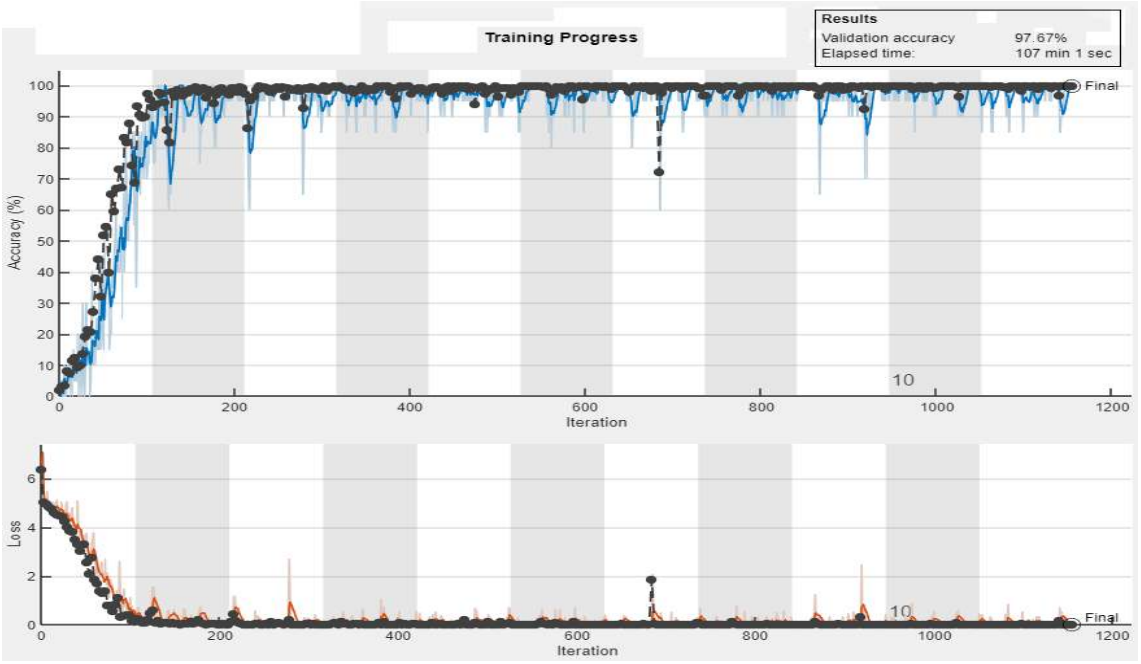

FIGURE 4.4: The Unimodal results of AlexNet algorithm.

Also, for unimodal tests, we will test the AlexNet algorithm by predicting a person's palmprint to see if the prediction is correct? The performances of some random tests are presented in Fig. 4.5. The results can provide that the prediction is correct for our tests.

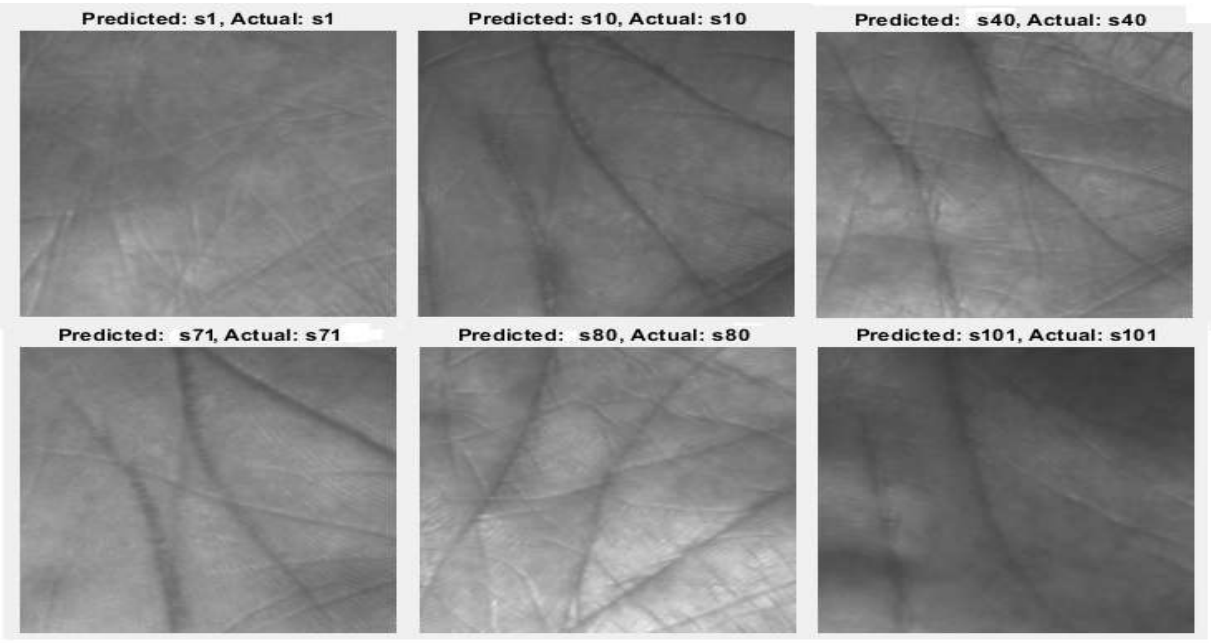

FIGURE 4.5: The unimodal tests prediction results of AlexNet algorithm.

4.4.2 Obtained Results of Multimodal Systems

The unimodal biometric face many obstacles such as paucity of distinctiveness, global similarity, and can be improved by using multimodal systems. In multimodal systems, biometric information can be fused at several different levels. In our work, we only choose the image level fusion, and we used an efficient image fusion algorithm, with the help of 2D-DWT techniques.

For multimodal, we will use the same configurations parameters we have already determined, from the result which are a GAR equal to 99.89% with an EER equal to 0.11% at a Time equal to 289min 20s. Thus, we can see that the fusion reduce the EER from 2.31% in unimodal to 0.11% in multimodal system. The accuracy results of multimodal systems based on AlexNet algorithm described in Fig. 4.6.

Also, for multimodal tests, we will test the AlexNet algorithm with an efficient image fusion algorithm by predicting a person's palmprint images. The results can provide that the prediction is correct for our tests, the performances of some random tests are presented in Fig. 4.7.

FIGURE 4.6: The multimodal test results of AlexNet algorithm.

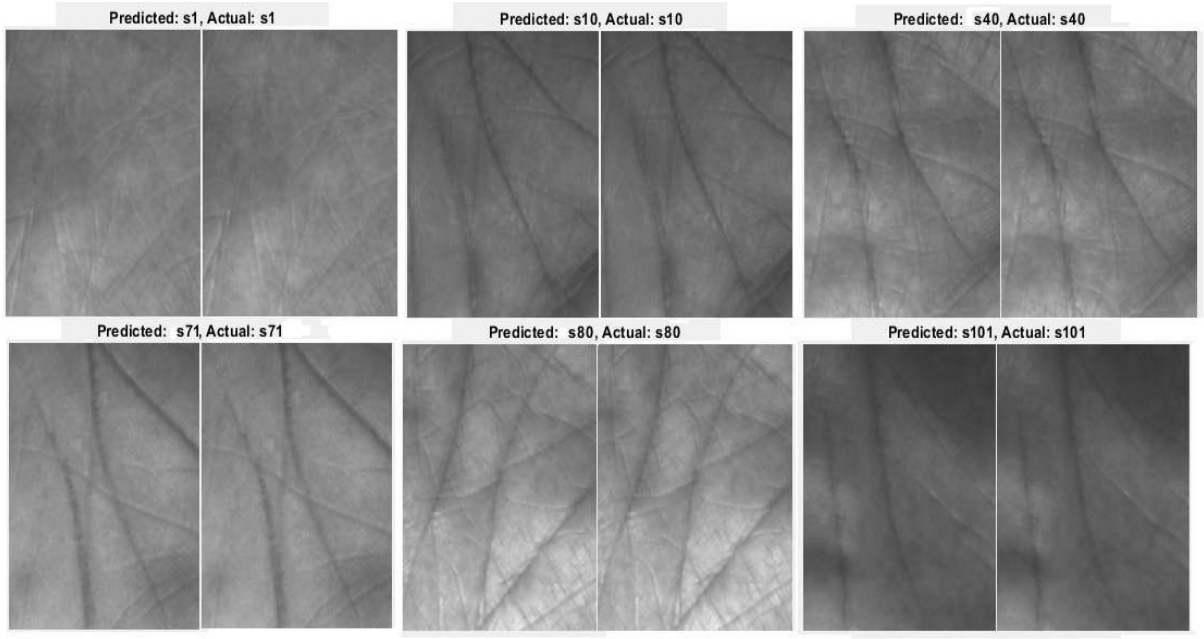

FIGURE 4.7: The multimodal tests prediction results of AlexNet algorithm.

The purpose of this study is to improve the performance and effectiveness of recognition and classification systems and provide biometric identification based on palmprint recognition. The obtained results showed an accuracy rate equal to 97.69% and an accuracy rate equal to 99.89% for the unimodal system and multimodal system, respectively.

4.5 Conclusion

This chapter presents a test and evaluation of one of the deep learning algorithms to identification system. The proposed multimodal system was developed and its performance was evaluated using fusion of image level. The tested database contains palmprint images of 150 individuals. Through multiple experiments, the AlexNet parameters were tested to select the best authentication performance. These parameters include: the mini batch size equal 20, the epochs number are 11, also the Initial Learning Rate is (1e-4).

In addition, this chapter obtained results from various experiments using unimodal and multimodal recognition systems. The performance are significantly improved by using the fusion of sample and can give a EER equal to 0.11% while the unimodal identification give only a EER equal to 2.31%.

In the end of this chapter, the performance of multimodal biometrics much improved then unimodal biometrics. Thus, we summarize that the fusion of images in multimodal biometric systems improves the performance and accuracy identifying.

Chapter 5

CONCLUSIONS AND FUTURE WORKS

THE science of authenticating a person's identity based on their physical, or behavioral traits is known as biometrics. A biometric system is simply a pattern recognition system that identifies people based on their features. In this work, we used palmprint biometrics, which is known for its high precision, reliability, and difficulty of manipulation. This technology is useful in various fields such as security and access control, secure payment applications.

In this thesis, two main techniques used, were Convolutional Neural Network AlexNet for feature extraction and for image classification. Then has been used 2D-DWT for image fusion level for proposed multimodal system. The tested PolyU Palmprint database contained palmrprint images of 150 individuals. Through many experiments, AlexNet parameters were selected to the best authentication performance. These parameters included the mini batch size equal 20, the epochs number are 11, also the Initial Learning Rate to $(1e-4)$.

From different experiments, the performance of the recognition system has been significantly improved by integrating multimodal recognition, achieving an Equal Error Rate (EER) of 0.02% , whereas unimodal recognition only achieves an EER of 5.98% . Thus, multi-modal recognition systems demonstrate efficiency and robustness in recognition rates.

As future work, we will apply deep learning methods with a more credible big database. Where, the identical conditions can be employed for further performance analysis, there is plenty of room to improvement by suggesting network architects able to balance accuracy needs with time and the high computational cost.

Bibliography

[1] A.F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey", *Pattern Recognition Letters*, Vol. 28, No. 14, pp. 1885-1906, 2007.

[2] K. Arai et al Eds, "Springer Nature Switzerland AG", Vol. AISC 858, No. SAI 2018, pp. 581-591, at: , 2019.

[3] A.K. Jain, A. Ross, S Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, Vol. 14, pp. 4-20, 2004.

[4] "Biometrics characteristics", available at:www.findBiometrics.com, 2012.

[5] A.A Iqbal, "An overview of leading biometrics technologies used for human identity", *In Student Conference on Engineering Sciences and Technology, SCONEST IEEE*, 2005.

[6] R. Alexander, "Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures?", A Quantitative Study, *Journal of Information Security*, Vol. 8, No. 166, 2017.

[7] D.W. Sanders, S.K. Kaufman, B.B. Holmes, M.I. Diamond, "Prions and protein assemblies that convey biological information in health and disease, Neuron", Vol. 89, pp. 433-448, 2016.

[8] M.W. Khan, M. Sharif, M. Yasmin, S.L. Fernandes, "A new approach of cup to disk ratio based glaucoma detection using fundus images", *Journal of Integrated Design and Process Science*, Vol. 20, pp. 77-94, 2016.

[9] C. Kant, and R. Jain, "Attacks on Biometric System: An Overview", *International Journal of Computer Science and Application*, Vol. 3-2, pp. 1090-1094, 2015.

[10] A. Obied, "How To Attack Biometric System In Your Spare Time", *International Journal Of Scientific and Technology Research*, Vol. 4, pp. 1-9, 2011.

[11] R. CHLAOUA. "Combination of Multiple Biometrics for Recognition of Persons", *Doctoral Thesis, UNIV. of KASDI MERBAH OUARGLA*, 2019.

[12] A. Ross, K. Nandakumar, A. K. Jain, "Handbook of Multibiometrics", Springer, 2006.

[13] K. Sasidhar, Vijaya L Kakulapati, "Multimodal Biometric Systems: STUDY To Improve Accuracy And Performance IJCSES", Vol.1, No.2, November 2010.

[14] A. Ross, A. Jain, "Information Fusion in Biometrics", *Journal of Pattern Recognition Letters*, vol. 24, pp. 2115-2125, 2003.

[15] G. H. Kumar, M. Imran, "Research Avenues in Multimodal Biometrics", *lJCA Special Issue on "Recent Trends image Processing and Pattern Recognition "*, RTIPPR, 2010.

[16] Sonal, A. Singh, "Review on Multibiometrics: Classications, Normalization and Fusion Levels", *IEEE, International Conference on Advances in Computing and Communication Engineering* , Vol, DOI:10.1109, No. 8441727, 2018.

[17] A.K. Jain, A. Ross, K. Nandakumar, "Introduction to Biometrics", Foreword by James Wayman, Springer.

[18] C. Sanderson, K. K. Paliwal, "Information fusion and person veriffication using speech and face information", IDIAPRes Inst, Martigny, Switzerland, Tech. Rep. Idiap RR-33 2002.

[19] M. Imran, A. Rao, G. H. Kumar, "A New Hybrid Approach for Information Fusion in Multibiometric Systems", *Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics*, DOI: 10.1109, NCVPRIPG, IEEE, 2011.

[20] V. Talreja, M. C. Valenti, N. M. Nasrabadi, "Multibiometric secure system based on deep learning", *IEEE Global Conference on Signal and Information Processing GlobalSIP*, DOI: 10-1109, No. 8308652, 2017.

[21] A. Rattani, N. Reddy, R. Derakhshani, "Multi-biometric Convolutional Neural Networks for Mobile User Authentication", *IEEE International Symposium on Technologies for Homeland Security HST*, DOI: 10-1109 THS, No. 8574173, 2018.

[22] R. Sharma, S. Das, P. Joshi, "Rank level fusion in multi-biometric systems", *IEEE Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics*, DOI:10-1109 .No. 7489952, 2015.

[23] S. Vani Nair, G. N. Reshmypriya, M. M. Rubeena, K. A. Fasila, "Multibiometric Cryptosystem Based on Decision Level Fusion for File Uploading in Cloud", *IEEE, International Conference on Recent Advances in Electronics and Communication Technology*, DOI: 10-1109, No. 19, 2017.

[24] M. Golfarelli, D. Maltoni, "Scienze dell'Informazione", Università di Bologna, via Sacchi 3, 47023 Cesena (FO), Italy.

[25] M. Al. Rousan, B. Intrigila,"A Comparative Analysis of Biometrics Types: Literature Review", *Journal of Computer Science*,Vol. 16-12, No. 1778-1788, 2020.

[26] W. Jia, B. Zhang, JT Lu, YH Zhu, Y Zhao, WM Zuo, "Palmprint recognition based on complete direction representation", *IEEE Trans Image Process*, Vol. 26-9, No. 4483-4498, 2017.

[27] I. Rida , R. Herault, GL. Marcialis, G. Gasso, "Palmprint recognition with an efficient data driven ensemble classifier", *Pattern Recognit Lett*, https://doi.org/10.1016/j.patrec.2018.04.033, 2018.

[28] Y. Liu , A. Kumar,"Contactless Palmprint Identification Using Deeply Learned Residual Features", *IEEE Trans, Biom. Behav, Identity Sci*, Vol. 2, No. 172-181, 2020.

[29] J. Fan, W. Xu, Y. Wu, and Y. Gong, "Human tracking using convolutional neural networks", *Neural Networks, IEEE Transactions*, 2010.

[30] A. Krizhevsky. "Convolutional deep belief networks on cifar-10". *Unpublished manuscript*, 2010.

[31] M. Elleuch, R. Maalej, M. Kherallah, "A New Design Based-SVM of the CNN Classifier Architecture with Dropout for Offline Arabic Handwritten Recognition", *The International Conference on Computational Science ICCS*, vol. 80, 2016.

[32] H. Huynh , B. Truong , K. Nguyen Thanh, D. Truong. "Plant Identification Using New Architecture Convolutional Neural Networks Combine with Replacing the Red of Color Channel Image by Vein Morphology Leaf. Vietnam J Comput Sci". Vol. 7, No. 2, 2020.

[33] L. Huang, , H. Zhuang, and S. Morgera, "A Method towards Biometric Feature Fusion", *International Journal of Biometrics*, Vol. 1, No. 4, pp. 479-494, 2009.

[34] D. Zhang, G. Zhenhua, L. Guangming, L. Zhang, W. Zuo. "An online system of multispectral palmprint verification", Vol. 59, 2010.