

**People's Democratic Republic of Algeria 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

Field: Science and Technology

Specialty: Telecommunications Systems

By: REZIG INAS

Theme:

Personal Information Security Using Biometric Traits

Sustained before the jury composed of:

Dr. Bensid Khaled	MCA	Ouargla University	President
Dr.Lati Abdelhai	MCA	Ouargla University	Examiner
Dr. Korichi Marouf	MCA	Ouargla University	Supervisor

2024/2025

Abstract

to the accelerated development in the fields of Science and technology, traditional means of protecting personal information such as cards and passwords are becoming less effective and more vulnerable to hacking and fraud. This has led to the emergence of biometric identification technologies as effective, secure and easy-to-use solutions, being based on the unique physiological or behavioral characteristics of individuals, making them suitable for many applications such as criminal identification, access control systems, correctional institutions, and banks. In this context, hand pattern recognition is one of the techniques distinguished by its high accuracy and its ability to extract rich characteristics from the hand image. In this work, we propose a biometric recognition system based on deep learning technologies using bypass neural networks (CNN), for which three well-known models were applied: AlexNet, VGG16, and VGG19. The system was evaluated in the cases of Unimodal and multimodal, with an analysis of the impact of the application of Tied Rank Normalization technology on performance. The simulation results showed the effectiveness of the models used, and also highlighted the differences between the single and multiple systems, which helps in determining the optimal strategy in terms of accuracy and efficiency.

Keywords: biometric, AlexNet, VGG16, VGG19, CNN, SVM, unimodal system, multi-modal system.

الملخص

بسبب التطور المتسارع في مجالات العلوم والتكنولوجيا ، أصبحت الوسائل التقليدية لحماية المعلومات الشخصية مثل البطاقات وكلمات المرور أقل فعالية وأكثر عرضة للقرصنة والاحتيال. وقد أدى ذلك إلى ظهور تقنيات تحديد الهوية البيومترية كحل فعال وأمنة وسهلة الاستخدام ، تستند إلى الخصائص الفسيولوجية أو السلوكية الفريدة للأفراد ، مما يجعلها مناسبة للعديد من التطبيقات مثل تحديد الهوية الجنائية وأنظمة التحكم في الوصول والمؤسسات الإصلاحية والبنوك. في هذا السياق ، يعد التعرف على أنماط اليد إحدى التقنيات التي تتميز بدقتها العالية وقدرتها على استخراج الخصائص الغنية من صورة اليد. في هذا العمل ، نقترح نظام التعرف على البيومترية على أساس تقنيات التعلم العميق باستخدام الشبكات العصبية الالتفافية (سي إن إن) ، والتي تم تطبيق ثلاثة نماذج معروفة: أليكسنيت ، فغ ١٦ ، وفغ ١٩. تم تقييم النظام في حالات متعددة الوسائط والوسائط ، مع تحليل تأثير تطبيق تقنية تطبيع الرتب المربوطة على الأداء. أظهرت نتائج المحاكاة فعالية النماذج المستخدمة ، كما أبرزت الاختلافات بين الأنظمة الفردية والمتعددة ، مما يساعد في تحديد الاستراتيجية المثلى من حيث الدقة والكفاءة.

الكلمات المفتاحية: البيومترية، أليكسنيت، فغ ١٦، فغ ١٩، الشبكات العصبية الالتفافية، س ف م، النظام أحادي النمط، النظام متعدد الأنماط.

Acknowledgment

Thank God who helped me complete this letter and patience, I thank Almighty Allah, who would not have been here if it had not been for his success .

I would also like to sincerely thank my thesis supervisor, Dr.Korichi Marouf, for his guidance and support during this dissertation . I would

especially like to thank all the members of the jury who accepted to preside and read this work and examine my thesis. I would also like to express my

thanks to the professor and doctors of the Department of electronics and communications from KASDI Merbah Ouargla University.

Dedication

I dedicate this work to parents dear to the heart and soul, to those who were my role models and to their joy, which was not completed only by my happiness, and to the father who sacrificed everything, dear mom who gave birth to me .

To my beloved sisters ikram, Ghoufrane, Mais, firdaows and my brother Abd el Rahman .

Thank you to all of you who have been really supportive in my academic career and beyond.

Contents

Abstract	I
الملخص	II
Acknowledgment	III
Dedication	IV
List of Figures	VI
List of Tables	VIII
Acronyms	X
General Introduction	1
Chapter 1: Introduction to Information Security and Biometric Recognition	
1.1 Introduction	4
1.2 Information Security	4
1.2.1 The main elements of Information Security	4
1.3 Biometric	5
1.3.1 Definition of Biometric	6
1.3.2 Basic characteristics of biometric features	6
1.3.3 Biometric Modalities	7
1.4 Unimodal biometric identification system	12
1.4.1 Architecture and Structure	12
1.4.2 limitation of unimodal biometric identification system	13

1.5	Multimodal biometric identification system	14
1.5.1	Architecture and Structure	15
1.5.2	Levels of Fusion	15
1.6	Performance metrics	16
1.6.1	Quantitative Metrics	16
1.6.2	Curve-Based Metrics	17
1.7	Conclusion	18
Chapter 2: Proposed Biometric Identification System Using Hand Related Traits		
2.1	Introduction	20
2.2	proposed system	20
2.2.1	pre-processing	20
2.2.2	Feature Extraction	22
2.2.3	Tied Rank Normalization techniques	28
2.3	Machine Learning (support vector machines)	28
2.4	Conclusion	29
Chapter 3: Experimental Results and Discussion		
3.1	Introduction	31
3.2	Why hand dorsal modality ?	31
3.3	Data base description	32
3.4	Assessment protocol	33
3.5	Work environment	34
3.6	Experimental results and discussion	34
3.7	Unimodal system test result	34
3.7.1	Experimental Results with AlexNet	35
3.7.2	Experimental Results with VGG 16	39
3.7.3	Experimental Results with VGG 19	43
3.7.4	unimodal Performance with Tied Rank Normalization	48
3.8	Multi-modal system test result	49
3.9	Fusion at matching level	49
3.9.1	Algorithmic Fusion	49
3.9.2	biometric Fusion	52
3.10	Conclusion	54
General Conclusion		55
Bibliography		56

List of Figures

1.1	Finger recognition.	8
1.2	Facial recognition.	8
1.3	Iris recognition.	8
1.4	Palm print recognition.	9
1.5	Ear recognition.	9
1.6	Retina recognition.	10
1.7	Gait recognition.	10
1.8	Voice recognition.	11
1.9	Signature recognition.	11
1.10	Electrocardiogram recognition.	11
1.11	Architecture of Unimodal biometric system.	13
1.12	Architecture of biometric system.	15
2.1	Automated segmentation of region of interest (second minor finger knuckle) .	21
2.2	ReLU operation	23
2.3	Max-Pooling Operation.	24
2.4	Fully-Connected Layers.	24
2.5	Architecture AlexNet.	26
2.6	VGG 16 and VGG 19 Layers details.	27
2.7	VGG-16 CNN model architecture.	27
2.8	VGG-19 Model.	28
3.1	Sample finger dorsal image	32
3.2	Assessment protocol.	33
3.3	unimodal system performance Based Alexnet without Tied Rank Normaliza- tion(open-set).	36
3.4	unimodal system performance Based AlexNet without Tied Rank Normaliza- tion (closed-set).	37
3.5	unimodal system performance Based Alexnet with Tied Rank Normalization(open-set).	38
3.6	unimodal system performance Based Alexnet with Tied Rank Normalization (closed-set).	39

3.7	unimodal system performance Based vgg 16 without Tied Rank Normalization (open-set).	40
3.8	unimodal system performance Based vgg 16 without Tied Rank Normalization (closed-set).	41
3.9	unimodal system performance Based vgg 16 with Tied Rank Normalization (open-set).	42
3.10	unimodal system performance Based vgg 16 without Tied Rank Normalization (closed-set).	43
3.11	unimodal system performance Based vgg 19 without Tied Rank Normalization (open-set).	44
3.12	unimodal system performance of the Baseline vgg 19 without Tied Rank Normalization (closed-set.)	45
3.13	unimodal system performance Based vgg 19 with Tied Rank Normalization (open-set).	46
3.14	unimodal system performance Based vgg 19 without Tied Rank Normalization (closed-set).	47

List of Tables

3.1	unimodal system Performance Based AlexNet Without Tied Rank Normalization	35
3.2	unimodal system Performance Based AlexNet with Tied Rank Normalization	37
3.3	unimodal system Performance Based VGG 16 without Tied Rank Normalization	39
3.4	unimodal system Performance Based VGG 16 with Tied Rank Normalization	41
3.5	unimodal system Performance Based VGG 19 without Tied Rank Normalization	43
3.6	unimodal system Performance Based VGG 19 with Tied Rank Normalization	45
3.7	multimodal system Performance Based Algorithmic without Tied Rank Normalization	50
3.8	multimodal system Performance Based Algorithmic with Tied Rank Normalization	51
3.9	multimodal system Performance Based biometric without Tied Rank Normalization	52
3.10	multimodal system Performance Based biometric with Tied Rank Normalization	53

Acronyms

ALIC Average Login Identification Cost

CMC Cumulative Match Characteristic

DET Detection error trade-off

DNA Deoxyribonucleic Acid

UBS Unimodal Biometric System

EER Equal Error Rate

FAR False Accept Rate

FRR False Reject Rate

ROI Region of Interest

ROR Recognition Rate

RPR Rank Position Recognition

ROC Receiver Operating Characteristic

VGG Visual Geometry Group

CNN Convolutional Neural Network

SVM Support Vector Machine

RBF Radial Basis Function

DC Dorsal Center

MUL Multiplication Score Fusion

SUM Summation Score Fusion

MIN Minimum Score Selection

MAX Maximum Score Selection

General Introduction

The issue of information security in the current era is a very important topic and is a concern for all users and technicians. This is a result of the widespread spread of electronic transactions over the Internet. The latter has witnessed a kind of insecurity in the use of passwords, text passwords, symbols and identification cards. All of these have not kept pace with the development that has occurred. Technicians are looking for methods to enhance security and identify identity, as biometric systems are considered the most appropriate alternative and are among the most effective systems in our time. Biometrics play an important element in identifying or recognizing identity. It is a process that allows the identification of a person through the unique behavioral and physiological characteristics that distinguish each individual and are measurable.[1]

One of the promising measurement technologies is hand biometrics, which has received great attention because it achieves high accuracy and due to the deep learning features that are interested in extracting features automatically, it is the most appropriate in identification .[2]

Among them are The Convolution neural network (CNN) is one of the popular models in deep learning, and its design was inspired by the mechanism of human visual perception, which made it one of the most widely used models in advanced research.

Through this study , we will review the possibility of using deep learning techniques using the CNN algorithm (Alexnet,Vgg 16,Vgg 19) to extract features with and without the use of Tied Rank normalization so that this system is able to identify with high accuracy and effectively, and this using the hand.

This system can be used in electronic protection systems, which has proven its effectiveness and can be considered as an alternative to cards and passwords, and it can also be used to control access to sensitive facilities such as banks and banks, where this system plays a crucial role in the criminal

field by identifying the perpetrator and also contributes to securing mobile applications and smart devices.

Our presented work consists of three chapters

The first chapter

In this chapter, we will get acquainted with the basic concepts of information security, biometrics and their types embedded in Physiology, behavioral and the traditional and modern biometric identification method. we also touch on unimodal and multimodal identification systems, both for identification and authentication, as well as learn about the types of biometrics.

The Second chapter

In this chapter, the structure of the identification system using manual attributes is explained and includes a description of the working methodology and a brief description of the deep learning and techniques adopted within the four basic stages of the adopted system .

The third chapter

In this chapter, we evaluate the performance of the proposed hand biometric identification system, where we will discuss the experimental results. In addition, we will compare the performance of a single-media and multimedia system with and without Tied Rank normalization.

Chapter 01

Introduction to Information Security and Biometric Recognition

1.1 Introduction

With the rapid development in the fields of technology and communication systems is an adult evolution that has made the world a small village . Security has become a very important thing or issue because there is no completely secure system, but the thing that can be done is to make the system more secure, difficult to hack or steal its data . Identity is the term used to describe the process of identifying the person in question, identifying source or type.[3]

In this chapter, we will first discuss information security and then move on to biometrics, followed by unimodel biometric identification systems and multimodal biometric identification systems. And finally, performance measures.

1.2 Information Security

The security of personal information is an essential part of life. Rapid technological advancements have led to an increase in security risks. Therefore, we must rely on methods that ensure its protection and confidentiality.

Information security, or "information security," is a set of practices designed to protect data from unauthorized access, modification, or destruction during storage or transmission. It is also referred to as data security. As the importance of knowledge has grown, the need to protect information from various threats has increased. [4]

The role of information security is to prevent fraud or protect data from unauthorized use, disclosure, disruption, inspection, or recording, such as personal information, social media accounts, and biometric data.[5]

1.2.1 The main elements of Information Security

The main elements of information security are very important because they are the basis of protection in this world that has become more interconnected, namely :

Confidentiality

It is the basic element of information security based on data protection Only authorized individuals have access to their sensitive data, which is protected by encryption technologies, passwords and access control systems .confidentiality can also be maintained in organizations by preventing unauthorized users from entering, whether during storage or transmission.[5]

Integrity

Integrity is one of the most important elements in information security, as the latter protects information from theft, deletion or unauthorized access and ensures the accuracy and reliability of data, which is confirmed through backups or digital signatures, as well as hash functions,

which enable organizations to increase the credibility as well as restore information and data in case of loss, forgetfulness or malicious attacks. [6]

Availability

Availability It means that it is available to all users, regardless of their situations, as it enables them to access their information at any time, and this is through the provision of powerful and user-friendly systems for users, as well as the availability of backup copies and the use of reliable servers. [4]

Authenticity

It is an important process in which information security services rely on identifying a person and his identity before granting access to information or services. It depends on three main factors:

- **Something You Know**

It is anything that the user remembers that he can use to verify his identity .It may be a password, an answer to a security question, or a secret code, and it is considered one of the simplest and most common ways to protect information, we may find it used to unlock a phone or an email account, but it is less secure because it is easy to hack or detect and also forgotten by the person (user) or share it with others.

- **Something You Have**

It refers to any physical or digital thing that a person owns and uses to confirm his identity, it may be an access card, badge, smart card, and a mobile phone that receives a one-time password, which is relatively more secure, but a person must always carry this thing with him, which depends on his identification, but it is considered the least practical because it is subject to theft or forgery.

- **Something You Are**

It symbolizes the unique features of each person that can be used to confirm identity . For example, canceling the phone using a fingerprint or face, which is one of the biometric features used that ensures the most security, accuracy and difficulty of penetration because it depends on characteristics from the self, but it needs special systems and devices, as well as sensors.

1.3 Biometric

Biometric authentication has emerged as a solution to the challenges faced by traditional identity verification methods (PIN,smart cards,etc), as it relies on unique characteristics of the user.

1.3.1 Definition of Biometric

Biometrics (ancient Greek: BIOS =”life”, Metron =”measure”) refers to two different concepts in the field of study and application. The first concept is considered the oldest and is used in Biological Studies. Among that forestry, is the collection, synthesis, analysis and management of quantitative data Biological communities such as forests. Biometrics in reference to biological sciences has It has been studied and applied for several generations and is more or less perceived as ”Biological statistics”.[6]

Biometrics is the science of establishing the identity of an individual based on the physical, or behavioral attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual’s identity in the context of several different applications. The proliferation of web-based services (online banking) and the deployment of decentralized customer service centres (credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.[7]

1.3.2 Basic characteristics of biometric features

It is basic and necessary to know what are the basic features of biometric features in order to find out whether this system can be purchased or used or not. [7]

For this, the following characteristics should be available:

- **Universality**

It symbolizes the distinctive and unique biometric characteristic from one person to another, where no two people have the same biometric characteristics, as it ensures the accuracy and reliability of the identification system devices because they are different between people and thus reduces the likelihood of false matches between individuals.

- **Uniqueness**

Uniqueness refers to the extent to which a biometric trait differs from one individual to another. It means that the biometric information should be highly distinctive, making it nearly impossible for two individuals to share the same feature. This property is essential in biometric systems to ensure accurate identification and reduce the chances of false matches, which enhances the overall security of the system.

- **Permanency**

Permanency refers to the stability of a biometric trait over time, meaning that the feature should remain consistent throughout an individual’s life without significant changes. This characteristic is essential in biometric systems, as it ensures that the biometric

information can be used for long-term identification without the need for frequent updates or re-enrollments. Biometric traits such as fingerprints and iris patterns are considered highly permanent, making them reliable for identity verification.

- **Collectability**

Collectability refers to the ability to measure a biometric trait easily using specific devices or systems. This characteristic is essential to ensure that biometric data can be collected in a practical and efficient way, simplifying the identity verification process. For example, fingerprints and facial features are considered highly collectible because they can be easily measured using available sensors or cameras, making them suitable for use in biometric recognition systems. Acceptability refers to the willingness of individuals to adopt and use biometric systems for identification or authentication purposes. It depends on how comfortable users feel about the technology, the level of privacy it provides, and the non-intrusive nature of the biometric trait being measured.

- **Acceptability**

Uniqueness refers to the extent to which a biometric trait differs from one individual to another. This means that the biometric information should be highly distinctive, making it nearly impossible for two individuals to share the same feature. This property is essential in biometric systems to ensure accurate identification and reduce the chances of false matches, which enhances the overall security of the system.

1.3.3 Biometric Modalities

Biometrics can be divided into two parts:

Physical characteristics (physiological and behavioral). The first part is called static measurements and depends on extracting data from the anatomical measurements of the person. The second part is called dynamic measurements and depends on extracting data from the actions of the person.

Physiological biometric

- **Finger recognition**

Scanners are one of the oldest forms of biometrics and are very reliable when it comes to authentication and recognition. These systems are easy to use, making them a favorite among users, and they never change from person to person no matter how old they are, as they rely on a fingerprint pattern of ridges and grooves on the tip of each finger. [8]



Figure 1.1: Finger recognition.

- **Facial recognition** Devices that work with this feature rely on extracting a set of features from a two-dimensional image of the user's face. It relies on determining one of two things:[8]

The shape and location of facial features such as eyes, eyebrows, nose, lips, and chin, and their spatial relationships.

A comprehensive (global) analysis of the face image that represents the face as a weighted combination of a number of standard faces.



Figure 1.2: Facial recognition.

- **Iris recognition**

Iris scanning is a biometric authentication method that uses unique patterns in the iris of the eye to verify a person's identity. The iris, the colored part of the eye surrounding the pupil, has highly complex and distinctive patterns that remain stable throughout life, making it an ideal feature for biometric identification. [8]



Figure 1.3: Iris recognition.

- **Palm print recognition**

As a means of identifying a person, this technology is considered one of the most reliable and accurate methods of verifying a person's identity, as palm print patterns are unique to each individual and cannot be repeated between people, even between identical twins. This technology relies on analyzing the lines and curves found in the palm of the hand. [9]



Figure 1.4: Palm print recognition.

- **Vein recognition**

Finger vein scanning is one of the latest biometric methods. It captures images of the unique vein patterns within a finger or hand by passing near-infrared light through it and recording the effect via a sensor. [9]

- **Ear recognition**

The ear can be identified using a thermal image, an ear print, or a digital photograph. An ear print can be taken by pressing the ear against a flat piece of paper. It is a rare biometric feature among individuals, but not everyone likes it. [10]

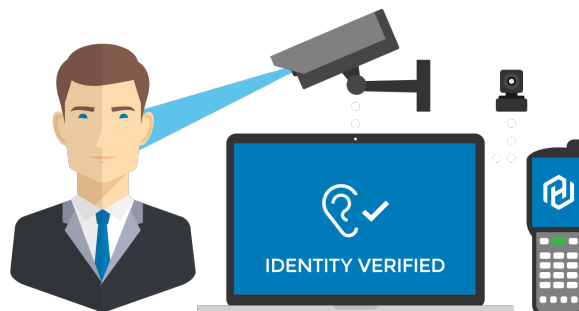


Figure 1.5: Ear recognition.

- **Retina recognition**

retina recognition Infrared retinal scanning is an authentication method based on the vascular patterns of the retina, which is one of the most precise biometric techniques available. The process begins with shining a small beam of infrared light into the eye. Retinal scanning is very accurate because of the uniqueness of the human retinal vessel pattern. Retinal patterns are stable and do not change from childhood through adulthood. However, since the retina is located inside the eye, it is not easy to obtain or alter. [8]

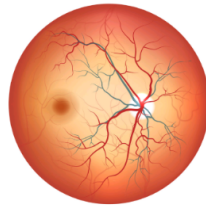


Figure 1.6: Retina recognition.

- **DNA recognition**

DNA stands for deoxyribonucleic acid, which is the nucleic acid that contains the genetic information needed for living organisms to grow, function, and identify individuals. DNA is the one-dimensional code of an individual's personality—except for the fact that identical twins have the same DNA pattern. This is why it is less secure than other traits and more difficult to access. [11]

Behavioral biometrics

- **Gait recognition**

The formal definition of gait refers to human movement, and is based on analyzing the way a person moves (gait) to identify them. Practical gait recognition algorithms incorporate both dynamic and static features (such as body shape) of a moving human body. Gait can be considered a behavioral trait that is influenced by the musculoskeletal structure of the human body. Each individual has a distinctive gait pattern that cannot be easily imitated. Gait can be recorded and analyzed using long-range cameras. [12]

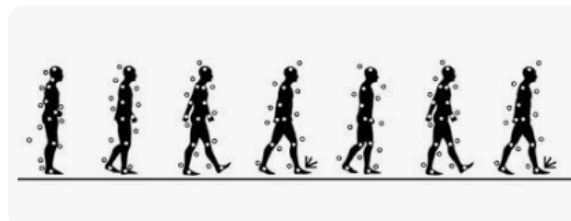


Figure 1.7: Gait recognition.

- **Voice recognition**

Voice recognition is a biometric technology that aims to verify a person's identity by analyzing their voice as they utter a predefined phrase. Voice has unique characteristics such as pitch, frequency, and volume, which depend on the structure of each individual's vocal tract, but the behavioral aspects of speech change over time due to age and medical condition. [11]

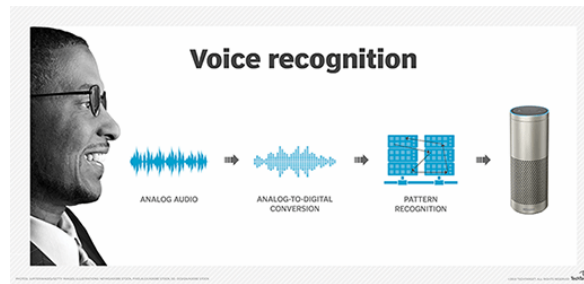


Figure 1.8: Voice recognition.

- **Signature recognition**

In this technique, identity is determined using handwriting signatures. Signature recognition systems analyze two elements: the signature itself (its shape) and the distinctive features of the signing process, such as speed, pen pressure, and directions.

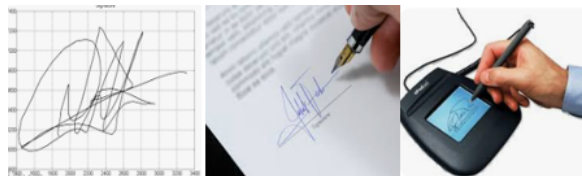


Figure 1.9: Signature recognition.

- **Keystrokes recognition**

The idea behind this technology is to record some characteristics of a person's keyboard usage and then try to determine whether they follow these characteristics. The keyboard usage recognition system measures two main variables: wait time and transition time. This approach is based on the assumption that each person has a unique and distinctive style of typing on the keyboard.

- **Electrocardiogram recognition(ECG)**

Human heartbeats can be used to identify a person. This technique relies on the time and amplitude distance between detected reference points. However, this feature remains difficult to achieve in devices in general.



Figure 1.10: Electrocardiogram recognition.

1.4 Unimodal biometric identification system

A unimodal biometric system relies on using only one biometric trait to verify or identify individuals. It consists of several fundamental components and often encounters issues during the registration process due to the non-universality of biometric traits, forgery, and inaccuracy caused by noisy data, leading to reduced accuracy. [7]

1.4.1 Architecture and Structure

It consists of a series of interrelated steps. Although the nature of the data collected (such as fingerprint, voice, retina, etc.) And the method used may vary, but the basic process remains the same.[13]

Enrolment

Is the process of capturing a user's biometric data for the first time in the form of an image, is collected, processed, and converted into a digital template. This template serves as a reference for future.

Biometric Data

The data presented by the user during registration is called unprocessed image data, which is also referred as raw biometric data . Raw biometric data cannot be used to perform biometric matches so it is used to generate biometric template with the help of feature extraction process.

Feature Extraction

The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction takes place during enrolment and verification, any time a template is created, and is the process of identifying and selecting the unique and important details from a person's biometric data.

Database

A mathematical representation of raw biometric data which is obtained after applying a number of feature extraction algorithms. A template size can vary in size as few bytes to several thousand bytes.The template created at the time of registration is called stored template and at the time of authentication is called live template.

Matching

A process where stored template is matched with live template at the time of verification and we obtained a score, on the basis of this score we conclude that a userreal user or an imposter.

Decision module

The Decision Module is the final step in the biometric system, where the system decides if the person is genuine or not based on the matching score. It compares the similarity score with a predefined threshold. If the score is equal to or higher than the threshold, the system confirms the person's identity. However, if the score is lower, access is denied.

- **Verification refers to 1:1**

Verification is the process of confirming a person's identity by comparing their live biometric data with a template stored in a one-to-one (1:1) matching system. In this process, the user provides their biometric data, which is then compared with the stored template linked to their identity. If the two templates match, access is granted.

- **Identification refers to 1: N**

Identification is the process of identifying a person, where the user provides a single biometric sample, and the system compares it against multiple stored templates across the entire database. When a match is found, the system identifies the person and displays a list of information related to them, such as their name, number, or any stored personal details.

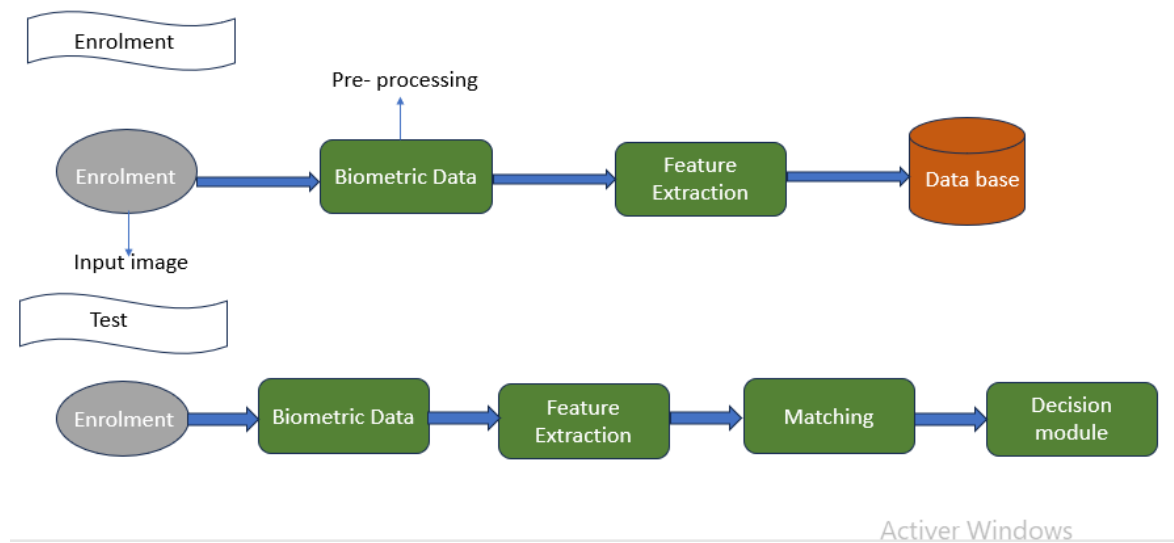


Figure 1.11: Architecture of Unimodal biometric system.

1.4.2 limitation of unimodal biometric identification system

Unimodal biometric identification systems provide a high level of security relatively; however, they suffer from several limitations that affect their accuracy and effectiveness. Some of these challenges include.

Noisy data noise

Noisy data refers to information that becomes distorted or unclear during the biometric registration process. This noise often occurs due to factors such as unclean or poorly maintained sensors, which affects the accuracy of the captured data and weak system performance.

Non-universality

A biometric system should be universal so that all users can provide a biometric attribute for identification. However, not all biometric attributes are universal. There are individuals with disabilities and other factors that hinder this process, which means that these individuals cannot be successfully included in the system's database. [13]

Lack of Individuality

The attributes obtained from a biometric system, such as a facial recognition system that deals with facial images, may be completely similar. A typical example is the case of identical twins or father and son. This results in a high false match rate due to the uniqueness issue. [12]

Susceptibility to circumvention

IS possible to impersonate an individual's trait by an impostor using spoofed traits, such as designing bogus fingers by using fingerprints and using them to wrongfully gain access to a biometric system. Due to these issues of unimodal biometric systems (UBS), the error rates in the systems are quite high, making them unacceptable for introduction in security applications. [8]

1.5 Multimodal biometric identification system

A multimodal biometric system is a type of biometric system that uses more than one biometric attribute to authenticate or recognize identity. It can incorporate various interconnected biometric measurements, such as multiple fingerprint impressions, multiple facial images in a video, multiple representations of a single input, multiple matches of a single pattern, or any combination of these. These systems aim to enhance accuracy and security by combining multiple biometric attributes to overcome the limitations of single-modality systems, such as susceptibility to forgery or changes in biometric traits. By utilizing multiple attributes, the system improves identity authentication and provides a higher level of security for sensitive applications. [13]

1.5.1 Architecture and Structure

The multi-modal biometric system relies on the same fundamental stages used in the single-modal system, Enrolment, Biometric Data, Feature Extraction, Database, Matching, and decision module. However, the key difference in multi-modal systems lies in the fusion of biometric features from multiple sources, where the extracted information is combined at one of the fusion levels, resulting in improved accuracy and higher security compared to single-modal systems.

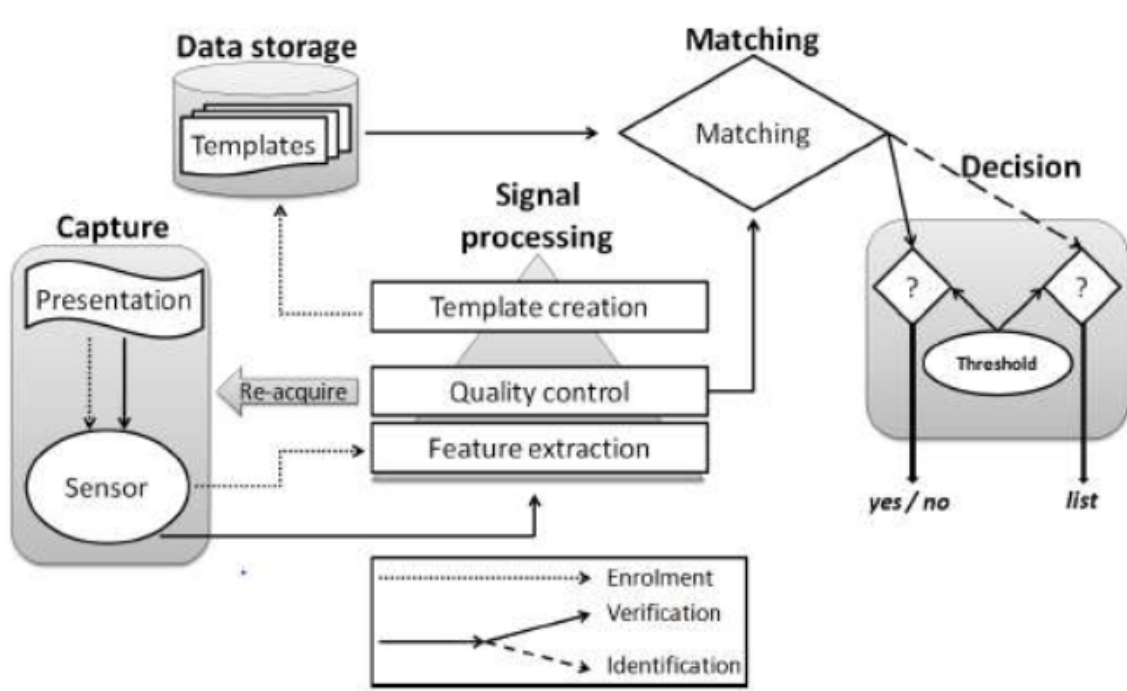


Figure 1.12: Architecture of biometric system.

1.5.2 Levels of Fusion

Multimodal biometric systems rely on integrating information extracted from multiple biometric indicators. The fusion process can be performed at different stages of the system. These levels are as follows:

Sensor level of Fusion

The integration of raw biometric data collected from multiple sensors. The acquired raw data is processed and combined to create new, more informative data, which is then used to extract features. This type of fusion enhances the quality and reliability of the data, leading to improved recognition performance.

Feature level of Fusion

The feature sets extracted from multiple data sources can be fused to create a new feature set to represent the individual. A feature selection/transformation procedure may be adopted to

elicit a minimal feature set from the high-dimensional feature vector.

Match score level of Fusion

Is the process of combining the scores produced by different biometric classifiers. Each classifier generates a score that indicates how similar the input biometric data is to the stored template. These individual scores are merged into a single final score, which represents the overall matching result. The system then compares this score with a predefined threshold to make the final decision.

Rank level of Fusion

This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity (a higher rank indicating a good match). Thus, fusion entails consolidating the multiple ranks associated with an identity and determining a new rank that would aid in establishing the final decision. Techniques may be used to make the final decision. [7]

Decision level of Fusion:

When each matcher outputs its own class label (i.e. accept or reject in a verification system, or the identity of a user in an identification system), a single class label can be obtained by employing techniques such as majority voting, behavior knowledge space ,This type of fusion increases the system's accuracy and reliability by making the final judgment based on multiple biometric traits. [7]

1.6 Performance metrics

These metrics are used to evaluate the accuracy and efficiency of biometric systems. They help assess how effectively the system identifies or verifies individuals based on biometric attributes. Performance metrics play a crucial role in highlighting the system's strengths, identifying its weaknesses, and enhancing overall system performance.

Performance metrics are typically divided into two main categories: Quantitative Metrics and Curve-Based Metrics.

1.6.1 Quantitative Metrics

False Reject Rate (FRR)

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

$$F_{RR}(\%) = \frac{\text{Total False Rejections}}{\text{Total True Attempts}} \quad (1.1)$$

False accept rate (FAR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

$$F_{AR}(\%) = \frac{\text{Total False Acceptance}}{\text{Total False Attempts}} \quad (1.2)$$

Equal Error Rate (EER)

The rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

EER is determined when the following condition is met:

$$\text{EER: } FAR = FRR \quad (1.3)$$

Recognition Rate(ROR)

It is used to measure the percentage of individuals correctly identified by the biometric system during the identification process.

Rank Position Recognition (RPR)

Is a performance metric that measures how likely the system is to find the correct person among the top results during the identification process. It shows how well the system ranks the correct identity among the closest possible matches.

1.6.2 Curve-Based Metrics

Receiver operating characteristic (ROC)

The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines

how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).[6]

Cumulative Match Characteristic (CMC)

A curve that represents the probability of the correct match appearing within the top N ranks of the biometric system's results.

Average Login Identification Cost(ALIC)

is a performance metric used to evaluate the computational cost and efficiency of a biometric system during the identification process. It measures the amount of time and resources required by the system to identify an individual from a database.

1.7 Conclusion

Throughout this chapter, we explored the importance of information security and the role of biometric systems in identity verification and data protection. To ensure accuracy and security, modern systems rely on integrating multiple biometric traits to reduce errors and enhance reliability. Despite the challenges these technologies face, such as technical errors and the possibility of forgery, continuous development contributes to improving their performance and making them more efficient.

Chapter 02

Proposed Biometric Identification System Using Hand Related Traits

2.1 Introduction

Biometric recognition systems are considered more secure and popular.

With the amazing progress in the world of technology and information security in particular, its use has become widespread and in areas where information protection and identification of individuals are required .

an identification system using hand recognition was proposed, which is the most promising feature in the science of information security that depends on the structure and shape of the hand and among the unique elements that make it easy to identify identity are (fingerprints, veins, skin grains, wrinkles, colors, lines, etc.).

These characteristics speed up identification and from the fact that this promising technology is safe to use in various applications and easy to handle for users, for this it is widely popular with individuals and companies, these companies rely on hand recognition technology in access control, Automated Teller Machines and bank transactions to reduce fraud or theft . This technique plays an important role in Personnel Management. In this chapter we will get acquainted with Biometric Identification System Using Hand Related Traits.

2.2 proposed system

The system to be studied is based on the recognition of individuals using the hand attribute on the basic elements: pre-processing, feature extraction, machine.

As these elements are the same elements that make up any biometric system as mentioned above, but the distinctive feature in this study is that it relies on one of the branches of artificial intelligence, which increases the accuracy of recognition and helps to adapt to changes in The Shape of the hand, which occur as a result of aging or environmental factors.

2.2.1 pre-processing

Pre-processing is the first step in biometric identification systems and is important because it enhances the quality of the captured ROI.

Because it relies on various techniques such as noise reduction, contrast enhancement, and interest area (ROI) extraction. This technique helps to smooth out the differences caused by lighting conditions, background noise and hand positioning. By applying pre-treatment methods.

The aim of preprocessing is an improvement of the image data that suppresses unwilling distortions or enhances some image features important for further processing.[14]

By providing a fingerprint, the dorsal surface of the fingers or the inner surface of the hand is revealed, as it depends on the anatomy of the fingers, which involves a complex interaction of the finger bones, the joints between the metacarpal bones and the nearby phalanges for Automatic Identification. We automatically divide this area of interest from the palm of the hand images and enhance them to accommodate lighting, scale and pose Differences resulting from contactless shooting. With a difference in the level of illumination, several steps are taken to process the captured images. It started with the histogram Equalization equation, which in turn improves the contrast of images and highlights more details. Binarization was used to convert images to binary (Binarization) using the Otsu algorithm, and then remove the noise by purifying the anomalous points. Extract hand borders (Contours) to determine the overall shape. Scale Normalization: due to the change of distances during shooting, the scale of images was standardized by calculating the ratio of the distance between fixed landmarks (such as fingertips and wrist midpoints) to a reference distance extracted from the arithmetic mean of several images. In order to extract the area of interest, a standard method is adopted for extracting the finger joint area or specific areas in the palm of the hand, such as skin nodes (Knuckle Lines) or line intersections. These zones were determined using points The center of the palm (calculated geometrically or via the algorithm for determining the center of mass). A 100×100 pixel square is then cut from each target area to be inserted into the training and identification phase.

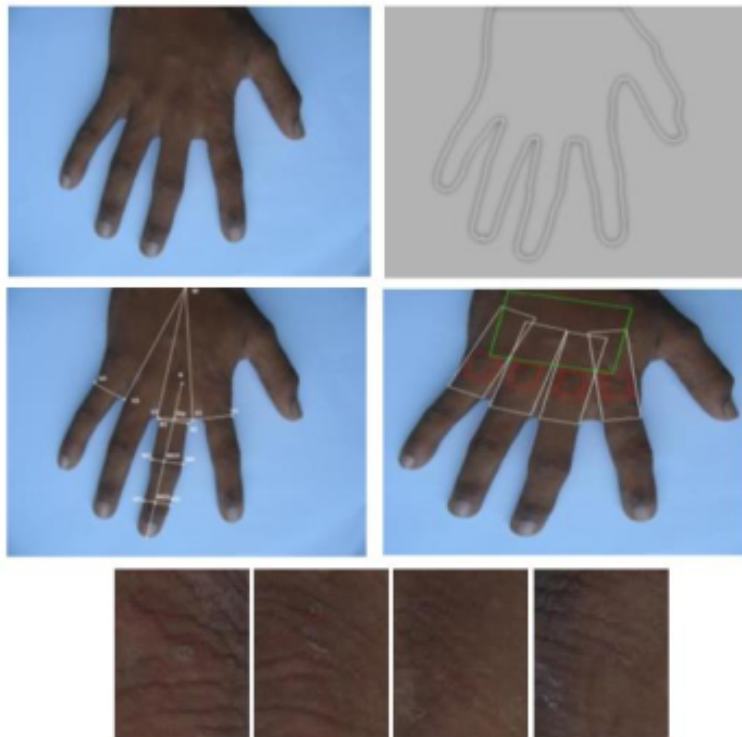


Figure 2.1: Automated segmentation of region of interest (second minor finger knuckle) .

2.2.2 Feature Extraction

The second element of the system, which can be said to be complementary to the first element, in which the features are extracted from the captured image or data provided by pre-processing , but at this stage the features represented by veins, wrinkles and skin grains are extracted.

This process is essential to ensure the accuracy and reliability of the system, as we use advanced techniques to analyze the extracted data and represented both deep learning and transfer learning .

Deep Learning

It is a branch of artificial intelligence based on artificial neural networks for data processing and analysis, where the functions are similar to human, and the latter relies on several layers, where each layer identifies and interprets the information received from the previous one. In the process, Deep Learning models can automatically extract features from raw data without the need for human intervention .[15]

There are several models of deep learning , but the most worthy and optimal in the system of recognizing individuals using the hand trait are CNN.

convolutional neural networks (CNN)

The CNN is one of the most important networks in deep learning and is also a kind of neural feeder that can extract features from data and is designed to process data that comes in the form of multiple matrices such as a gray image (One 2D array) and a Color Image (three 2D arrays). When inserting the image passes through several layerswhich is similar to the way the human visual cortex processes image data. Convolutional layering is done at the level of this layer by applying mathematical folding or wrapping to input elements (neurons of the previous layer or pixels of the input image) using filters or convolution cores to obtain a value from feature maps where each module is associated with local corrections Previously, based on common weights, using one of the nonlinear activation functions such as the corrected linear unit (Rilo), the local weighted sum could be obtained. The next stage is the assembly layer, which consists of a set of Assembly modules, each of which is engaged in calculating the maximum Assembly and the average assembly. In the process, the maximum summation takes the maximum score in the total window , and the average sum determines the average total result.[16] The CNN structure can be described as follows:

- **Convolution layer**

The Convolution layer is the first layer in extracting features from images , it is formed based on mathematical operations and contains two inputs, the image matrix and the filter , or a kernel that maintains the relationship between pixels by learning image features using small unit input data boxes , through this process it is possible to detect

edges, blur or sharpen.

Stride

symbolizes the number of pixels by which the filter moves over the input matrix. When the step value is 1, the filter moves one pixel at a time. If it's stride 2, the filter moves two pixels at a time, and so on.

Zero padding

is the efficient method for padding the boundaries of the input and Provide additional management on the dimensions of production volumes. To calculate the spatial dimensions of the output torsion layers there are two methods that can be used.

Padding with zeros or valid padding, where we preserve the good part of the image, only padding can be used if the filter does not fit the image.

Non-Linearity (ReLU)

The corrected linear module (usually Shortened to Rilo) is intended to extract the activation made by The previous class, which is a nonlinear process, is given by:

$$f(x) = \max(0, x)$$

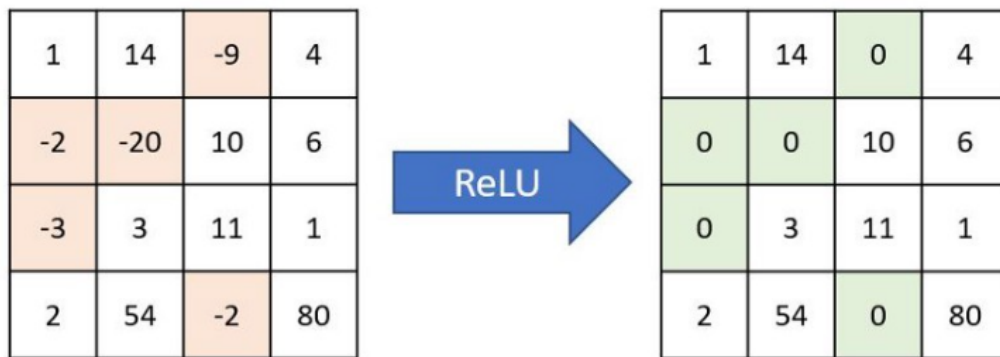


Figure 2.2: ReLU operation .

- **Pooling layer**

The Pooling layer immediately after Convolution layer, where the outputs of the torsion layer are the inputs of the assembly layers the assembly layers work by cutting the dimensions from the feature maps and it is indicated by taking the common or maximum value The pooling layer works on each activation map and reduces the dimensions . O uses a 2×2 core filter with stride 2.

and there are several types of Assembly The most important are the maximum assemblage and also average pooling, L2-norm pooling , spectral pooling , spatial pyramid

pooling , stochastic pooling , and multiscale orderless pooling .

Figure shows the operation of max pooling.

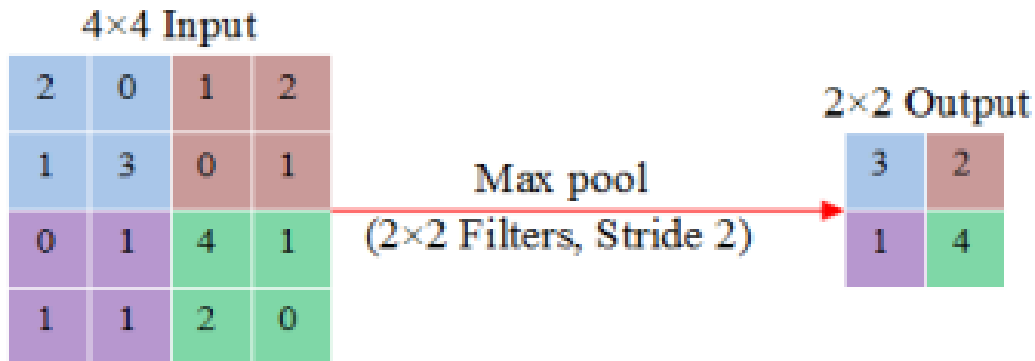


Figure 2.3: Max-Pooling Operation.

- **Fully connected layer**

The latter represents the final layer of CNN fully connected layers or what is known as FC, contains the input layers features (a) and hidden layers(HL) these latter use activation functions and finally we have the output layers that provide the final result of the classification model where we are each cell in a particular layer connected to all cells in the next layer.

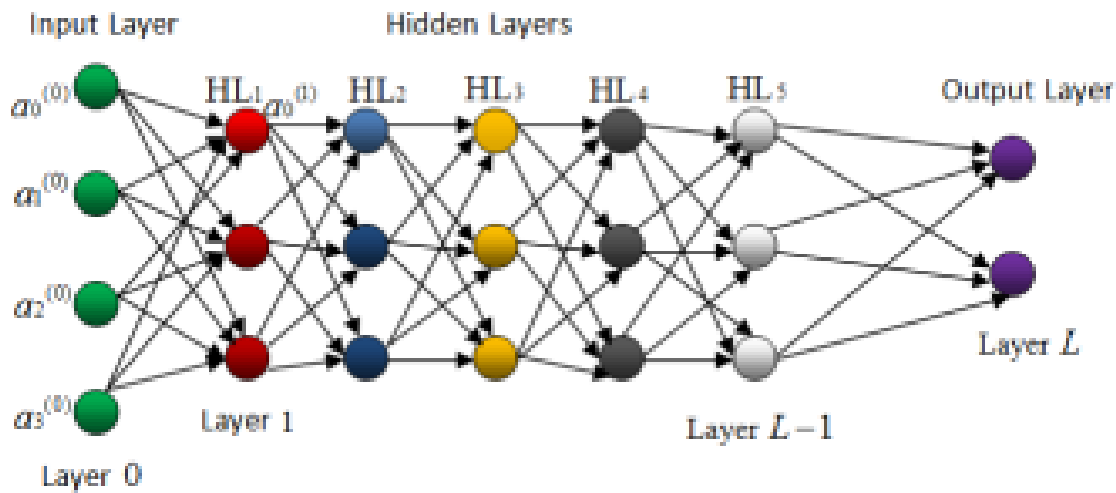


Figure 2.4: Fully-Connected Layers.

Transfer Learning

Transfer learning It is a deep learning technique that uses pre-trained models to solve new tasks without The need to train a model from scratch. These models have already learned useful patterns From large data sets, which allows them to be used in several areas, so that they can be Adapts to new problems with minimal changes. The model can focus on the determinant

The details of the new task while continuing to benefit from her previous knowledge. This The approach saves time, requires less data and improves performance. Transfer learning reduces the computational costs required to build models for new problems. By reusing pre-trained models or pre-trained networks to process a different task, users can reduce the amount of model training time, training data, processor modules and other computational resources.[17]

for example In our system , we will rely on the use of a model to transfer learning, but without having to pox change in it, but in the last classes only this helps us in accuracy due to its distinctive characteristics and also the speed of training because its weights are ready as we can also modify as we want, we will rely on two models namely Visual Geometry Group and AlexNet.

AlexNet

In 2012, Alex kryzhevsky proposed Alexnet AlexNet has achieved the latest technology Accuracy of recognition in the learning and computer vision approach. It was big Breakthrough in the field of machine and computer learning A vision of visual recognition and classification tasks, namely A point in history where interest in deep learning increased Hurry up. [18]

AlexNet architectureis one of the first deep neural networks in deep learning from the field of image classification, and it won the 2012 ImageNet competition. The network receives an input image with a size of $227 \times 227 \times 3$, followed by the first convolution layer (Conv1) containing 96 filters with a size of 11×11 with Step 4, and then an assembly layer (Max Pooling) with a size of 3×3 with Step 2. Then comes the Conv2 layer containing 256 filters with a size of 5×5 , an assembly layer has also been made. After that, the data passes through three additional convolution layers (Conv3, Conv4, Conv5)with different filters . The data is then flattened (flattened), and then passed through two FC layers containing 4096 units each. Finally, the data passes through an output layerfc containing 1000 units, representing the number of varieties in the ImageNet dataset, and then the Softmax function is applied to produce classification probabilities.

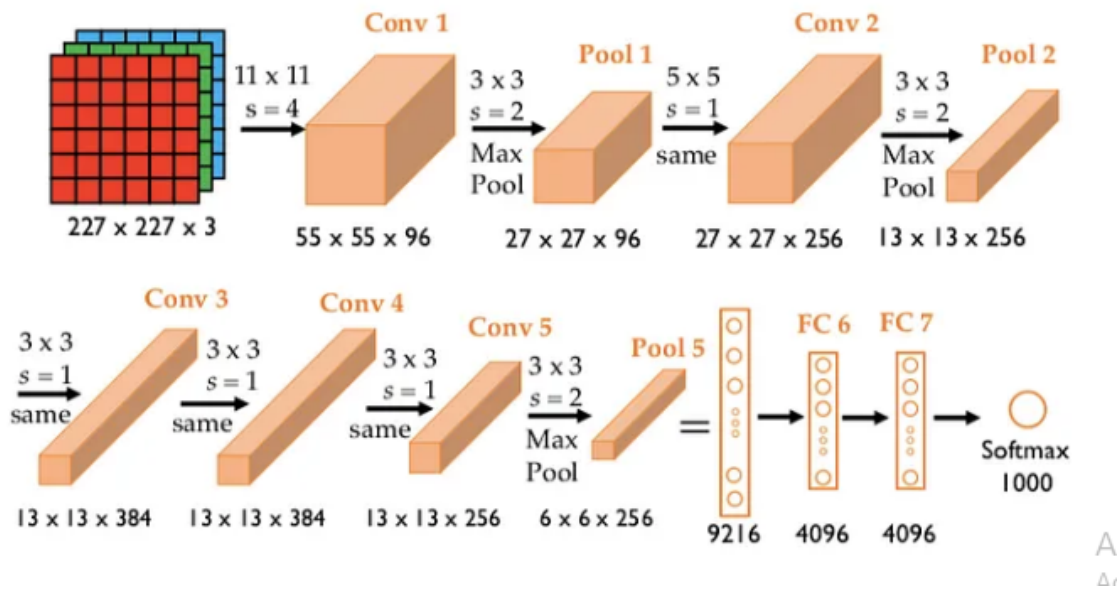


Figure 2.5: Architecture AlexNet.

Visual Geometry Group

The Visual Geometry Group (VGG) refers to the CNN model developed by research A collection at the University of Oxford by K. Simonyan and A. Zisserman. It is one of the most well-known structures in Computer vision, recognized for its deep structure that uses sequential convolution layers with small filters 3×3 . This design allows for efficient feature extraction, achieving an accuracy of 92.7 percent, Which makes VGG extremely effective for image classification and task recognition. The model was Widely used in various applications, Where its structure is from an input image of size $224 \times 224 \times 3$. After that, this image is transmitted by several layers convolution + ReLU, and the visual features are extracted through small filters of 3×3 size. After each set of wrapping layers, Max Pooling layers are used to reduce spatial dimensions while preserving important attributes. The number of channels increases from 64 to 512 and the image dimensions are gradually reduced. After the extraction layers are completed, the data is converted into a vector via Flatten, and then passes through two Fully Connected layers of 4096 modules, which combine attributes to determine the final category. Finally, we use the Softmax layer to generate classification probabilities . There are two main versions of VGG: VGG 16 and VGG 19.

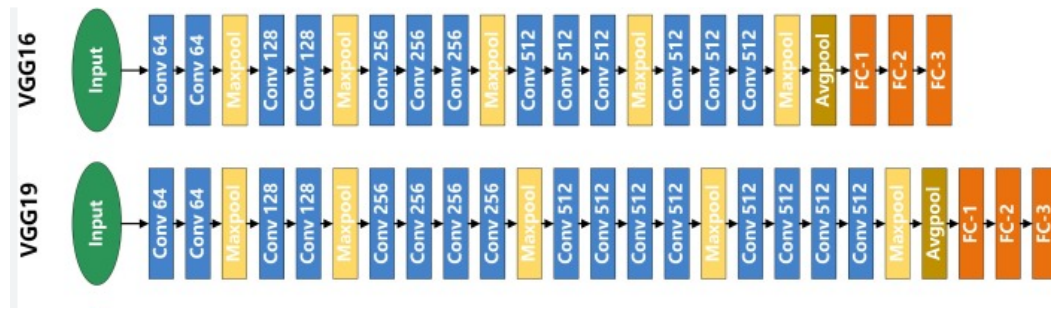


Figure 2.6: VGG 16 and VGG 19 Layers details.

- **VGG16** is a CNN designed for image processing and pattern recognition. It consists of 16 layers, including convolutional, pooling, and fully connected layers. The model uses small 3×3 filters, allowing it to gradually analyze fine details in images. VGG16 follows a simple yet effective approach, making it widely used in tasks like image classification, object detection, and hand recognition. However, despite its high accuracy, it requires significant computational power due to its large number of parameters, making it less efficient than newer models in terms of speed and resource consumption.

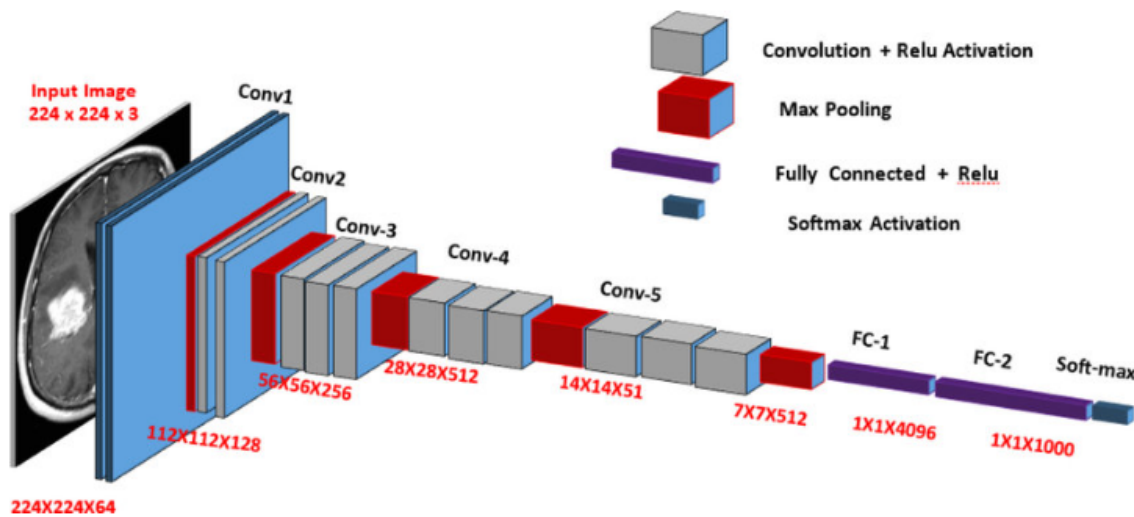


Figure 2.7: VGG-16 CNN model architecture.

• VGG19

is a convolutional neural network (CNN) model developed by the Visual Geometry Group, consisting of 19 layers. Unlike VGG16, which has 16 layers, VGG19 includes additional convolutional layers, making it more complex and capable of capturing more detailed patterns in images. It uses small 3×3 filters across all its convolutional layers, which helps in extracting fine-grained features from images. While VGG19 demonstrates improved accuracy in tasks like image classification and object detection, its increased depth requires more computational resources, making it less efficient in terms of speed and resource consumption compared to simpler models.

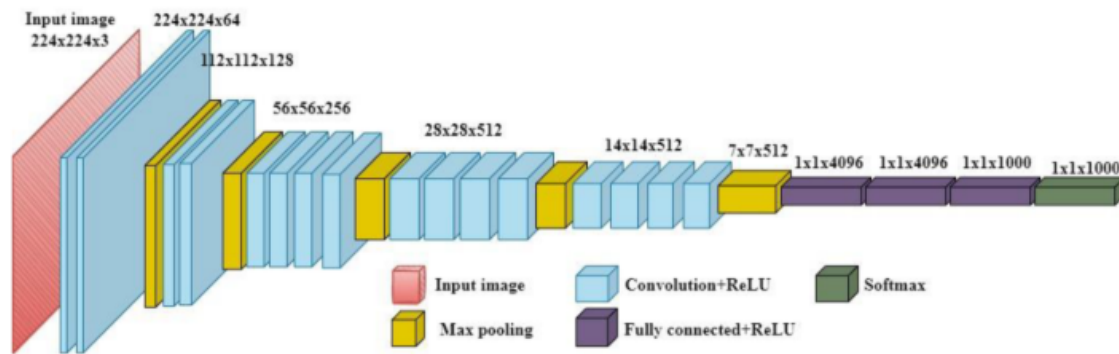


Figure 2.8: VGG-19 Model.

2.2.3 Tied Rank Normalization techniques

This approach is frequently utilized in predictive modeling and statistical analysis, where values within a dataset are reordered and ranked based on their original sequence. It plays a crucial role in ensuring a more balanced and structured data distribution.[19]

This technique is often applied in predictive models and statistical analysis, especially in biometric data, to maintain consistency and ensure a fair distribution of values. Linked order is used when the data contains duplicate values. In other words, The Associated ordering is applied to handle repeated values in the data set. And when there is a correlation between the data, significant changes in values and variability may occur, which makes it difficult to accurately understand the data. Ultimately, this method is aimed at improving the accuracy and reliability of data analysis and interpretation.

2.3 Machine Learning (support vector machines)

Machine learning is a branch of artificial intelligence used in identification systems using the hand attribute by analyzing unique patterns where computers can learn from the data and enable identification based on this, this technique relies on training the model and classifying new data to contribute to the assistance of identification systems. One of the most important or widely used technologies are support vector machines SVM are one of the most powerful algorithms used in classification and regression, as they rely on finding the best separation limit (Hyperplane) separating different categories by the widest possible margin, which makes them effective with high-dimensional data. When the data is not linearly separable, kernel functions such as Radial Basis Function(RBF) kernel or polynomial are used to transform the data to a higher dimension so that it becomes separable. SVM is characterized by its ability to deliver strong performance with small and medium datasets, it is also resistant to overadaptation, but it may suffer from slowness when dealing with huge datasets or when there is significant noise. They are used in multiple applications such as text classification, image recognition and financial forecasting, which makes them a powerful tool in data analysis and decision-making based on detected patterns.

2.4 Conclusion

In conclusion, the proposed biometric identification system using the dorsal hand demonstrates significant advantages, particularly in its ability to leverage advanced learning techniques such as Machine Learning, Transfer Learning, and Deep Learning. By integrating these approaches, the system enhances feature extraction and classification accuracy, ensuring reliable biometric recognition. Additionally, the feature matching process is reinforced by robust normalization techniques.

Chapter 03

Experimental Results and Discussion

3.1 Introduction

We have discussed in previous chapters that the identification system is based on four stages of pre-processing, feature extraction (deep learning, transfer learning), matching (SVM) and the decision stage. The majority of physiological patterns used in identification are associated with biometric data.

Hand images of volunteers from 500 cases of right-handedness were used inside an indoor or outdoor environment through non-contact hand imaging to determine uniquely and automatically recognizable performance using the surface of the finger or palm (metacarpal bones of the hand and proximal phalanges) we used all images to divide 100×100 pixel ROI corresponds to the main and second finger joint area as we indicated in the next chapter

In this chapter we will discuss the experimental results of evaluating the biometric identification system using images from the hand based on the best methods.

3.2 Why hand dorsal modality ?

With the rapid development, relying on biometric identification systems has become extremely important in several areas where security must be carried out with high accuracy, such as banks, and with the variety of biometric features present such as fingerprint, iris, and face recognition, the back of the hand has emerged as a feature that achieves accuracy and ease of use after the back surface of the hand. One of the most proven and distinctive parts of the hand in the identity verification process. This is due to a set of fundamental factors that make this part of the hand very convenient to rely on in modern biometric systems, as it combines the constancy of attributes, the richness of biometric details.

- **Lack of exposure to change**

The appearance of the hand is a trait that is less likely to change over time. It is aged and more easy to shoot in different environmental conditions.

- **Rich in biometric features**

It contains characteristic details such as Knuckles, veins, finger shape, features that are difficult to imitate. These details are unique to each person and can be easily extracted using advanced imaging techniques as it consists of 13 ROI.

- **Comfort and lack of contact**

Photos of the back surface of the hand can be taken in a non-contact (contactless) way, and this is generally welcomed by users

- **Suitable for open and closed systems**

The back hand surface can be effectively used in open and closed identification systems, as it can be relied on for verification and identification even in large groups of people .

- **Ease of processing and analysis**

Photos taken of the back surface of the hand are often less complicated in terms of wrinkles or fine lines, which facilitates pre-processing and feature extraction.

3.3 Data base description

A database consisting of hand-made photos of male and female volunteers was obtained on the campus of the Hong Kong Polytechnic University and in some villages in India, where this data consists of 5010 photos of 500 people, so that each individual submits 5 PHOTOS, These photos are represented on the four fingers, middle and ring fingers . The area of interest is examined for each finger, represented by 3 finger joint patterns formed on the dorsal finger surface,

knuckle patterns formed on finger dorsal surface joining middle phalanx and proximal phalanx bones (PIP joints),

knuckle patterns formed between distal and middle phalanx bones (DIP joints)

knuckle patterns formed between metacarpal and the proximal phalanx bones (MCP joints)

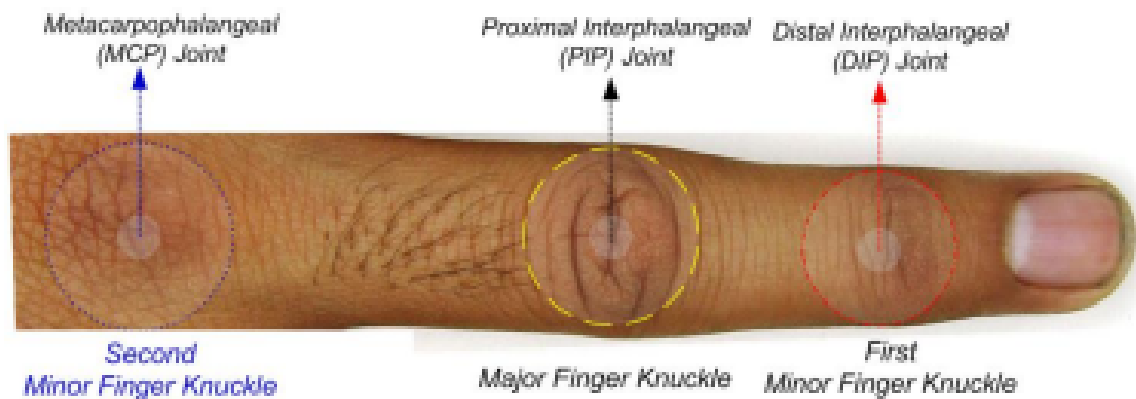


Figure 3.1: Sample finger dorsal image .

The study is based on the evaluation of these data in the training set and another test so that 3 training images and 2 test images for each of the selected areas on the hand , which generated 13 ROI per image Petals on each of the four fingers and the Dorsal Center These images were obtained by the method of non-contact photography and were in the form of JPG.

Another database was also obtained, which is also for the back of the hand, but obtained over a long period of 2 to 7 years, which provides an important basis for conducting in-depth

studies on the stability of hand Joint patterns over time, and makes it possible to assess how resistant the system is to the formation of changes caused by factors such as aging or various environmental conditions.

3.4 Assessment protocol

After completing the collection of the dorsal fingerprints of the participants, which were 500 individuals, we organized the data, separated and classified them in such a way as to ensure their distribution into groups independent of other databases. This division was made based on the characteristics of different individuals and categories, so that each category is grouped into a specific subset that includes only the Associated dorsal imprints.

After the classification, we selected two main groups: one for training, the other for testing. We have made sure that these collections are varied and well-weighted in terms of the number of images and categories, in order to ensure accurate and effective performance when building recognition models.

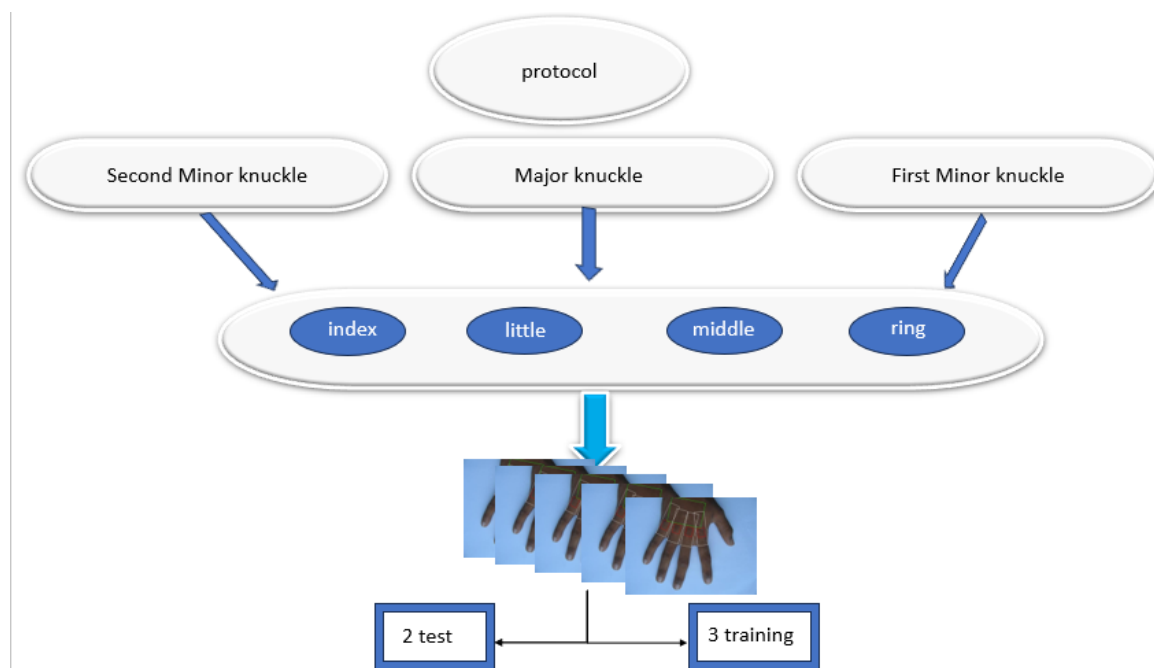


Figure 3.2: Assessment protocol.

3.5 Work environment

In this section, we present the hardware and software environments of our work.

Hardware environment

We will rely on a set of equipment to investigate the project that has been provided to us a **computer HP ProDesK 600 G3 SFF** and from the specifications of the device :

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

Software environment

With the development of software science and the emergence of deep learning that pushes companies to develop scientific programming languages, MathWorks has developed its Matlab products and the software environment we use is:

- The software tool that we used in our system is: **Matlab R2024a**.
- The operating system used in our system is: **Windows 10**.

3.6 Experimental results and discussion

The next section will put the Unimodal and Multimodal systems to the test and to do this we have trained the transfer learning architectures AlexNet, Vgg16, Vgg19 models based on the data that we have the following calibrated extractors to compare and verify:

In open set identification:

- Equal Error Rate (EER).
- T0 (threshold).

In closed set identification:

- Recognition Rate (ROR).
- Rank Perfect Recognition (RPR).

3.7 Unimodal system test result

Our aim of this procedure is to evaluate the performance of a unimodal biometric identification system using Segmented hand attributes(single attribute) that are evaluated separately using

feature extraction methods based on deep learning. The assessment includes open and closed set models, where the Open is lower than EER and the closed is higher than RPR using the previous models The protocol .

We have hired three pre-trained CNN architectures AlexNet, vgg 16, and vgg 19-to extract features from the selected ROI. Where we were able to identify any trait that can be considered excellent in identification, based on two methods, the first without tied rank normalization and the other with tied rank normalization.

The test results for each technique were written down and the best performance was shaded in yellow.

3.7.1 Experimental Results with AlexNet

Performance Based AlexNet without Tied Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		2.6999	0.8160	89.7	264
first	index	4.8525	0.7570	77.7	319
	middle	3.6102	0.7620	84.3	497
	ring	3.0220	0.7660	88.1	458
	little	3.3087	0.7570	84.8	388
second	index	3.1954	0.8410	87.7	438
	middle	2.1634	0.8240	91.3	354
	ring	2.5958	0.8120	88.9	271
	little	1.9926	0.8210	89.7	450
major	index	2.3914	0.8100	89.8	384
	middle	1.9926	0.7580	94.0	470
	ring	1.8008	0.7490	94.8	392
	little	1.4995	0.7800	93.5	205

Table 3.1: unimodal system Performance Based AlexNet Without Tied Rank Normalization

Discussion

After analyzing **Table 3.1**, we note that the **major knuckle** achieved the best performance with all fingers(index,middle,ring and little) and this is if the system was operating in the open-set selection mode and **alexnet without Tied Rank Normalization** , where it achieved the best performance at **major knuckle-based little** with a value of **ERR=1.4995** at the threshold of **T0=0.7800**. Followed by major knuckle-based ring , followed by major knuckle-based middle and major knuckle-based index.

can be considered A relatively acceptable performance of second knuckle(middle,ring, little)and DC, but the worst performance was at first knuckle for all fingers(index,middle,ring and little) where the highest value was at the **first knuckle-based index** with a value of **ERR=4.8525** at the threshold of **T0=0.7570**. We have drawn a comparison of the performance of everyone to put the definition of an open set in Figure 3.3.

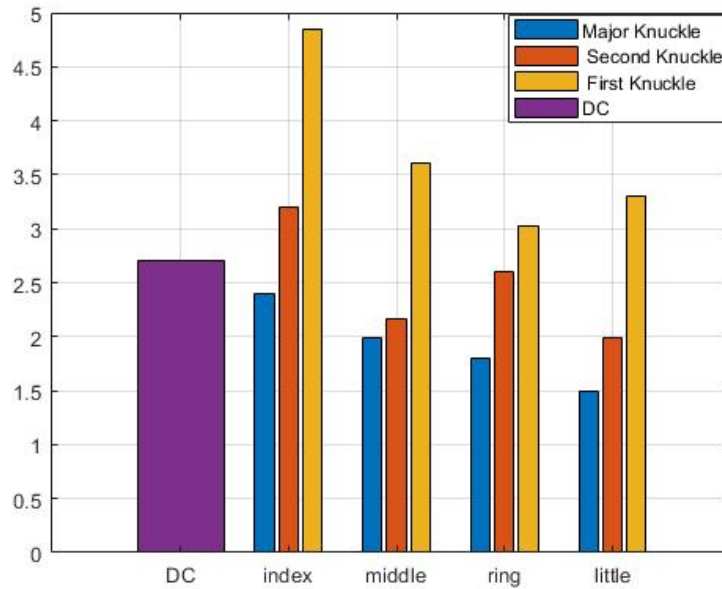


Figure 3.3: unimodal system performance Based Alexnet without Tied Rank Normalization(open-set).

According to the results of the closed -set, we note that **major knuckle-based ring** achieves the best result with **ROR=94.8** and **RPR=392** , and always the major knuckle achieve the best performance, second knuckle and DC average performance at **ROR=89.7** and **RPR=264**, The worst identification was at first knuckle-based index In proportion **ROR=77.7** and **RPR=319**. Figure 3.4 illustrate the closed-set identification based proposed system performances.

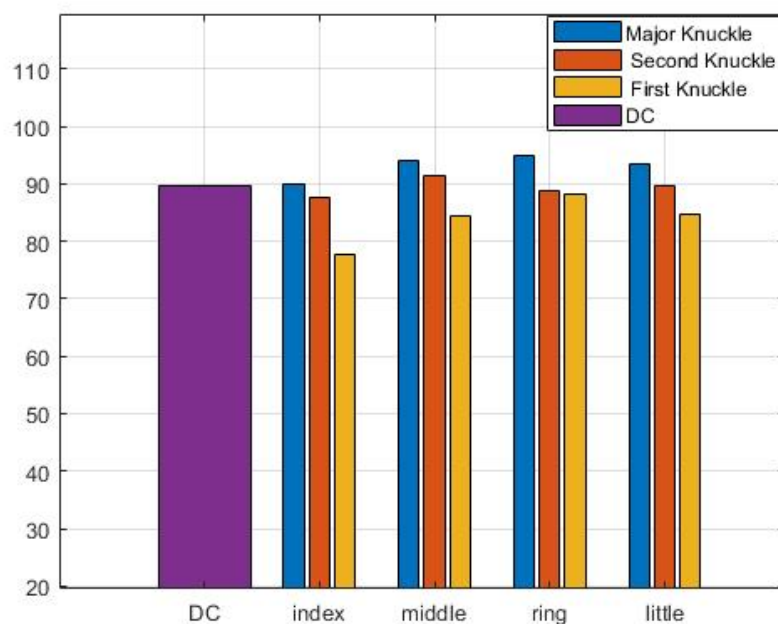


Figure 3.4: unimodal system performance Based AlexNet without Tied Rank Normalization (closed-set).

Performance Based AlexNet With Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		1.4022	0.6740	91.0	225
first	index	4.8086	0.6830	77.6	256
	middle	3.2925	0.6950	84.7	414
	ring	2.9053	0.6950	89.0	429
	little	3.2999	0.6970	83.7	370
second	index	2.6070	0.7330	87.9	424
	middle	1.5992	0.7100	92.8	311
	ring	2.1972	0.7320	89.7	265
	little	1.7703	0.7190	90.7	448
major	index	1.9996	0.7190	90.1	475
	middle	1.4014	0.6480	94.8	406
	ring	1.1041	0.6610	94.9	333
	little	1.5031	0.6950	92.9	188

Table 3.2: unimodal system Performance Based AlexNet with Tied Rank Normalization

Discussion

Through table 3.2, we noted the concentration of the highest and most favorable ratios in terms of efficiency in the open-set or closed-set state of the system, respectively, they are **EER=1.4014** and **ROR=94.9**, represented at **major knuckle-midelle** and **major knuckle-ring**, followed by performance **DC**, **second knuckle** and the last is always the worst known at **first knuckle-index** by **ERR=4.8086** and the threshold of **T0=0.6830**, **ROR=77.6** and **RPR=256**.

We have drawn a comparison of the performance of everyone to put the definition of an open set and closed-set in Figure 3.5 and 3.6.

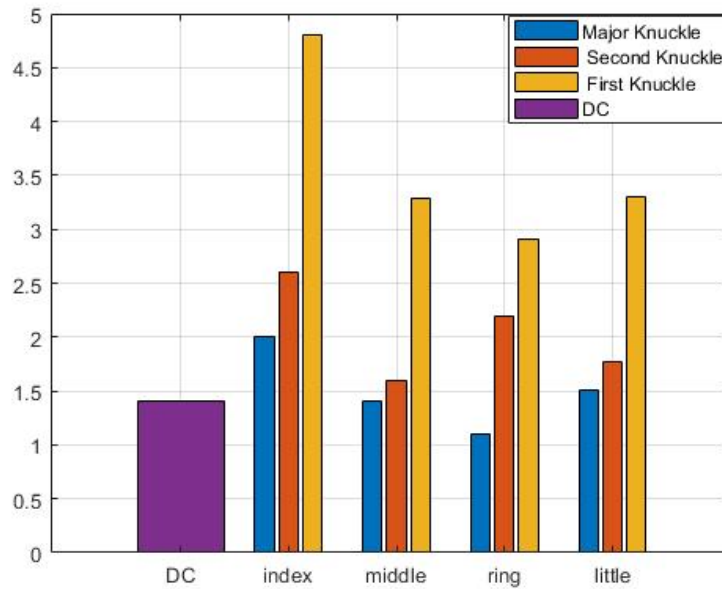


Figure 3.5: unimodal system performance Based Alexnet with Tied Rank Normalization(open-set).

We noticed a significant improvement in the values of **EER**, **T0**, **ROR** or even **RPR**, where at **major knuckle-midelle**, which was in the open -set **EER=1.99926** and the threshold of **T0= 0.7580** and now it has become **EER=1.4014** and the threshold was estimated at **T0= 0.6480**, but in the closed-set it was **ROR=94.0 470**, or after using Tied Rank Normalization it became **ROR=94.9**, **RPR=333** with a very slight relative decline in the ratios of **major knuckle-little**. Thus, we can say Tied Rank Normalization improved performance when used in AlexNet.

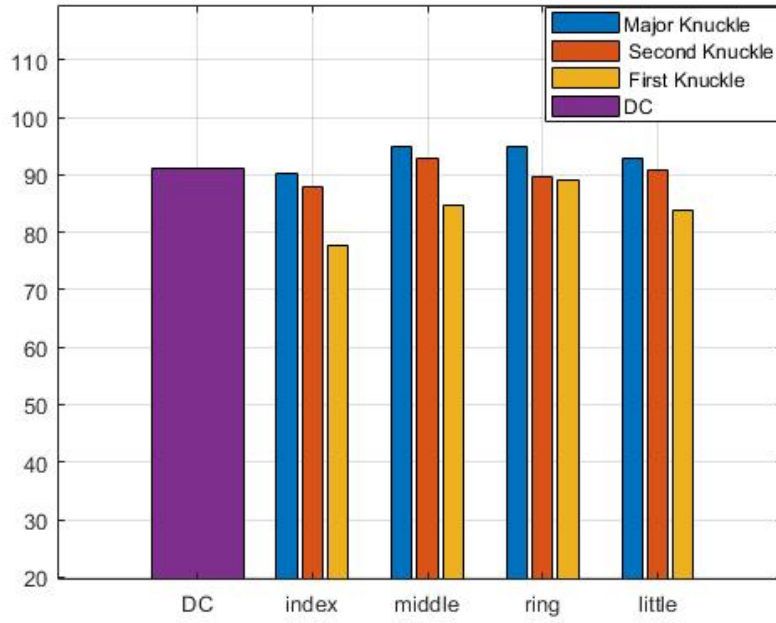


Figure 3.6: unimodal system performance Based Alexnet with Tied Rank Normalization (closed-set).

3.7.2 Experimental Results with VGG 16

Performance Based VGG 16 Without Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		1.3952	0.7860	90.0	247
first	index	6.2357	0.7600	67.3	431
	middle	5.0873	0.7290	75.2	444
	ring	5.2433	0.7190	77.1	475
	little	5.4720	0.7340	72.6	485
second	index	3.4255	0.7490	80.2	324
	middle	2.9031	0.7720	84.8	296
	ring	3.0897	0.7490	82.6	329
	little	2.2746	0.7450	86.0	311
major	index	3.5324	0.7880	85.7	408
	middle	2.4931	0.7820	90.0	497
	ring	2.8736	0.7860	90.0	348
	little	2.7219	0.7640	85.7	227

Table 3.3: unimodal system Performance Based VGG 16 without Tied Rank Normalization

Discussion

After analyzing **table 3.3**, We note that the best known disease was at DC with a line rate of **EER=1.3952** and at a threshold estimated at **T0=0.7860**, followed by second knuckle-little with **EER=2.2746** and a threshold of **T0=0.7450**, the finger performance at second knuckle and major knuckle can be considered relatively acceptable . He scored first knuckle on all fingers without purchase, and in our case this is **the open set test, and Vgg 16 without third Rank** and scored the worst performance in identification in first knuckle -index with **EER=4.8525** and a threshold of **T0=0.8160** We have drawn a comparison of the performance of everyone to put the definition of an open set in Figure 3.7.

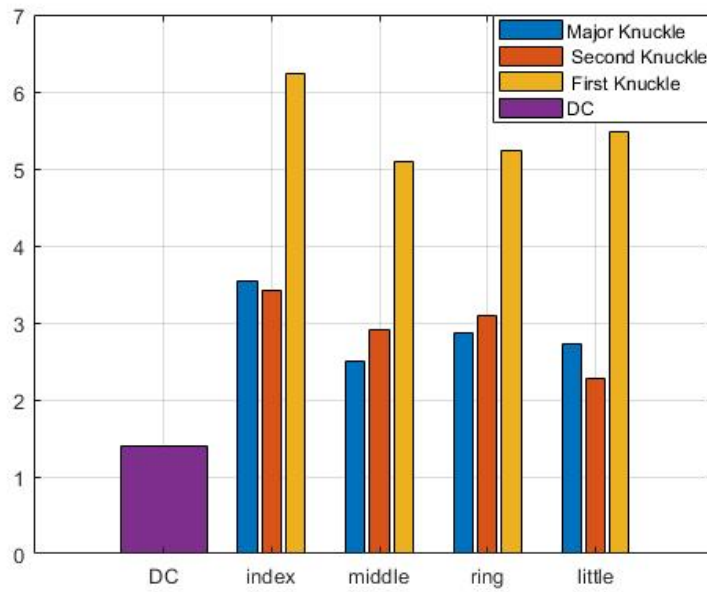


Figure 3.7: unimodal system performance Based vgg 16 without Tied Rank Normalization (open-set).

According to the **results of the closed -set** , we performance that **DC** are issued with the best known **ROR=90,RPR=247**, but **major knuckle(middle and ring)** share the same value as the custom**ROR**, but with a difference in the percentage of **RPR**, which are respectively **497** and **348**, we can say that the ratios of second knuckle and major knuckle(little and index)are acceptable or well defined, but for **first knuckle**, the worst was always at an average Figure 3.8 illustrate the closed-set identification based proposed system performances.

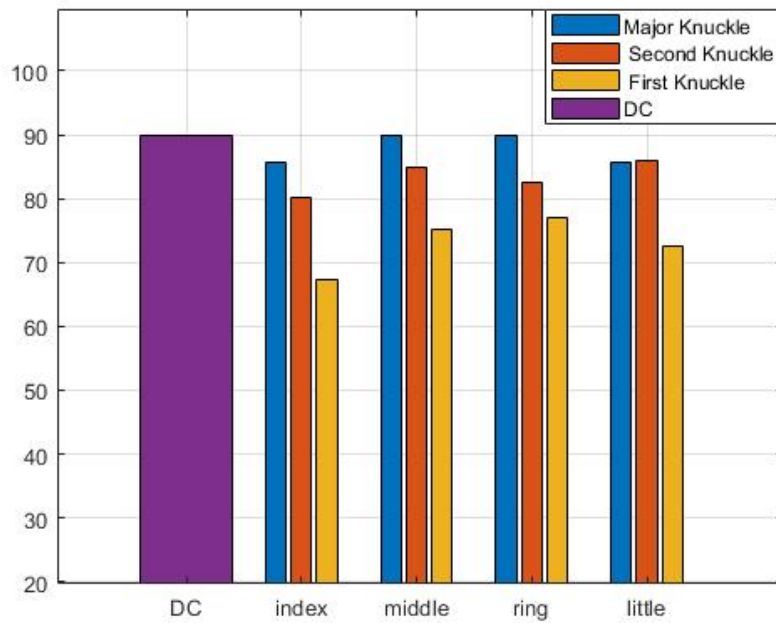


Figure 3.8: unimodal system performance Based vgg 16 without Tied Rank Normalization (closed-set).

Performance Based VGG 16 With Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		1.3021	0.7070	90.8	247
first	index	5.3942	0.7060	68.2	402
	middle	4.3199	0.6900	74.4	422
	ring	4.8662	0.6600	76.5	423
	little	4.9818	0.6900	73.5	472
second	index	3.4076	0.6920	81.8	366
	middle	2.5770	0.7050	85.2	257
	ring	2.5063	0.6940	83.6	303
	little	2.1974	0.6860	86.2	319
major	index	3.1077	0.7160	86.0	408
	middle	2.1007	0.7110	90.7	493
	ring	2.4975	0.6900	91.3	264
	little	2.3081	0.7190	87.3	254

Table 3.4: unimodal system Performance Based VGG 16 with Tied Rank Normalization

Discussion

Through **table 3.4**, we noted the concentration of the highest and most favorable ratios in terms of efficiency in the open-set or closed-set state of the system, respectively, they are **EER=1.3021** and **ROR=94.9**, represented at **DC and major knuckle-ring**, followed by performance **major-middle**, **second knuckle** and the last is always the worst known at **first knuckle-index** by **ERR=4.80865.3942** and the threshold of **T0=0.6900**, **ROR=74.4** and **RPR=422**. We have drawn a comparison of the performance of everyone to put the definition of an open set and closed-set in Figure 3.9 and 3.10.

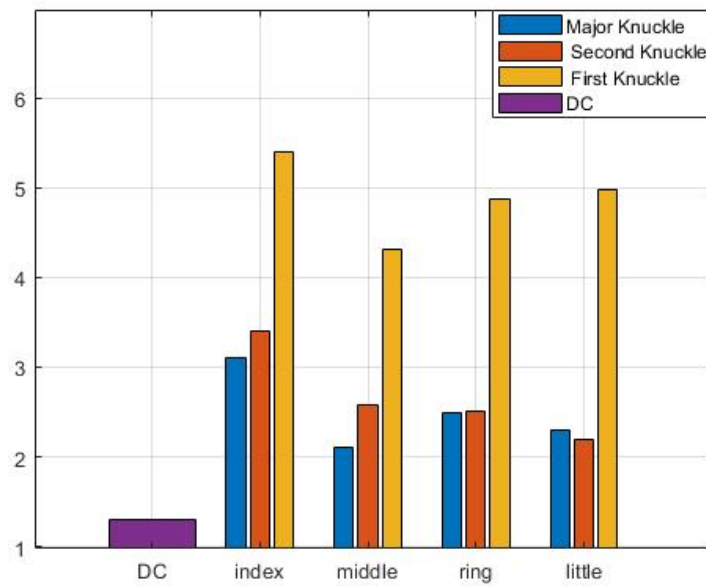


Figure 3.9: unimodal system performance Based vgg 16 with Tied Rank Normalization (open-set).

We noticed a significant improvement in the values of **EER**, **T0**, **ROR** or even **RPR**, where at **DC**, which was in the open -set **EER=1.3952** and the threshold of **T0= 0.7860** and now it has become **EER=1.3021** and the threshold was estimated at **T0= 0.7070**, but in the closed-set **major knuckle-ring** it was **ROR=90**, or after using Tied Rank Normalization clit became **ROR=91.3**, Thus, we can say Tied Rank Normalization improved performance when used in Vgg16 .

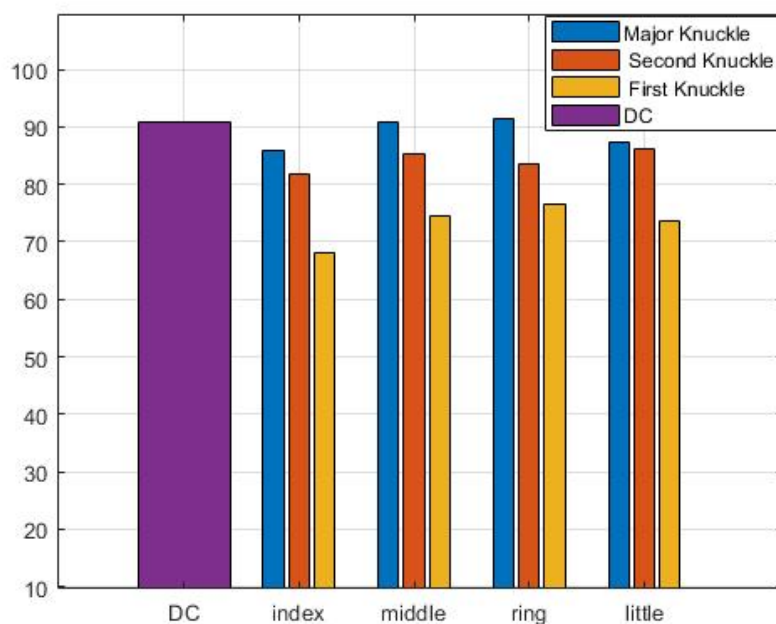


Figure 3.10: unimodal system performance Based vgg 16 without Tied Rank Normalization (closed-set).

3.7.3 Experimental Results with VGG 19

Performance Based VGG 19 Without Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		1.5300	0.7810	90.7	485
first	index	5.9822	0.7440	68.2	416
	middle	5.2861	0.7150	77.4	469
	ring	3.9406	0.7300	78.5	473
	little	5.1858	0.7330	74.4	424
second	index	3.3217	0.7830	81.0	337
	middle	3.6058	0.7520	85.2	417
	ring	2.8971	0.7390	83.2	290
	little	2.9327	0.7410	86.5	250
major	index	2.7998	0.7680	86.5	436
	middle	2.7057	0.7730	91.5	499
	ring	2.1049	0.7510	90.9	289
	little	2.3974	0.7700	88.1	270

Table 3.5: unimodel system Performance Based VGG 19 without Tied Rank Normalization

Discussion

After analyzing **Table 3.5**, we note that the **DC** and this if the system was operating in the open-set selection mode and **VGG 19 without Tied Rank Normalization**, where it achieved the best performance at with a value of **ERR=1.5300** at the threshold of **T0=0.7810**. can be considered A relatively acceptable performance of second knuckle and major knuckle(middle,ring, little and index), but the worst performance was at first knuckle for all fingers where the highest value was at the **first knuckle-based index** with a value of **ERR=5.9822** at the threshold of **T0=0.7440**. We have drawn a comparison of the performance of everyone to put the definition of an open set in Figure 3.11.

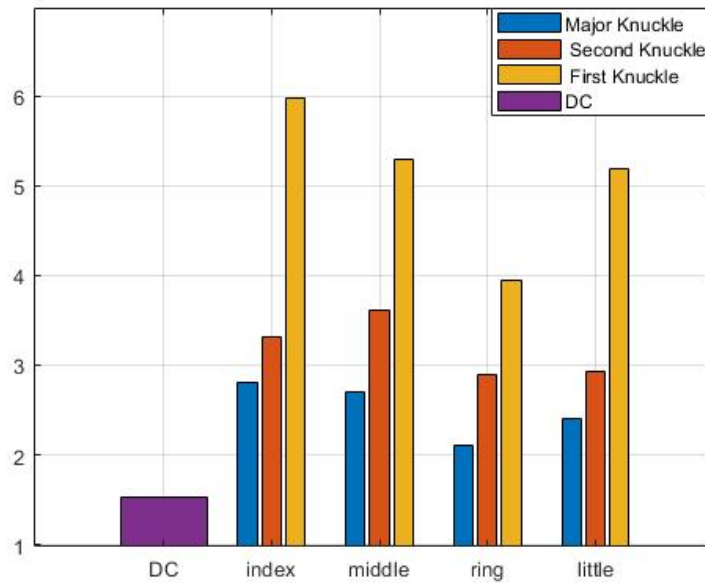


Figure 3.11: unimodal system performance Based vgg 19 without Tied Rank Normalization (open-set).

According to the results of the closed -set, we note that **major knuckle-based middle** achieves the best result with **ROR=91.5** and **RPR=499**, and always the major knuckle achieve the best performance, second knuckle and DC average performance at **ROR=90.7** and **RPR=485**, The worst identification was at first knuckle-based index In proportion **ROR=68.2** and **RPR=416**. Figure 3.12 illustrate the closed-set identification based proposed system performances.

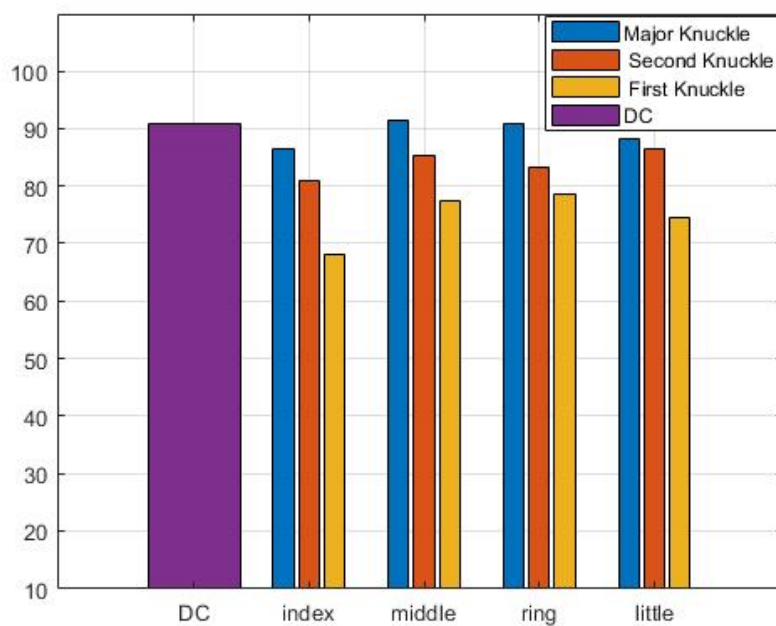


Figure 3.12: unimodal system performance of the Baseline vgg 19 without Tied Rank Normalization (closed-set.)

Performance Based VGG 19 With Rank Normalization

		open-set		closed-set	
		EER	T0	ROR	RPR
DC		1.4078	0.7180	90.7	488
first	index	5.4837	0.7030	69.3	431
	middle	4.4999	0.6600	78.6	430
	ring	3.9023	0.6860	80.2	464
	little	4.7079	0.6960	75.4	430
second	index	2.8885	0.7240	81.8	314
	middle	3.0078	0.6940	85.4	384
	ring	2.7344	0.6780	84.2	248
	little	2.7055	0.6710	86.7	222
major	index	2.9091	0.7070	86.9	411
	middle	2.5081	0.6950	91.2	499
	ring	1.7932	0.6950	91.4	278
	little	1.9201	0.7180	88.2	238

Table 3.6: unimodal system Performance Based VGG 19 with Tied Rank Normalization

Discussion

Through table 3.6, we noted the concentration of the highest and most favorable ratios in terms of efficiency in the open-set or closed-set state of the system, respectively, they are **EER=1.4078** and **ROR=91.4**, represented at **DC and major knuckle-ring**, followed by performance **major knuckle, second knuckle** and the last is always the worst known at **first knuckle-index** by **ERR=5.4837** and the threshold of **T0=0.71800**, **ROR=69.3** and **RPR=431**. We have drawn a comparison of the performance of everyone to put the definition of an open set and closed-set in Figure 3.13 and 3.14.

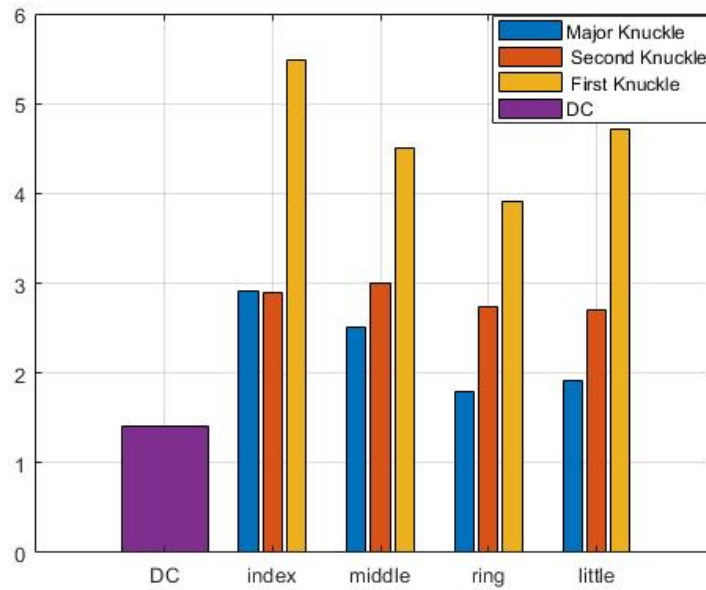


Figure 3.13: unimodal system performance Based vgg 19 with Tied Rank Normalization (open-set).

We noticed a significant improvement in the values of **EER**, **T0**, **ROR** or even **RPR**, where at **DC**, which was in the open -set **DCEER=1.5300** and the threshold of **T0= 0.7810** and now it has become **EER=1.4078** and the threshold was estimated at **T0= 0.7180**, but in the closed-set **major knuckle-ring** it was **ROR=90.9**, or after using Tied Rank Normalization it became **ROR=91.4**, Thus, we can say Tied Rank Normalization improved performance when used in Vgg 19.

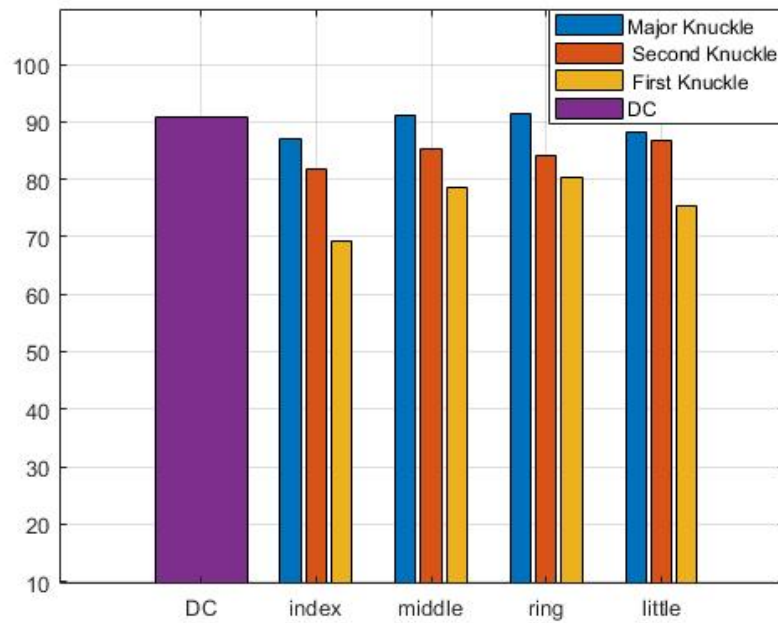


Figure 3.14: unimodal system performance Based vgg 19 without Tied Rank Normalization (closed-set).

Comparison of the results of the alexnet, vgg 16 and Vgg 19 unimodal without Tied Rank Normalization

- The AlexNet network demonstrated significantly faster inference times compared to VGG 16 and VGG 19.

And this is due to the synthetic structure of the alexnet, which is simpler and lighter, as it contains fewer layers and fewer filters compared to Vggs and thus achieves an amazing computational speed.

VGG networks rely on long chains of small (3x3) Convolution layers, which increases the calculations per image compared to AlexNet which has larger but fewer layers.

- AlexNet excelled especially in the major joints such as major-ring and major-middle, where the ROR rates reached about 94.8, while the highest ROR ratios in VGG16 and VGG19 ranged around 90 - 91.5 only.
- Although the ROR values are similar, there is a clear difference in RPR values between the hand areas:

The RPR value expresses the order in which the correct identity is located during the recognition process.

The areas of the hand that seemed equal in the overall success rate (ROR), differed in the speed of reaching the correct identity across the ranks.

This indicates that some regions, despite reaching the same recognition rate, required a higher order to achieve a match, reflecting a subtle disparity in the strength of the representative characteristics.

- AlexNet recorded the lowest EER values, reaching 1.4995 in the major-little area, and 1.8008 in the major-ring, surpassing VGG16 and VGG19, whose best results ranged from 1.3952 to 1.5300.
- Alexnet can be considered the most worthy and optimal in identification or identification without application tied Rank Normalization.

3.7.4 unimodal Performance with Tied Rank Normalization

The same as the previous experiments were carried out but using the Tied Rank Normalization technique to improve the distribution of values extracted from neural networks. The results were presented in the following tables.

The test results for each technique were written down and the best performance was shaded in yellow.

Comparison of the results of the alexnet, vgg 16 and Vgg 19 unimodal with Tied Rank Normalization

- VGG16 and VGG19 recorded a significant improvement in performance when applying Tied Rank Normalization compared to alexnet , especially in reducing EER and improving ROR, which confirms the actuality and importance of normalization in improving attribute discrimination.
- Major Knuckle areas were distinguished, especially the ring and middle always.
- The First knuckle continued to give poor results in terms of ERR and ROR, despite a slight improvement after normalization , but they always remained in the final ranking
- AlexNet recorded the lowest air values, ranging from 1 to 2 mostly, except in two cases I got 3 and 4 in vgg16 and in vgg19, whose best results ranged from 2 to 5 So it can be said that the best way to identify both open-set and closed-set systems is AlexNet.

Abstract (Unimodal systems with and without Tied Rank Normalization)

By analyzing the results of single models (AlexNet, VGG16, and VGG19), it becomes clear that the areas of the major knuckles (Major Knuckles) were the most distinguished in terms of performance, recorded the lowest error rates (EER) and the highest discrimination rates (ROR), especially in the ring and middle fingers. In contrast, the first Knuckle regions showed relatively weaker performance in all networks, which indicates the limitations of the attributes extracted from them. The application of Tied Rank Normalization also contributed

to significantly improving performance, which confirms the importance of normalization in raising the efficiency of models and reducing its variability.

3.8 Multi-modal system test result

The integration of information extracted from different types of fingers at a stage of the biometric recognition system, whether at the sensor level, the feature level, the level of matching results or the decision-making level, significantly contributes to enhancing the overall performance of the system. However, the most common and effective integration patterns in multimedia biometric systems take place at the level of matching results (fusion matching level), due to the excellent balance it offers between ease of integration and information richness. We have conducted experiments to evaluate the effectiveness, where algorithmic and biometric integration was tested with and without the application of Tied Rank and we have written down the results in the following tables and include a set of integration strategies at the level of the Maximum score, Minimum score, Summation rule and multiplication rule.

The test results for each technique were written down and the best performance was shaded in yellow.

3.9 Fusion at matching level

3.9.1 Algorithmic Fusion

In this level we will integrate both the DC, major, second and first of four fingers (Index, Middle, Ring, Little), using three deep networks (AlexNet, VGG16, VGG19).

Algorithmic Fusion without Tied Rank Normalization

Discussion

According to table 3.7 in the case of determining the Open set, it can be noted that the system has significantly improved In terms of efficiency, the proportions have been reduced to about **EER=0.993** and **T0=0.7910** at **DC**, and this is when using **SUM** or even at first, second and major for all fingers, we note a significant improvement in terms of results and recognition . As for **MUL**, the identification ratios were relatively acceptable and improved compared to (Alexnet, vgg 16 and vgg19) without Tied Rank Normalization, but the worst identification was recorded at **MIN** and **MAX** with a decrease in identification.

As for the case of closed-set identification, we note where the system has improved in terms of efficiency and identification Where the ratios were raised to approximately **ROR=96.2** and **RPR=309** in the **Major ring** , we also notice a noticeable increase in the ratios of the first, second and major for all fingers compared to **MUL**, but the worst identification was

recorded at MIN and MAX with a decrease in identification.

		SUM	MUL	MIN	MAX
DC	EER	0.903	2.0763	1.4857	1.40361
	T0	0.7910	0.9510	0.8320	0.7710
	ROR	93.5	93.5	92.4	92
	RPR	375	392	355	415
First index	EER	3.4112	3.7165	5.2052	4.2130
	T0	0.7580	0.8990	0.7670	0.7610
	ROR	83.5	83.7	76.2	77
	RPR	330	310	431	319
First midlle	EER	2.6044	2.9005	4.2120	3.4002
	T0	0.7320	0.8880	0.7650	0.7250
	ROR	86	86.1	81.2	82
	RPR	492	492	496	480
First ring	EER	2.1976	2.7858	3.8054	3.2018
	T0	0.7290	0.8800	0.7620	0.7220
	ROR	90.3	90.6	85.2	86.5
	RPR	457	455	458	475
First little	EER	2.2953	2.5844	3.9958	2.8975
	T0	0.7530	0.8970	0.7600	0.7470
	ROR	87.3	87.1	80.7	82.5
	RPR	429	431	372	425
Second index	EER	2.2925	2.9047	3.4642	2.4020
	T0	0.7780	0.9270	0.8450	0.7700
	ROR	91.8	91.8	87.7	87.2
	RPR	429	431	392	325
Second midlle	EER	1.7994	2.8240	2.6589	2.3075
	T0	0.7640	0.9320	0.8220	0.7500
	ROR	93.5	93.1	91.4	90
	RPR	250	229	361	243
Second ring	EER	1.7950	2.6240	2.9061	2.2995
	T0	0.7600	0.9270	0.8140	0.7420
	ROR	92.6	92.5	87.7	89.3
	RPR	200	195	270	285
Second little	EER	1.4036	2.0847	2.6995	1.8931
	T0	0.7460	0.9120	0.8040	0.7360
	ROR	92.9	93.2	89.8	89.4
	RPR	337	356	298	462
Major index	EER	1.5770	2.3266	2.2935	2.1990
	T0	0.7810	0.9240	0.8200	0.7600
	ROR	93.2	93.3	88.9	91.2
	RPR	415	414	391	427
Major midlle	EER	1.7003	2.2036	2.1960	2.0022
	T0	0.7510	0.9320	0.7780	0.7480
	ROR	95.8	95.9	92.8	94
	RPR	498	498	497	472
Major ring	EER	1.3057	2.1314	2.0070	1.7988
	T0	0.7480	0.9240	0.7770	0.7450
	ROR	96.1	96.2	93.9	94.8
	RPR	340	309	392	289
Major little	EER	0.9992	1.8058	1.8066	1.3745
	T0	0.7760	0.9270	0.7910	0.7700
	ROR	94.9	95.1	91.2	92.9
	RPR	197	202	204	267

Table 3.7: multimodal system Performance Based Algorithmic without Tied Rank Normalization

Algorithmic Fusion with Tied Rank Normalization

		SUM	MUL	MIN	MAX
DC	EER	0.5990	0.8967	0.998	1.0995
	T0	0.6970	0.8590	0.7250	0.6790
	ROR	93.7	93.6	92.3	92.4
	RPR	374	364	468	315
First index	EER	3.1117	3.3561	4.6859	3.8122
	T0	0.7070	0.8450	0.7190	0.7060
	ROR	83.7	83.9	76.3	76.6
	RPR	312	286	402	379
First middle	EER	2.2959	2.6004	3.7190	3.0785
	T0	0.6810	0.8300	0.7140	0.6710
	ROR	86	86.2	81.2	83.3
	RPR	449	450	388	471
First ring	EER	2.2054	2.7033	3.2242	2.9932
	T0	0.6770	0.8230	0.7130	0.6690
	ROR	90.2	90.3	84.3	87
	RPR	443	441	429	423
First little	EER	2.2983	2.4692	3.8006	3.3878
	T0	0.6990	0.8470	0.7160	0.6870
	ROR	87.4	87.5	80.7	82.7
	RPR	430	433	463	431
Second index	EER	2.1077	2.4305	3.7571	2.5023
	T0	0.6930	0.8640	0.7470	0.6950
	ROR	91.8	91.8	87.7	87.7
	RPR	322	319	340	361
Second middle	EER	1.5918	2.1127	2.2977	1.8927
	T0	0.6750	0.8490	0.7180	0.6790
	ROR	93.9	93.9	91.1	91.3
	RPR	257	260	372	299
Second ring	EER	1.8016	1.9854	2.5021	1.9786
	T0	0.6750	0.8560	0.7340	0.6800
	ROR	93.5	93.5	88	90
	RPR		180	237	259
Second little	EER	1.3005	1.5067	1.9717	1.6042
	T0	0.6710	0.8420	0.7160	0.6790
	ROR	92.6	92.7	89.9	89.8
	RPR	328	332	342	352
Major index	EER	2.1077	2.4305	2.7571	2.5023
	T0	0.6930	0.8640	0.7470	0.6950
	ROR	91.8	91.8	87.7	87.7
	RPR	322	319	340	361
Major middle	EER	1.5027	1.6170	1.8012	1.7065
	T0	0.6500	0.8370	0.7080	0.6550
	ROR	95.6	95.9	93.2	94.5
	RPR	497	497	493	407
Major ring	EER	0.9992	1.4732	1.5003	1.1033
	T0	0.6510	0.8270	0.6980	0.6790
	ROR	96	95.9	93.6	94.9
	RPR	250	233	255	280
Major little	EER	0.9013	1.3023	1.4875	1.3808
	T0	0.7150	0.8720	0.7360	0.7080
	ROR	94.6	94.5	92.7	92.4
	RPR	145	149	187	255

Table 3.8: multimodal system Performance Based Algorithmic with Tied Rank Normalization

Discussion

According to table 3.8 in the case of determining the Open set, it can be noted that the system has significantly improved In terms of efficiency, the proportions have been reduced to about

EER=0.5990 and **T0=0.069700** at **DC**, and this is when using **SUM** or even at first, second and major for all fingers, we note a significant improvement in terms of results and recognition. As for MUL, the identification ratios were relatively acceptable and improved compared to (Alexnet, vgg 16 and vgg 19) with Tied Rank Normalization, but the worst identification was recorded at MIN and MAX with a decrease in identification.

As for the case of closed-set identification, we note where the system has improved in terms of efficiency and identification. Where the ratios were raised to approximately **ROR=96** and **RPR=250** in the **Major ring**, we also notice a noticeable increase in the ratios of the first, second and major for all fingers compared to **MUL**, but the worst identification was recorded at MIN and MAX with a decrease in identification.

3.9.2 biometric Fusion

Since alexnet scored better results than vgg 16 and vgg 19, then we will rely on them in the study this bold.

biometric Fusion without Tied Rank Normalization

		SUM	MUL	MIN	MAX
first	EER	0.7213		3.0020	1.2949
	T0	0.8		0.8060	0.84
	ROR	93.7		88.8	91.6
	RPR	375		491	327
second	EER	0.7017		1.9284	1.5968
	T0	0.84		0.8390	0.810
	ROR	96.3		93.3	94.6
	RPR	426		308	453
major	EER	0.6164		1.5298	0.9966
	T0	0.7670		0.821	0.750
	ROR	98.2		95.1	96.8
	RPR	135		392	336
DC+first	EER	0.0997	0.1946	2.8903	0.2987
	T0	0.842	0.976	0.8540	0.785
	ROR	99.2	99.3	90.8	97.2
	RPR	18	9	372	35
DC+second	EER	0.5976	1.5924	1.9932	1.3209
	T0	0.844	0.996	0.849	0.801
	ROR	97.0	97.1	93.6	95.4
	RPR	328	382	156	453
DC+major	EER	0.0999	0.0716	1.6917	0.123
	T0	0.7790	0.9840	0.8570	0.7820
	ROR	99.7	99.7	95	99
	RPR	4	3	392	23

Table 3.9: multimodal system Performance Based biometric without Tied Rank Normalization

Discussion

This table shows the performance of the biometric recognition system using various integration techniques (SUM, MUL, MIN, MAX) without applying the Tied Rank Normalization

technique. The results show that the use of the combination between the Dc area and the joints (especially the DC+major joint) has achieved outstanding performance compared to the use of only single joints. In particular, when using the **Mul** fusion method for the DC+major group, the lowest **EER** error rate of **0.0790** was achieved, with a high **ROR** recognition rate of **99.7** and a low **RPR** recognition order of **3**, which indicates a high efficiency in distinguishing individuals. However, values in some other areas such as the first and second joint still indicate the possibility of improving performance.

biometric Fusion with Tied Rank Normalization

		SUM	MUL	MIN	MAX
first	EER	0.7017		2.9071	1.3278
	T0	0.744		0.7570	0.699
	ROR	96.2		89.3	91.9
	RPR	214		429	305
second	EER	0.7003		1.4985	1.3013
	T0	0.723		0.7570	0.701
	ROR	96.5		93.7	93.8
	RPR	381		377	230
major	EER	0.4929		1.1731	0.7139
	T0	0.6620		0.753	0.7139
	ROR	98.5		95.2	96.5
	RPR	77		306	336
DC+first	EER	0.0088	0.0851	1.8967	0.2999
	T0	0.8760	0.9450	0.7910	0.7380
	ROR	99.1	99.2	91.8	97.6
	RPR	4	5	327	83
DC+second	EER	0.5005	0.8889	1.1964	0.7990
	T0	0.6960	0.944	0.768	0.674
	ROR	97.0	97	94.3	94.7
	RPR	276	301	247	230
DC+major	EER	0.0999	0.1053	1.1005	0.3017
	T0	0.6630	0.918	0.761	0.6520
	ROR	99.5	99.6	95.8	98.9
	RPR	15	14	304	149

Table 3.10: multimodal system Performance Based biometric with Tied Rank Normalization

Discussion

This table shows the same consolidation strategies used in the previous table, but with the application of the Tied Rank Normalization technique. By comparison, it becomes clear that this technique contributed to significantly improving the results of the system. The DC-major combination using the **MUL** method recorded the best performance among all combinations, the error rate of **EER** decreased to **0.918**, the **ROR** recognition rate increased to **99.6**, with RPR remaining at a low level of **14**. Other combinations such as DC+first and DC+second also showed a noticeable improvement in performance. the best result recorded at DC+first according to **EER** was **0.0088** at **SUM**.

3.10 Conclusion

In this chapter, the proposed model of biometric recognition using the hand area was evaluated and studied, a pre-trained deep learning network known as AlexNet, VGG16 and vgg 19 was used to extract characteristics from hand images. After that, these characteristics were dispensed with and were used to train the SVM classifier in order to demonstrate their important role in improving recognition.

The proposed model was tested using a hand database that includes hand photos of 500 people. Experimental results have shown that the integration strategies adopted in this system provide better performance Multi-modal to the use of Unimodal, both in open-set and closed-set recognition mode, where a very low **EER** error rate of 0.0088 was achieved in open recognition mode and when using integration biometric Fusion , and a high **ROR** recognition rate of **99.700** in **closed-set** recognition mode and when using biometric Fusion.

General Conclusion

Identification of persons or identification based on physical or behavioral characteristics (e.g. finger print, iris, gait, or hand print) Or what is known as biometric identification , as this area has received increased attention By researchers, companies or also research centers of criminals, especially in places that require careful security systems. Among the The biometric methods used, the dorsal hand method, thanks to being unique and fixed with age, received great attention as a promising feature in the investigation and identification.

This research aims to provide an effective methodology to improve the performance of biometric identification systems through the use of hand images, specifically images of the joints of the four fingers, relying on deep learning techniques (using AlexNet, vgg 16 and vgg 19) and this with and without normalization of the parity rank to derive the most distinctive and effective features, also in open and closed-set we will study cases in uni-modal and multi-model highlighting the difference between them and their effectiveness and it is more.

The system proposed in this study is based entirely on processing, relying on non-contact imaging, which makes it possible to deal with possible variations in images caused by environmental and personal factors. Experimental results on a database of 500 people show that finger joints and dc carry high potential as accurate biometric features.

In conclusion, we hope that this work will serve as a stimulating starting point for the development of innovative biometric methods, and an effective contribution to supporting future applications based on hand-to-hand recognition.

Bibliography

- [1] Ilhem Hadjij, Miloud Sardou, Hanifi Missoum, and Said Maouche. Flood-related deaths in northwestern algeria from 1966 to 2019. *Arabian Journal of Geosciences*, 14(18):1923, 2021.
- [2] Maarouf Korichi, Aicha Korichi, and Meriem Korichi. A deep learning-based biometric system for hand dorsal identification: Improving accuracy and robustness through tied-rank normalization. In *2025 International Symposium on iNnovative Informatics of Biskra (ISNIB)*, pages 1–4. IEEE, 2025.
- [3] G Jagadamba, R Sheeba, K N Brinda, K C Rohini, and S K Pratik. Adaptive e-learning authentication and monitoring. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pages 277–283, 2020.
- [4] Manal Khedidja BENDANIA and Amel ZEKRI. *Biometric Crypto System for Person Information Security*. PhD thesis, UNIVERSITY OF KASDI MERBAH OUARGLA, 2020.
- [5] Sanjay Kanade. *Enhancing information security and privacy by combining biometrics with cryptography*. PhD thesis, Institut National des Télécommunications, 2010.
- [6] Bhattacharyya Debnath, Ranjan Rahul, Alisherov Farkhod, Choi Minkyu, et al. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3):13–28, 2009.
- [7] ELUPU Pop and G Petre. Multimodal biometric systems overview. *ActaTech. Napocensis Electron. Telecommun*, 49(3), 2008.

- [8] Lawrence O’Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.
- [9] Michael Goh Kah Ong, Connie Tee, and Andrew Teoh Beng Jin. Touch-less palm print biometric system. In *International Conference on Computer Vision Theory and Applications*, volume 2, pages 423–430. SCITEPRESS, 2008.
- [10] Dyala R Ibrahim, Abdelfatah A Tamimi, and Ayman M Abdalla. Performance analysis of biometric recognition modalities. In *2017 8th international conference on information technology (ICIT)*, pages 980–984. IEEE, 2017.
- [11] Kai Cao and Anil K Jain. Automated latent fingerprint recognition. *IEEE transactions on pattern analysis and machine intelligence*, 41(4):788–800, 2018.
- [12] Anil K Jain, Arun A Ross, Karthik Nandakumar, Anil K Jain, Arun A Ross, and Karthik Nandakumar. Iris recognition. *Introduction to Biometrics*, pages 141–174, 2011.
- [13] Himanshu Srivastava. A comparison based study on biometrics for human recognition. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 15(1):22–29, 2013.
- [14] Milan Sonka, Vaclav Hlavac, Roger Boyle, Milan Sonka, Vaclav Hlavac, and Roger Boyle. Image pre-processing. *Image processing, analysis and machine vision*, pages 56–111, 1993.
- [15] M. Bahaz and M. Hamza. Palmprint and palmvein recognition based on deep learning. Master’s thesis, Université Ouargla, 2018.
- [16] Huang Jin Jie and Putra Wanda. Runpool: A dynamic pooling layer for convolution neural network. *International Journal of Computational Intelligence Systems*, 13(1):66–76, 2020.
- [17] Fuzhen Zhuang, Zhiyuan Qi, Keyu Duan, Dongbo Xi, Yongchun Zhu, Hengshu Zhu, Hui Xiong, and Qing He. A comprehensive survey on transfer learning. *Proceedings of the IEEE*, 109(1):43–76, 2020.
- [18] Md Zahangir Alom, Tarek M Taha, Christopher Yakopcic, Stefan Westberg, Paheding Sidike, Mst Shamima Nasrin, Brian C Van Esesn, Abdul A S Awwal, and Vijayan K Asari. The history began from alexnet: A comprehensive survey on deep learning approaches. *arXiv preprint arXiv:1803.01164*, 2018.
- [19] Annapoorna Shetty, Shravya Shetty K, and Krithika K. A review on asymmetric cryptography–rsa and el gamal algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 2014.