

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR - ANNABA



جامعة باجي مختار- عنابة

Faculté: Sciences de l'ingéniorat
Département: Electronique

Année : 2021

THÈSE

Présentée en vue de l'obtention du diplôme de Doctorat 3^{ème} Cycle

Intitulé

**Fusion multimodale de données : Application en
biometrie
Multimodal data fusion : Biometric application**

Option : Traitement de l'Image et signaux biomédicaux

Par : DAAS Sara

DIRECTEUR DE THÈSE : BOUGHAZI Mohamed Pr. Université d'Annaba

CO-DIRECTEUR DE THÈSE : BOURENNANE EL bay Pr. Université de Bourgogne

DEVANT Le JURY

PRESIDENT : SAOUCHI Kaddour Pr. Université d'Annaba

EXAMINATEURS : OUCHTATI Salim Pr. Université de Skikda

HAFS Toufik MCA Université d'Annaba

INVITE: Bakir Toufik Pr. Université de Bourgogne

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR - ANNABA

جامعة باجي مختار - عنابة



Faculty: Sciences of Engineering
Department: Electronics

Year: 2021

THESIS

Presented in order to obtain the diploma of Ph.D 3rd Cycle

Entitled

Multimodal data fusion: biometrics application

Option: Biomedical Image and Signal Processing

By: DAAS Sara

Committee Members:

President:	SAOUCHI Kaddour	Pr. Univ. Annaba Algeria
Supervisor:	BOUGHAZI Mohamed	Pr. Univ. Annaba Algeria
Co-Supervisor:	BOURENNANE EL Bay	Pr. Univ. of Burgundy Dijon France
Reviewers :	OUCHTATI Salim	Pr. Univ. Skikda Algeria
	HAFS Toufik	MCA Univ. Annaba Algeria
Guest :	Bakir Toufik	Pr. Univ. of Burgundy Dijon France

ACKNOWLEDGEMENT

First of all, I thank Allah the almighty, for allowing me to reach this modest scientific level and for giving me the courage and the patience to carry out the work done in this thesis.

I would like to express my deep and sincere gratitude to my research supervisor, Pr. BOUGHAZI Mohamed, for giving me the opportunity to do research and providing invaluable guidance throughout this research.

I take this opportunity to express my sincere thanks to my thesis co-supervisor, Pr. BOURENNANE El-Bay with whom, I learned to analyse, criticize, and express myself as clearly as possible. I wouldn't be exaggerating to say that his dynamism, vision, sincerity, motivation and belief in me have deeply inspired me. I am extremely grateful for what he has offered me. I also want to thank Pr. Toufik Bakir from the university of burgundy Dijon, France, for their guidance and helpful comments. It has been an honour and pleasure to work with him. I would particularly like to thank all the jury members who have accepted to preside and read this work. Pr. SAOUCHI Kaddour from Annaba University as jury president, Dr. HAFS Toufik from Annaba University and Pr. OUCHTATI Salim from Skikda University.

I owe my deepest gratitude to Pr. Salah Toumi for his eminent support and encouragement throughout my research project. I am extending my heartfelt thanks to my colleagues and friends Dr. Yahi Amira and her husband, Dr. AIT-IZEM Tarek, for their acceptance, patience, support, help and advice. Finally, I would like to give my gratitude to my family members for their persistent and unconditional understanding and support. To the most magnificent mother, Somaah Rahma and best sister Djihad, always supported me and encouraged me to go as far as possible in my studies.

DAAS SARA

Abstract

Title : Multimodal data fusion : biometric application

In nowadays, the identification or recognition of presence using secure systems is a critical issue. Various solutions are proposed to achieve a secure information system. The most known means used *Biometrics* traits. Unimodal biometrics have improved the possibility of establishing secure systems capable of identifying and managing the flow of individuals according to the available intrinsic characteristics. Unfortunately, and despite their effectiveness, those Unimodal biometric suffer from different limitations such as non-revocability, non-template diversity, and the possibility of privacy. To overcome those limitations, a reliable, secure recognition system requires multiple resources. The combination and fusion of several biometric systems, Which is known as "*Multimodal biometrics*".

This thesis aims to combine and fuse different finger-based biometrics (Finger Vein (FV), and Finger Knuckle Print (FKP)). In his context, this work treats the deep learning approaches with different convolutional neural network architectures (CNN). The informative features for FP, FV, and FKP are performed using transfer learning CNN models. After that, the key step aims to select separate features from each unimodal biometrics modalities and combine them using various fusion approaches. The obtained results indicate that the finger-based biometric recognition systems using deep learning are secure, robust and reliable.

Keywords : Biometric, Multimodal biometrics, Image processing, Deep learning, Transfer learning, Data fusion, Fingerprint, Finger vein, Finger knuckle print.

Résumé

Titre : Fusion Multimodale de données : Application en biométrie

De nos jours, l'identification ou la reconnaissance de présence à l'aide de systèmes sécurisés est un enjeu critique. Différentes solutions sont proposées pour réaliser un système d'information sécurisé. Les moyens les plus connus utilisaient les traits "*biométriques*". La biométrie unimodale a amélioré la possibilité de mettre en place des systèmes sécurisés capables d'identifier et de gérer les flux d'individus en fonction des caractéristiques intrinsèques disponibles. Malheureusement, et malgré leur efficacité, ces biométries Unimodales souffrent de différentes limitations telles que la non-révocabilité, la diversité sans modèle et la possibilité de confidentialité. Pour résoudre ces limitations, un système de reconnaissance fiable et sécurisé nécessite de multiples ressources. La combinaison et la fusion de plusieurs systèmes biométriques, connue sous le nom de "*biométrie multimodale*".

Cette thèse vise à combiner et fusionner différentes biométries basées sur les doigts (Empreinte Veineuse, Empreinte d'articulation de doigt). Dans son contexte, ce travail traite les approches d'apprentissage en profondeur avec différentes architectures de réseaux de neurones convolutifs (CNN). Les fonctions informatives pour les doigts sont exécutées à l'aide de modèles CNN d'apprentissage par transfert. Après cela, l'étape clé vise à sélectionner des caractéristiques distinctes de chaque modalité biométrique unimodale et à les combiner à l'aide de diverses approches de fusion. Les résultats obtenus indiquent que les systèmes de reconnaissance biométrique à base le doigt utilisant l'apprentissage en profondeur sont sécurisés, robustes et fiables.

Mots clés : La Biométrie, Biométrie multimodale, Traitement d'images, Apprentissage profond, Apprentissage par transfert, Fusion de données, Empreinte digitale, Empreinte Veineuse, Empreinte d'articulation de doigt.

ملخص

العنوان: دمج البيانات متعدد الوسائط: تطبيق على القياسات الحيوية

في الوقت الحاضر ، يشكل تحديد هوية الشخص أو التعرف عليهم باستخدام نظم أمانة مسألة بالغة الأهمية. وقد تم اقتراح العديد من الحلول المختلفة لتحقيق نظام معلومات امن. أكثر الوسائل المعروفة تستخدم سمات القياسات الحيوية. وقد حسنت القياسات الحيوية الأحادية الوسائط إمكانية إنشاء نظم أمانة قادرة على تحديد وإدارة تداد الأفراد وفقا للخصائص الحيوية المتاحة. ولكن من المؤسف أن تلك القياسات الحيوية الأحادية الوسائط غير مجدية ، على الرغم من فعاليتها هي تعاني من قيود مختلفة مثل عدم القابلية للإلغاء ، والتنوع غير النمطي ، وإمكانية الخصوصية. للتغلب على تلك القيود ، يتطلب وجود نظام معتمد ومأمون للاعتراف موارد متعددة والذي يعتمد على الجمع والاندماج من عدة أنظمة القياس الحيوي ، و يعرف باسم القياسات الحيوية متعددة الوسائط. تهدف هذه الأطروحة إلى الجمع بين مختلف القياسات الحيوية القائمة على الأصابع. و يعالج هذا العمل مناهج التعلم العميقة مع هياكل شبكة عصبية متشابكة مختلفة (سي إن إن). وتجري المميزات الإعلامية لأصابع باستخدام نماذج تعلم النقل لـ(سي إن إن). وبعد ذلك ، تهدف الخطوة الرئيسية إلى اختيار سمات منفصلة من كل طريقة قياس حيوي أحادي الوسائط ودمجها باستخدام نهج اندماج مختلفة. وتشير النتائج المتحصل عليها إلى أن نظم التعرف على القياسات البيولوجية القائمة على الأصابع التي تستخدم التعلم العميق أمانة وقوية وموثوق بها.

الكلمات الدالة: القياسات الحيوية ، القياسات الحيوية متعددة الوسائط ، معالجة الصور ، التعلم العميق ، نقل التعلم ، دمج البيانات ، بصمات الأصابع ، وريد الأصابع ، بصمة مفصل الإصبع.

CONTENTS

List of Figures	viii
List of Tables	xi
List of Acronyms	xii
General Introduction	1
.1 Context of the research and motivation	3
.2 Problem statement and objectives	4
.3 Contributions	5
.4 Thesis Outline	6
I Biometrics Overview	7
I.1 Introduction	8
I.2 Biometrics Technologies	8
I.2.1 Biometrics Definition	8
I.2.2 Biometrics History	8
I.3 Biometrics Modalities Types	10
I.3.1 Morphological Biometrics	10
I.3.2 Behavioural Biometrics	13
I.3.3 Biological Biometrics	15
I.3.4 Hidden Biometrics	16
I.3.5 Comparative Study Between Different Biometrics Modalities	18
I.4 Biometrics Applications	23
I.5 Biometrics Systems Process	26
I.6 Unimodal Biometrics System Architecture	26
I.7 Biometrics Recognition	28
I.7.1 Enrollment Biometrics Modes:	28
I.7.2 Verification Or Identification Biometrics Modes:	28
I.8 Biometrics Systems Performances Evaluation	30
I.9 Conclusion	34
II Multimodal Biometric Systems	35
II.1 Introduction	36
II.2 Unimodal Biometrics Systems Limitations	36
II.3 Multi-modality in Biometrics	37

II.3.1	Data Fusion Concept	37
II.3.2	Multi-Biometrics Sources	38
II.3.3	Multimodal Biometrics System Architectures	39
II.4	Biometrics Fusion Levels	41
II.4.1	Fusion Pre-Classification:	41
II.4.2	Post-Classification:	43
II.5	Biometrics Fusion Methods	47
II.6	Conclusion	48
III	Finger-based Biometrics	49
III.1	Introduction	50
III.2	Bibliometric Analysis of Finger-Based Biometrics	50
III.2.1	Research process	50
III.2.2	Preliminary Search Results	51
III.2.3	Exploratory Data Highlights	54
III.2.4	Deductions from Bibliometric Analysis	59
III.3	Fingerprint Biometrics	59
III.3.1	Fingerprint Imaging Principle	60
III.3.2	Fingerprint Databases	60
III.4	Finger Vein Biometrics	62
III.4.1	Finger Vein Imaging Principle	63
III.4.2	Finger Vein Databases	63
III.5	Finger Knuckle Print Biometrics	65
III.5.1	Finger Knuckle Print Imaging Principle	65
III.5.2	Finger Knuckle Print Databases	66
III.6	Conclusion	67
IV	Deep Learning Overview	68
IV.1	Introduction	69
IV.2	Machine learning Overview	69
IV.2.1	Machine Learning types	70
IV.2.2	Machine Learning "Classic"	71
IV.3	Artificial Neural Network	75
IV.4	Deep Learning and Convolutional Neural Networks overview	76
IV.4.1	Convolution Neural Network (CNN)	77
IV.4.2	Convolution Neural Network (CNN) trend Architectures	79
IV.5	CNN training workflow and Transfer Learning concept	82
IV.5.1	Training workflow	82
IV.5.2	Data augmentation and transfer learning	83
IV.6	Conclusion	83
V	Finger-Based Multimodal Biometrics Recognition Systems Using Deep Learning	85
V.1	Introduction	86
V.2	Multimodal Biometric Recognition Systems Using Deep Learning based on the Finger vein and Finger knuckle print Fusion	86
V.2.1	Related Work	86
V.3	The Proposed Architectures	87
V.3.1	Unimodal System	88
V.3.2	Multimodal system	89
V.3.3	Used Databases	90
V.4	Results and Discussion	92

V.4.1	Training of deep learning architectures	92
V.5	Performances Evaluation	93
V.5.1	Test and analysis of the proposed biometrics recognition systems	93
V.5.2	Unimodal Recognition	93
V.5.3	Multimodal Recognition	95
V.5.4	Comparative Study	96
V.6	The proposed Finger Vein Biometric Scanner	99
V.6.1	Related work	99
V.6.2	Finger vein designed device	100
V.6.3	Near-infrared light controlling	101
V.6.4	Finger vein acquisition and control system	102
V.7	Results and discussion	104
V.8	Conclusion	107
General Conclusion		107
A Measuring Quality of Scientific Production		I
A.1	Publish or Perish Tool	I
A.2	VOSviewer Tool	II
A.3	Finger multimodal biometrics trend Analysis	II
B Data collection for finger vein biomtric		VI
Bibliography		XVII

LIST OF FIGURES

1	Relationships between the different objectives of the design of a biometric system .	4
I.1	Example of biometrics modalities	10
I.2	Example of fingerprint biometric modality	11
I.3	Example of finger knuckle print biometric	11
I.4	Example of Palmprint / hand geometry biometric modalities	12
I.5	Example of face biometric modality	12
I.6	Example of iris / retina biometric modalities	13
I.7	Example of ear biometric modality	13
I.8	Example of gait biometric modality	14
I.9	Example of voice biometric modality	14
I.10	Example of signature biometric modality	14
I.11	Example of keystroke dynamics biometric modality	15
I.12	Example of DNA biometric modality	15
I.13	Example of thermography biometric modalities	16
I.14	Example of vascular biometric modalities	16
I.15	Example of ECG / EEG biometric modalities	17
I.16	Example of brain biometric modality	17
I.17	Example of X-Ray biometric modalities	18
I.18	Comparison of different modalities according to Zephyr™ Analysis	22
I.19	Market size of different biometric technology	23
I.20	Example of mobile biometrics market	24
I.21	Example of consumer electronics biometrics market	25
I.22	Example of consumer electronics private biometrics market	26
I.23	Example of global biometrics technology market size	26
I.24	Biometric systems structure	27
I.25	Example of Enrollment biometric system	28
I.26	Example of verification biometric system	29
I.27	Example of identification biometric system	29
I.28	Example of FRR/FAR Illustration	32
I.29	Example of ROC and PR curves illustration	33
I.30	Example of CMC Curve	33
II.1	Example of Unimodal Biometric System limitations.	37
II.2	Example of Multimodal Biometrics Sources.	38
II.3	Example of fusion architectures	40

II.4	Example of different fusion levels of biometric systems.	41
II.5	Flowchart of fusion at the sensor level.	42
II.6	Flowchart of fusion at the feature extraction level.	42
II.7	Example on Feature Level Fusion of two Heterogeneous Feature Vectors.	43
II.8	Flowchart of fusion at the score level.	44
II.9	Flowchart of fusion at the decision level.	46
II.10	A diagram of the various levels of biometric fusion.	47
II.11	Fusion methods types example.	48
III.1	Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Flowchart of the research process	50
III.2	Language wise trend analysis	52
III.3	Documents Source wise type analysis	53
III.4	Documents by Year	53
III.5	Network visualization map of terms in title and abstract in the finger multimodal biometrics literature.	54
III.6	Density of Keywords map of terms in title and abstract.	55
III.7	Network visualisation map of author keywords in documents in the finger multi- modal biometrics.	55
III.8	Fused finger-based modalities of trend annalysis	56
III.9	Fusion level wise of trend analysis	57
III.10	Illustration of taxonomy of fingerprint feature levels	59
III.11	Principle of fingerprint imaging:(a) Optical Fingerprint Scanners, (b) Capacitive Fingerprint Scanners	60
III.12	Example of Fingerprint acquisition; Left: Rolled print, Middle: plain or slap print and Right: latent print.	61
III.13	Samples of images SDUMLA-HM fingerprint database.	62
III.14	Samples of images FVC 2004 fingerprint database.	62
III.15	Finger-vein pattern imaging : light reflection methods.	63
III.16	Finger-vein pattern imaging : light transmission methods.	64
III.17	Sample finger dorsal image to illustrate prior work in finger knuckle identification.	65
III.18	Finger knuckle print data acquisition module.	65
III.19	Finger knuckle Print (FKP) Acquisition Device.	66
IV.1	Relations between "Artificial intelligence", "Machine learning" and "Deep learning"	69
IV.2	Traditional programming (Top) VS Machine learning (Bottom).	70
IV.3	Machine learning types.	70
IV.4	Process of image classification steps common to most applications.	71
IV.5	Categories of feature extraction methods in the image.	72
IV.6	Biological (left) vs Artificial neuron (right).	75
IV.7	Examples of activation functions.	75
IV.8	Example of Multi-Layer Perceptron.	76
IV.9	Traditional machine learning vs deep learning pipelines.	76
IV.10	Standard CNN architecture.	77
IV.11	Convolution operation	78
IV.12	Max-pooling vs average pooling operations.	79
IV.13	AlexNet architecture	79
IV.14	AlexNet architecture	80
IV.15	Inception module.	80
IV.16	GoogLeNet architecture.	81
IV.17	Residual block.	81

IV.18 ResNet architecture.	81
IV.19 CNN training workflow.	82
IV.20: Data augmentation techniques, geometric transformation (left), GAN (right) . . .	83
V.1 Deep networks Architectures: (a) AlexNet, (b) VGG16 and (c) ResNet50	87
V.2 Unimodal recognition system	88
V.3 Multimodal recognition system based on feature level fusion	90
V.4 Multimodal recognition system based on score level fusion	91
V.5 Example of input images of different recognition systems: (a) Original databases images, (b) ROI images and (c) Images after preprocessing	91
V.6 Unimodal Finger vein recognition system: (a) Using Softmax, (b) Using SVM . . .	94
V.7 Unimodal finger knuckle print (FKP) recognition system: (a) Using Softmax, (b) Using SVM	95
V.8 multimodal recognition system feature level fusion: (a) Concatination methode using SVM , (b) Concatination methode using Softmax , (c) Addition methode using SVM ,(d) Addition methode using Softmax	96
V.9 Multimodal recognition system score level fusion	97
V.10 Finger-vein pattern imaging : light transmission methods	99
V.11 The general diagram of designed device.	100
V.12 PWM controller ISIS Circuit Design and Simulation for Arduino Microcontroller	101
V.13 Implement of finger vein acquisition control system.	102
V.14 Realised finger vein scanner.	104
V.15 Two-dimensional entropy curve in different light intensity.	104
V.16 Finger vein images under different light intensities.	105
V.17 The ten captured finger vein images in Same brightness level.	105
A.1 Publish or Perish software Main Window	II
A.2 VOSviewer software Main Window	II
A.3 Documents by subject area	III
A.4 h- index for documents	III
A.5 Network visualization map of citation document.	IV
B.1 Finger vein biomtrics data collection	VI

LIST OF TABLES

I.1	Comparison between biometric modalities	19
I.2	Advantages and disadvantages of different biometric techniques.	20
I.3	Prediction Confusion Matrix of a C-Class Classifier	30
I.4	Two-class classifier prediction confusion matrix	31
III.1	The Main Research Questions	51
III.2	Significant keyword and their combinations (i.e Using Scopus dataset)	52
III.3	Top ten documents in the related field from the data collected from the Scopus database.	58
III.4	Comparison between finger vein databases	64
III.5	Finger Knuckle Print Databases	67
IV.1	A comparative study on widely used four supervised classification algorithm	74
IV.2	Comparison between biometric modalities	77
V.1	Deep learning Networks Comparisons	87
V.2	Finger vein and Finger knuckle print used databases description	92
V.3	Description of initial parameters for training of various CNN models	93
V.4	Performance of unimodal finger vein (FV) recognition	94
V.5	Performance of unimodal finger knuckle print (FKP) recognition	94
V.6	Performance of finger vein(FV) and finger knuckle print (FKP) multimodal feature level fusion	95
V.7	Performance of finger vein (FV) and finger knuckle print (FKP) multimodal score level fusion.	96
V.8	Performance comparison of the proposed unimodal recognition with the state of the art systems	98
V.9	Performance of multimodal recognition	98
V.10	Finger vein devices proposed in research	100
V.11	Image quality metrics overview	103
V.12	RESULTS OF IMAGE TWO-DIMENSIONAL ENTROPY	105
V.13	Performance evolution parameters for reference image and captured finger vein images.	106
V.14	Comparison of the lowest MSE and highest PSNR of different brightness level.	106
V.15	Comparison of the lowest MSE and highest PSNR of Same brightness level.	107

LIST OF ACRONYMS

ACC

Accuracy

AD

Average Difference

ANN

Artificial Neural Network

AUC

Area Under the Curve

CCD

Charge Coupled Device

CMC

Cumulative Matching Characteristic

CNN

Convolution Neural Network

DCT

Discrete Cosine Transform

DET

Detection error tradeoff

DLA

(Dynamic Link Architecture)

DNA

Deoxyribo Nucleic Acid

DNN

Deep Neural Networks

DWT
Discrete wavelet transform

ECG
Electrocardiography

EDA
Exponential Discriminant Analysis

EEG
Electroencephalography

EER
Equal Error Rate

ELM
Extreme Learning Machine

FAR
False Acceptance Rate

FKP
Finger knuckle Print

Fn
False Negative

FP
FingerPrint

Fp
False Positive

FRR
False Rejection Rate

FV
Finger Vein

GAN
Generative Adversarial Networks

GAR
Genuine Acceptance Rate

HCA
Hierarchical Cluster Analysis

ICA
Independent Component Analysis

IQA
Image Quality Assessment

IQI
Image Quality Index

K-NN
K-Nearest Neighbor

LBP
(Local Binary Pattern

LDA
Linear Discriminant Analysis

LED
Light Emitting Diode

LMSE
Laplacian Mean Squared Error

LTP
(Local Ternary Pattern

MD
Maximum Difference

MLP
Multi-Layer Perceptron

MRI
Magnetic Resonance Imaging

MSE
Mean Squared Error

N
Negative class Total Number

NAE
Normalized Absolute Error

NIR
Near-infrared

NK

Normalized CrossCorrelation

NLP

Natural Language Processing

P

Positive class Total Number

PCA

Principal Component Analysis

PIN

Personal Identification Number

Pneg

The total number of samples classified negatively

Ppos

The total number of samples classified positively

PR

Precision-Recall

PRISMA

Preferred Reporting Items for Systematic Reviews and Meta-Analyses

PSNR

Peak Signal to Noise Ratio

PWM

Pulse Width Modulation

ResNet

Residual Neural Network

RNN

Recurrent Neural Networks

ROC

Receiver Operating Characteristic

ROI

Region Of Interest

ROR

Rank One Recognition

RPR

Rank of Perfect Recognition

SC

Structural Content

SIFT

Scale-Invariant Feature Transform

SVM

Support Vector Machine

TanH

Hyperbolic Tangent Normalisation

Tn

True Negative

Tp

True Positive

GENERAL INTRODUCTION

*“Research is to see what everybody
else has seen, and to think what
nobody else has thought.”*

Albert Szent-Gyorgyi

.1 Context of the research and motivation

Nowadays, individuals security and safety, properties, and information need to be assured and present one of the major concerns, especially after the great spread of technologies [1]. People who want to travel borders must use their passports to verify their identities. Also, those who want to traverse buildings or enter a university must verify their access cards. People who want to use banking services must first create an account with a user name and password. Nevertheless, these traditional methods show great weaknesses for identity verification. Indeed, a person's identity. Indeed, a person's identity is directly related to what they possess (such as passport, access card, etc.) or/and that they know (password, PIN codes, etc.). Nonetheless, PIN codes and passwords may be forgotten or compromised, and access cards may be falsified or duplicated, which lead to identity spoofing. In this respect, experts are searching for a technology that resolves these problems by providing more convenience to persons and assure highly secured access by relating a person's identity. Biometry is the most appropriate technology for identity verification or identification using physiological features, including biological, morphological and behavioural characteristics. This technology makes identity data theft more difficult and thus increases user confidence as the physical presence is necessary during identification.

Historically speaking [2], biometry emerged as a replacement for anthropometric recognition in the past. Fingerprint analysis was the first, and it was utilized by police to identify people. A French criminologist developed the scientific technique known as "forensic anthropology" in the 19th century to identify offenders based on physiological measurements. Indeed, fingerprints are still used for criminal identification, and this usage has never been abandoned. Due to advanced computing algorithms employed in devices, the increased power of computers may now contribute to individual recognition. As a result, biometry is a challenging topic whose goal is to use technology systems to identify people based on their biological characteristics. It's no longer only about fingerprints and criminal records. The use of biometry is widespread around the world and takes an important place in our daily life. For example, firstly, to identify or authenticate individuals and secondly to control public spaces such as banking, airports, hospitals, museums, railway and bus stations.

Different unimodal biometric systems based on unique biometric modality have been developed. While unimodal biometric techniques promise to be very efficient, we may not assure a good recognition rate. Indeed, they present three main limitations, which are as follows: limitation in terms of performances, limitation in terms of the universality of use and limitation in terms of fraud detection [3]. Consequently, in recent years, there has been an increasing interest in the evaluation of biometric systems security, which has led to the creation of numerous and very diverse initiatives focused on this field of research. The most employed solution is using several biometric modalities called multimodal biometric systems.

In 1995 the first work of multimodal biometrics was proposed, using the fusion of face and voice. Since then, many studies have been carried out combining different modalities and considering the different levels of data fusion and multiple fusion rules.

There are five types of multimodal systems: multisensors, multiinstances, multialgorithms, multisamples and multibiometrics. These different types of multimodal systems could reduce several problems encountered in single-mode systems. For example, the first four systems combine information resulting from a single modality capable of improving recognition performance by reducing intra-class variability. However, these systems cannot deal with the problem of the non-universality of certain biometrics, such as resistance to fraud. So unlike multimodal systems which use multiple biometric data, they are able to build a more flexible system.

In this context, the works presented in this thesis are located. Various multimodal approaches are proposed here, using different multi-biometrics fusions for both identification modes. These approaches are based essentially on finger-based biometrics. In fact, our motivation to use these

modalities is due to the popularity of fingerprint, finger vein, and finger knuckle print biometrics trait. Compared to other biometric modalities, finger-based biometrics (fingerprint, finger vein, and finger knuckle print) presents the following advantages:

- The finger-based trait is more acceptable by the public compared to other modalities;
- The finger-based information may be extracted using low-resolution images;
- The finger based acquisition devices are simple and inexpensive.
- The modalities are close geometrically and can integrate them and embedded in one biometric system.

.2 Problem statement and objectives

The design of each biometric system should take into account five major and related factors: cost, accuracy, user acceptance and environmental constraints, security and computation speed (see Figure 1). In fact, decreasing user acceptance may improve accuracy, decreasing accuracy may increase speed and increasing cost may ameliorate security [4].

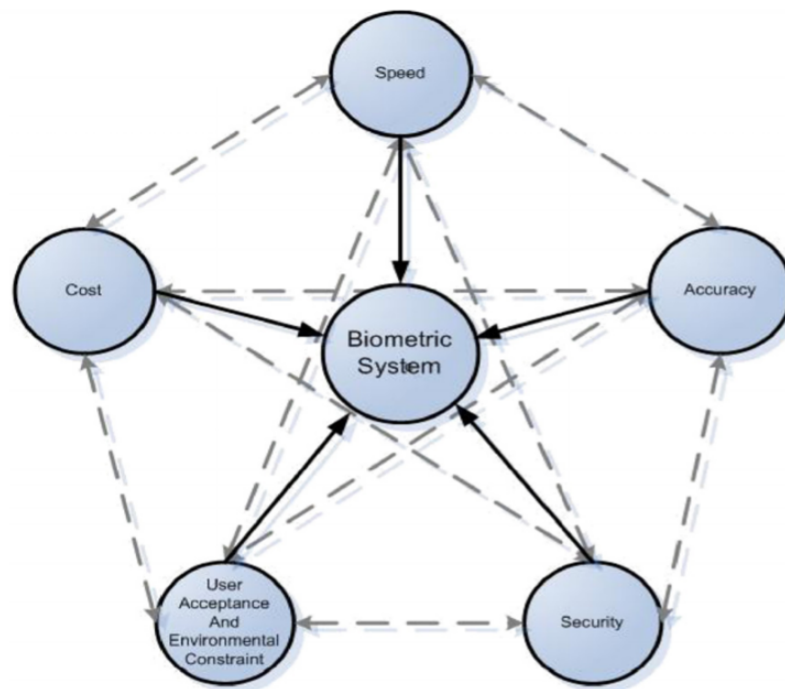


Figure 1: Relationships between the different objectives of the design of a biometric system¹.

To increase accuracy, two biometric modalities are acquired simultaneously from a single acquisition of the fingerprint trait. Nevertheless, fingerprint biometrics present some problems which may deal with respecting the mentioned objectives. The sensor device of the fingerprint modality are available and cheap. However; the fingerprint map is subject to copying and spoofing [5] Which weaken this modality as an information security biometrics. Moreover, fingerprint sensor needs contact yielding imprecise record and possible diseases transmission. Indeed, the previous fingerprint biometric systems were based on the direct contact of the finger trait with the system device to capture, which may decrease accuracy and biometrics system security.

¹Image source: [A survey of palmprint recognition](#)

For this reason, recent works have been focusing on contact-less and contact-free acquisition systems making it more comfortable and hygienic by eliminating the contact obligation. The acquisition device of finger vein and finger knuckle print are based contact-less equation system. Where the finger vein biometrics exhibit several advantages, such as a permanent vein pattern [6], indeed, the blood vessel network underneath the skin is unique for every individual and could not be replicated or damaged. Besides all the benefits of finger vein biometrics, there is a problem affecting the system performance.

In fact, finger vein recognition devices using near-infrared light and monocular camera capture threads from one side of the finger, and thus only one-third of the vein pattern is recorded. In addition, because of the contactless sensor, reference recorded finger vein information and imprecise subject finger position during the identification process could not match due to finger rotation and translation [7–9]. Moreover, finger knuckle print or finger dorsal texture is unique and used as a biometrics identification technique in many works. It is difficult to damage (people usually use the inner side of their hands), and its acquisition device is non-invasive and cheap. Besides, the lack of anti-counterfeiting capability remains a limit for such a visible biometrics modality. Finger knuckle print is affected by displacement and rotation of finger as well because of contactless sensor [10–12].

Research in this area is certainly interesting via the multiplicity and diversity of these problems. In fact, finger-based biometrics modality has received much attention from research laboratories as well as industrial ones.

.3 Contributions

According to the cited problems and to ensure the design of our finger-based biometric system success, our objectives focus on the proposition of a solution that increases the accuracy. The speed of the person recognition process decreases the cost of the biometric system and increases user acceptance.

Hence, our solution is based on a multimodal hand finger-based biometric system fusing various parts of the finger-based modality and satisfying the different objectives mentioned above. Therefore, the hypothesis would be the multimodal fusion of finger vein, and finger knuckle print by integrating different techniques and architectures. Several multi-types approaches have been developed, including finger vein and finger knuckle print using the proposed deep learning methods to ensure higher security.

On the other hand, Finger vein biometric systems gained a lot of attention in recent years due to the increasing demand for high-security systems [1]. Most of the existing finger vein capturing devices are not suitable for any research, development because of their private verification software. For that reason, we designing and developing a finger vein biometric system based on an Arduino and Raspberry Pi board.

In order to achieve the objectives detailed in the previously, some works are suggested based on finger-based biometrics modality. The contributions of this thesis are summarized as follows:

- **A review of finger vein biometrics authentication System [13]**

Sara DAAS, Mohamed BOUGHAZI, Mauna SEDHANE, Badreddine BOULDJEFANE, "A review of finger vein biometric authentication systems", IEEE proceeding in International conference on Applied Smart Systems (ICASS), Medea 2018.

- **Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion[14]**

Daas, Sara, Amira Yahi, Toufik Bakir, Mouna Sedhane, Mohamed Boughazi, and El-Bay Bourennane. "Multimodal biometric recognition systems using deep learning based on the

finger vein and finger knuckle print fusion." IET Image Processing 14, no. 15 (2020): 3859-3868.

- **Deep Convolutional Neural Network for Finger Knuckle Print biometrics identification:**

Sara DAAS, Yahi Amira, Badreddine BOULDJEFANE, Mohamed BOUGHAZI, Mauna SEDHANE, Bourennane El-Bay, "Deep Convolutional Neural Network for Finger Knuckle Print biometrics identification", 4th International Conference on Embedded Systems in Telecommunications and Instrumentation, Annaba, October, 28th-30th, 2019.

- **Finger Vein Biometric Scanner Design Using Raspberry Pi[15]**

Sara DAAS, Yahi Amira, Mohamed BOUGHAZI, Bourennane El-Bay. Finger Vein Biometric Scanner Design Using Raspberry Pi. International Journal of Computational Systems Engineering, Special Issue on: ISPR 2020 Recent Advances in Intelligent Systems and Pattern Recognition, 2021.

- **Finger-Based Biometrics Bibliometric Analysis:(Submitted Articles)**

.4 Thesis Outline

The thesis is structured as follows:

Chapter I reports the general context of the biometrics overview. Chapter II presents a multi-modal biometric systems description, types and their fusion concept. Chapter III presents a survey of finger-based modalities in which the state of the art of fingerprint, finger vein, and finger knuckle print modalities is detailed, and bibliometrics analysis is introduced. However, Chapter IV focuses on the deep learning overview. Chapter V depicts the proposed finger-based multi types fusion for finger vein and finger knuckle modalities. Also, description of proposed finger vein biometric system based on an Arduino and Raspberry Pi board. Finally, the last chapter concludes the thesis and discusses its most important results and contributions. Future works and perspectives are also put forward.

CHAPTER I

BIOMETRICS OVERVIEW

Contents

I.1	Introduction	8
I.2	Biometrics Technologies	8
I.2.1	Biometrics Definition	8
I.2.2	Biometrics History	8
I.3	Biometrics Modalities Types	10
I.3.1	Morphological Biometrics	10
I.3.2	Behavioural Biometrics	13
I.3.3	Biological Biometrics	15
I.3.4	Hidden Biometrics	16
I.3.5	Comparative Study Between Different Biometrics Modalities	18
I.4	Biometrics Applications	23
I.5	Biometrics Systems Process	26
I.6	Unimodal Biometrics System Architecture	26
I.7	Biometrics Recognition	28
I.7.1	Enrollment Biometrics Modes:	28
I.7.2	Verification Or Identification Biometrics Modes:	28
I.8	Biometrics Systems Performances Evaluation	30
I.9	Conclusion	34

I.1 Introduction

Nowadays, personal identity is becoming an essential task in governmental and private organization's procedures. Biometric technology increasing the level of protection of secret and confidential information. This chapter introduces some background information about biometric systems, including the biometric definition and history. Under a biometrics modality type, we moreover discuss the biometrics resource and study the comparative between them. Subsequently, we define the biometric application, process and modes. Eventually, we display the biometric architecture as well the performance evaluation metrics.

I.2 Biometrics Technologies

The modern world faces important challenges, particularly within information security, to confirm security, privacy and confidence. Individual user identification or verification is a critical element of various applications. Traditionally, user identification or authentication has been based on PIN, password, smart card, a badge or passport. These traditional methods of the user authentication, unfortunately, do not authenticate the user as such. One of the best solutions that have proven their effectiveness and efficiency in several fields is biometric.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [16, 17].

There are various important reasons to use unimodal biometrics such as [16]:

- **High security:** In comparison with other technology, such as encryption or smart card, several systems make it very difficult to attempted fraud.
- **Comfort:** By replacing traditional methods, such as a password, biometrics makes it possible to respect the essential rules of security. And when these rules are respected, biometrics prevent the controller from answering the many requests for password changes.
- **Security / Psychology:** In some cases, particularly for electronic commerce, the user has no confidence. E-commerce members need to convince consumers to make transactions. One means of biometric authentication could change consumer compartment.

I.2.1 Biometrics Definition

Biometrics is an emerging technique that allows us to verify an individual's identity by using one or more of his or her personal characteristics. It refers to a recognition technology that consists of transforming a biological, morphological, behavioural or hidden characteristic into a digital print [17–19].

The word "biometrics" came from Greek and it splits into two roots: "bio" means life and "metrics" -to measure [18].

Unimodal biometric refers to using a single biometric modality to authenticate or identify an individual and multimodal biometrics refers to using multiple biometrics modalities of the same individual to identify or authenticate that respective individual.

I.2.2 Biometrics History

The use of biometrics as a means of authentication dates back to the beginning of human civilization when the prehistorical man had used handprints as a signature for their paintings prior 31000 years ago. Another example of the beginnings of biometrics appeared in classical China through the use of handwritten signatures engraved on stamps by Chinese emperors to sign their official

acts. Joao de Barros, a XIVth century Spanish adventurer and researcher, mentioned the usage of fingerprints for business transactions by Chinese merchants. Besides, the hands and feet of young children fingerprint on paper using ink to identify them. It is often used today, which was one of the oldest biometrics in practice. The same process was used by the Babylonians to sign commercial contracts in the form of clay tablets. Many architects in Pre-Columbian America have left traces of their colourful hands on the walls of renovated caves [16, 18, 20].

The development of contemporary biometric technologies was observed in the late XIXth and early XXth centuries, as a result of the efforts of criminology experts and judicial agencies to identify and classify criminals. In 1879, the criminologist Alphonse Bertillon, developed a body measurement system, known as "Anthropometry", to identify criminals. He used multiple body measurements such as the height of the skull or the length of their fingers; this method confronted certain issues when it was realized; most people shared the same measurements and were therefore convicted by accident. By the late 1800s, known as finger printing was introduced known as fingerprinting; which used fingerprint patterns and ridges to identify humans, this trait was found to be specific for each and therefore more accurate in identifying.

Further, biometrics began more and more popular:

- In 1960s Automated fingerprint identification systems were developed.
- 1965 beginning of automated signature recognition research.
- In 1980, the idea of face recognition was developed. Also , the fist model of voice or speech biometric was produced.
- In 1980 the term biometrics began to be used to describe methods of automated human personal identification. The police experts had to manually cross-reference thousands of records in different regional files. It was not until 1987 that the process was automated and the creation of the automated fingerprint file.
- In the middle of 80th state callifornia began to collect fingerprints for driver license applications.
- In 1986 international biometrics association was created which is the foundation of the first biometric association.
- In 1990 the iris recognition technology was created.
- In 1992 the immigration system used fingerprints for the first time.
- In 1994 the United state installed the boarding system which was based on hand geometry.
- In 1997 the first biometric test centre was founded.
- In 2002 adoption of the first biometric standards.

Nowadays, thanks to the computing power of computers and data storage, combined with complex computer programs, biometric solutions are being widely established and implemented currently to provide people with high security. The recognition of the quality of biometric systems is increasing in recent years, and they improved a significant amount. A strategy to increase the use of biometric technologies is being implemented by governments, and also by the private sector to combat terrorism and fraud, given the huge security and economic challenges associated.

In Algeria:

- May 25, 2011, the Algerian authorities decided to use the biometric feature in the passport application file to issue a new biometric passport to comply with the new global standards and the requirements of the international civil aviation organization.
- In 2016 the issuance of the first Algerian national biometric identification card, which based on fingerprint and face traits.
- In 2019 the transfer of ordinary driving licenses to biometric driving licenses as part of the Algerian modernization plan and reinforcement of data information security.

I.3 Biometrics Modalities Types

Biometrics consists of defining the identity of a person using his biometric characteristics, which are called modalities, and which we classify among three categories: morphological, behavioural, biological and hidden [16, 20–22]. In the following Figure I.1, some modalities are illustrated.

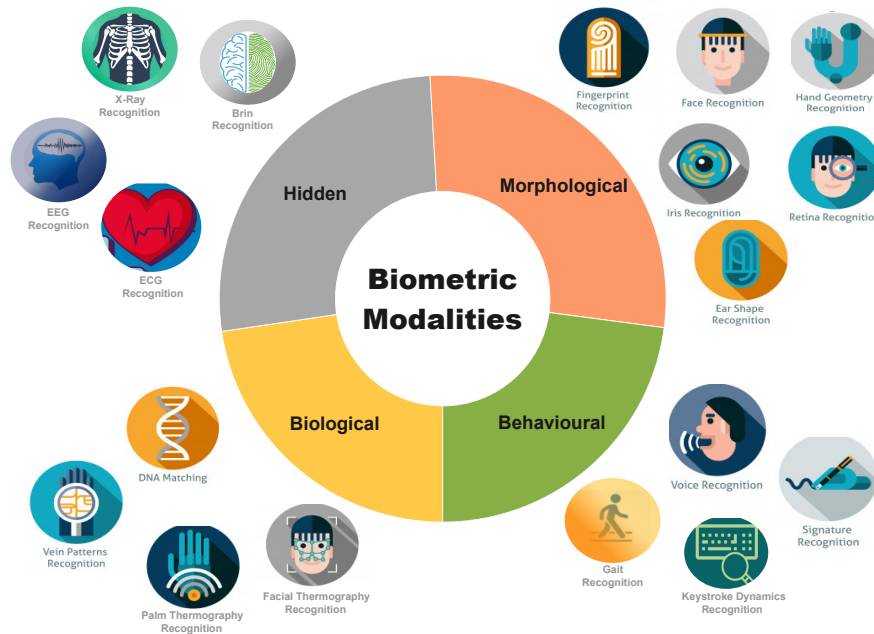


Figure I.1: Example of biometrics modalities

I.3.1 Morphological Biometrics

The morphological biometric methods are focused on recognizing physiological characteristics that are specific and permanent for each individual. It consists of using a part of the human body, such as fingerprint, face, iris,... etc. The measure of this modality is non-invasive (no physical contact) and well accepted by the general public because of its similarity with the human process recognition. In nowadays, the morphological traits considered as the promised biometrics because they have several advantages. This section presents a description of some popular biometric morphological features proposed in the literature [5, 16, 20].

- **Fingerprint:** probably the most usual form of biometrics available today. This modality is one of the oldest used and one of the best known to the general public. We can define fingerprints as follows: A **FingerPrint (FP)**(see Figure I.2) is an impression produced by

perspiration, grease, oil or ink present in the uneven crest lines contained in the upper part of each hand finger of a human being. These fingerprints are unique to each individual. Even perfect twins never have identical fingerprints [5, 16, 21].



Figure I.2: Example of fingerprint biometric modality¹.

- **Finger Knuckle Print:** The back of the finger, also known as the hand dorsal side or **Finger knuckle Print (FKP)** (see Figure I.3), can be very useful to recognise the person. The pattern of the finger bent is very specific and making this texture of the finger knuckle a distinctive biometric measure. The modality knuckle involves characteristics such as main lines, secondary lines and ridges that can be extracted from the low-resolution pictures [5, 20, 21].

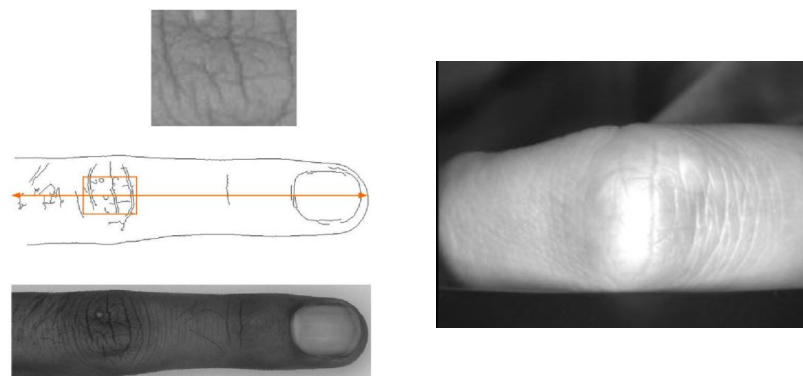


Figure I.3: Example of finger knuckle print biometric².

- **Palmprint / Hand Geometry:** Palmprint is the region between the wrist and fingers (see Figure I.4a), and it has many common points in with fingerprints in the extraction of characteristic points like principle lines, wrinkles, ridges, minutiae points, singular points, and the texture pattern. The acquisition of this modality is the major limitation of this modality; this sensor is very expensive compared to other modalities. Unlike other biometrics, the acquisition of hand geometry (see Figure I.4b) does not require any particular effort for the user, except often a particular positioning of the hand around "markers" to keep the same position between measurements. Despite this, this modality is not precise and presents a high risk of similarity between two people [16, 20, 21].
- **Face:** Face recognition occurs spontaneously in the daily life of human beings. It is the most common and most popular since it corresponds to what we naturally use to recognize a person. Facial authentication (see Figure I.5) is based on the shape and position of the eyes, eyebrows, nose, and mouth or the total examination of the facial picture as a number of popular figures presenting a face. It is challenging to compare facial photos obtained from

¹Image source: economictimes.indiatimes.com/fingerprints-and-fool-biometric-systems

²Image source: biometrics.manguet.org/finger

³Image source: homes.di.unimi.it/Palmprint

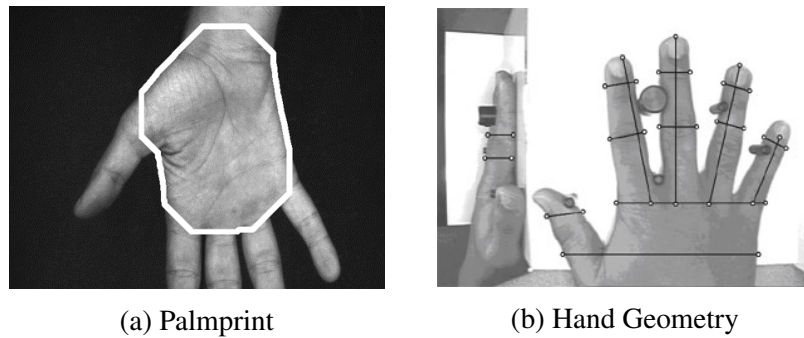


Figure I.4: Example of Palmprint / hand geometry biometric modalities³.

two various angles and under varying lighting conditions in a face recognition system. In addition, the face of a person may be altered through time. Both of these criteria allow the process of identity recognition unclear whether the face itself is still necessary to recognise an individual from a large number of identities [16, 20, 21].

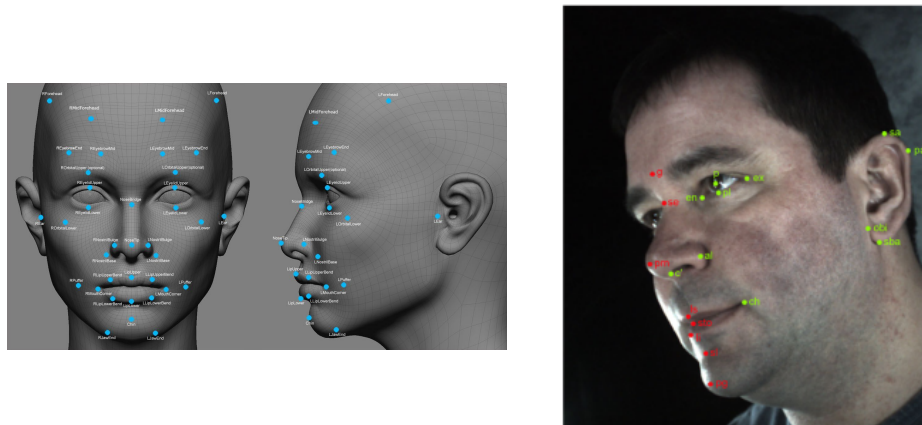


Figure I.5: Example of face biometric modality⁴.

- **Iris / Retina:** Both modalities are measured at eye level. The iris (see Figure I.6a) is present on the anterior side of the eyeball and resembles a "diaphragm" controlling the intensity of light captured, while the retina is on the inner side and is the sensitive organ of vision. The retina (see Figure I.6b) is measured by scanning the vascular network of the retinal membrane. This biometric technique is among the most reliable in terms of safety due to the stability of the retina over time, the very strong uniqueness of the retinal motif and the difficulty of falsification of the latter. On the other hand, it is not very attractive to the user due to the acquisition constraints requiring a stationary positioning close to the camera. The main sources of intrinsic disturbance to the subject area related to diseases such as glaucoma, diabetes or cataract. In the same way as for the retina, one of the advantages of measuring the iris is the great uniqueness of the motif [16, 20, 21].
- **Ear:** The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark position on the ear. The ear (see Figure I.7) is made up of standard anatomical features including the helix, the antihelix, the lobe, and the U-shaped interior groove between the ear hole and the lobe. The influence of random factors in the form of the ear can be observed by comparing the left and right ears of the same person:

⁴Image source: eforensicsmag.com/biometric-facial-recognition

⁵Image source: medium.com/biometric-blog/iris-recognition-vs-retina

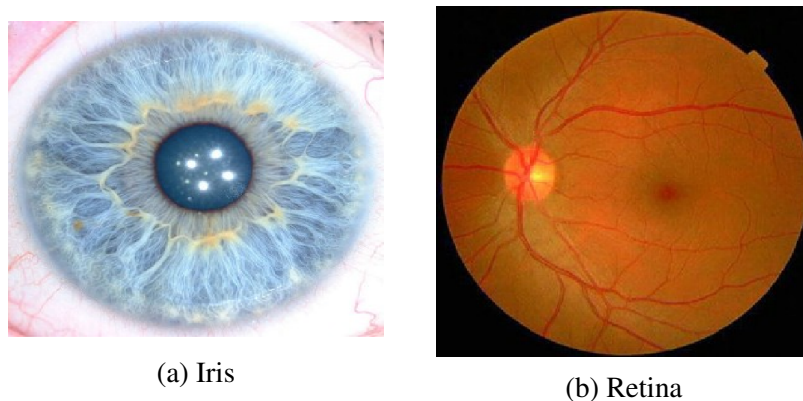


Figure I.6: Example of iris / retina biometric modalities⁵.

although they have similarities, they are not symmetrical. As for the face, this measurement is done remotely, but can easily be disturbed by the presence of hair or earrings [16, 20, 21].

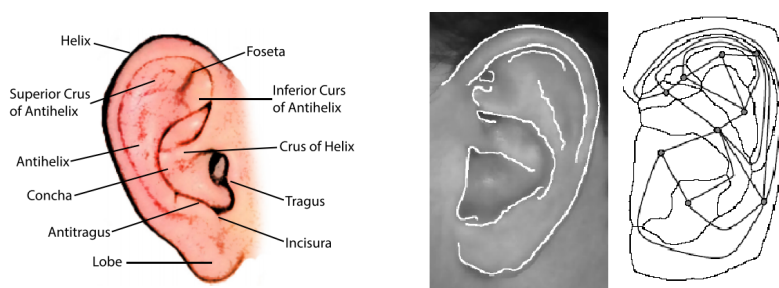


Figure I.7: Example of ear biometric modality⁶.

I.3.2 Behavioural Biometrics

It is a type of biometrics characterized by an attitude trait learned and acquired over time rather than a physiological characteristic. Consequently, behavioural modality may change over time. The compartmental biometric system is a basic feature obtained through consumer attitude like speech, gait, keystroke dynamics or signature. This section presents a description of some popular biometric behavioural features proposed in the literature [16, 23, 24].

- **Gait:** Gait refers to how a person walks (see Figure I.8). In a recognition system by gait modality, one inquires to identify an individual by walking and moving while analysing video images of the applicant walk. So it's a remote identification modality. People show different traits while walking like body stay, the distance between the two feet, the joint's position, such as the knees and ankles and the moving angles, identifying them. The gait biometric systems are affected by the environment's change and the psychological state during the measurement.
- **Voice:** the recognition of voice or speech recognition is a technology in which sounds, sentences and terms voiced by human beings are converted into electrical signals (see Figure I.9). Voice is noticed as a distinctive trait of every human and uses various voice characteristics such as tone, duration and volume to distinguish one person. A person's voice varies with time due to age, medication, mental state, etc. Speech is often not distinguishable, and may not be useful for authentication or distinguishing purposes [24, 25].

⁶Image source: [semanticscholar.org/paper/ear-biometrics](https://www.semanticscholar.org/paper/ear-biometrics)

⁷Image source: [intechopen.com/books/gait-recognition](https://www.intechopen.com/books/gait-recognition)

⁸Image source: [securitybrief.com.au/story/voice-biometrics](https://www.securitybrief.com.au/story/voice-biometrics)

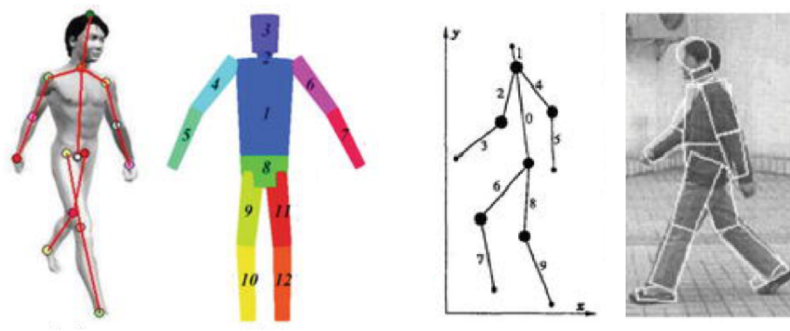


Figure I.8: Example of gait biometric modality⁷.



Figure I.9: Example of voice biometric modality⁸.

- **Signature:** This modality is known as the way of signing one's personal name, and it is a characteristic of that identity (see Figure I.10). Signature-based recognition system can be operated either in static mode or a dynamic way to sign your name through an optical scanner or a camera. The group is known as "off-line". The dynamic mode is known as "on-line" where users sign using a digitizer tablet, which records the signature in real-time. The devices can also be operated on a tablet, or by using a stylus on a smartphone [21].

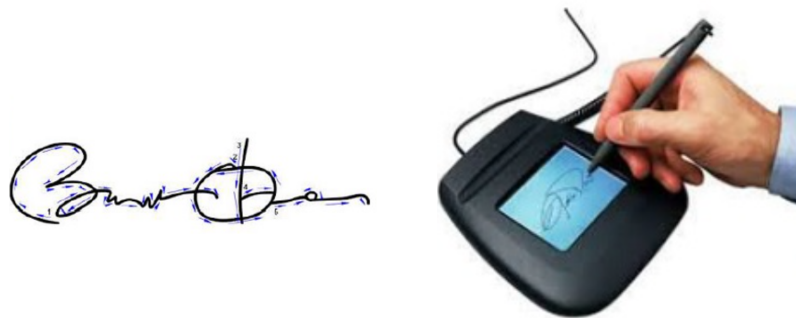


Figure I.10: Example of signature biometric modality⁹.

- **Keystroke dynamics:** The dynamics of keyboarding are a behavioural characteristic of each individual. It is, in a way, the transposition of graphology to electronic means (see Figure I.11). The characteristics measured are the flight time (time between two different keystrokes), the pressure-time (time between pressure and the release of the same key), the complete duration of a sequence, the frequency of errors, the use of the numeric keypad, the strength of the keystrokes (for equipped keyboards) and how to use capital letters. Measurements are disturbed by the subject's emotional state, posture, type of keyboard, etc [21, 23].

⁹Image source: tutorialspoint.com/biometrics/behavioral-modalities

¹⁰Image source: tutorialspoint.com/biometrics/behavioral-modalities



Figure I.11: Example of keystroke dynamics biometric modality¹⁰.

I.3.3 Biological Biometrics

The biological characteristic is a biometric trait-based mainly on the anatomy or detailed physiology of an individual. This involves characteristics such as DNA, facial or palm thermography and vein shape, etc. This section presents a description of some popular biometric biological features proposed in the literature [16, 20, 21].

- **DNA:** In all cells, **Deoxyribo Nucleic Acid (DNA)** is a biological macromolecule containing all genetic information (see Figure I.12) allowing the development, functioning and reproduction of living beings. The DNA extracted from any biological sample from a person (blood, saliva, skin or hair fragment, etc.) is unique for each person used in the form of identification. Most commonly used in legal medicine, this method isolates and compares sequences of DNA segments of different individuals, with a risk of similarity between two people of less than one per cent billion. Very expensive in processing time and equipment, this method is not real-time and inconvenient in the collection of samples [16, 20].



Figure I.12: Example of DNA biometric modality¹¹.

- **Facial / Palm Thermography:** Biometrics thermography detects heat patterns from the skin by the branching of blood vessels. Such patterns, named thermograms, are particularly distinctive such as facial and palm biometrics (see Figure I.13). Even identical twins have different thermograms. Thermography operates much like face recognition, except that the pictures are taken with an infrared sensor. Also in warm light or complete darkness, infrared systems run reliably [16].
- **Vascular:** Vascular modality is a recognition system for identifying a person's unique vein patterns (see Figure I.14). Veins as a biometrics tool contain the blood vessels measurement

¹¹Image source: yourgenome.org/what-is-a-dna-fingerprint

¹²Image source: slideplayer.com/Biometrics Kayla Burke



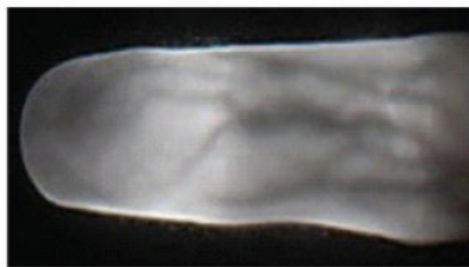
(a) Facial thermography



(b) Palm thermography

Figure I.13: Example of thermography biometric modalities¹².

methods on the back of palm or a single finger of a hand. The technology takes an image of a person's vein pattern under their skin. When a person's hand is placed on the scanner, they are mapped with **Near-infrared (NIR)** light. The red blood cells in the veins absorb the radioactive rays as they pass through the hand, whereas the remaining arteries and veins show up as white [26]. Various advantages and applications exist today for **Finger Vein (FV)** technologies [27, 28].



(a) Finger vein



(b) Palm vein

Figure I.14: Example of vascular biometric modalities¹³.

I.3.4 Hidden Biometrics

These modalities are a particularly robust biometric concept. In comparing the classical biometric modalities based on the obvious characteristics of the human being, the hidden modalities instead consider the intrinsic and non-visible characteristics of the human body. Any physiological signal or human organ is potentially a candidate for biometric applications. Hidden biometrics use data generally used in the medical field. The techniques are ideal toward spoofing and identification, but they need good processing. This section presents a description of some popular biometric hidden features proposed in the literature [1].

- **ECG / EEG:** Growing interest has currently been dedicated to the study of physiological measures, which comprise brain and heart electrical stimulation. As potential indicators of

¹³Image source: computerscijournal.org/biometric-technology-based-on-hand-vein

biometric characteristics, **Electrocardiography (ECG)** and **Electroencephalography (EEG)** have been widely researched [1, 28]. The **ECG** is a signal representing the activity of the heart. It is mainly used in clinical applications to diagnose cardiovascular disease. The **ECG** signal is characterized by beating shape, and it consists of five typical waves, namely P, Q, R, S, and T or sometimes U wave (see Figure I.15). **ECG** biometrics have been the subject of several studies which are based on signal processing analysis [1, 28]. The **EEG** is used to calculate fluctuations in the brain's activity by electrodes placed on the brain. It is the voltage difference that creates the tracks known as brain waves (see Figure I.15). Every individual has a specific neural network pattern that defines their activity in the brain. This renders it impossible to forge an **EEG** biometric system and is therefore ideal for use in high-security systems [1].

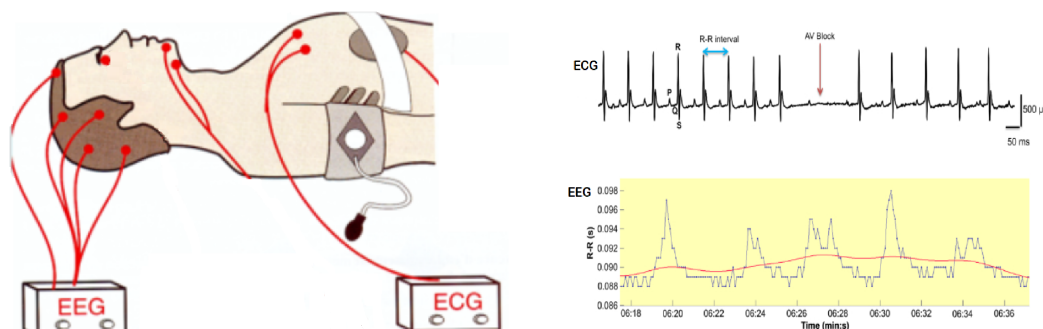


Figure I.15: Example of **ECG / EEG** biometric modalities¹⁴.

- **Brin:** The brain biometrics are to characterize the human brain through 2D and 3D **MRI** images. In medical applications, **MRI** is a non-invasive radiography technique used to visualize 2D or 3D images of human body organs with relatively high resolution. From the 2D **MRI** images, it is possible to reconstruct the 3D image brain for texture information (see Figure I.16). Thus, the brain volumetric characteristics and the number of parameters extracted from a 3D brain image can define what we call brain code or bar code of the brain, which can be very useful for the identification [1, 21].

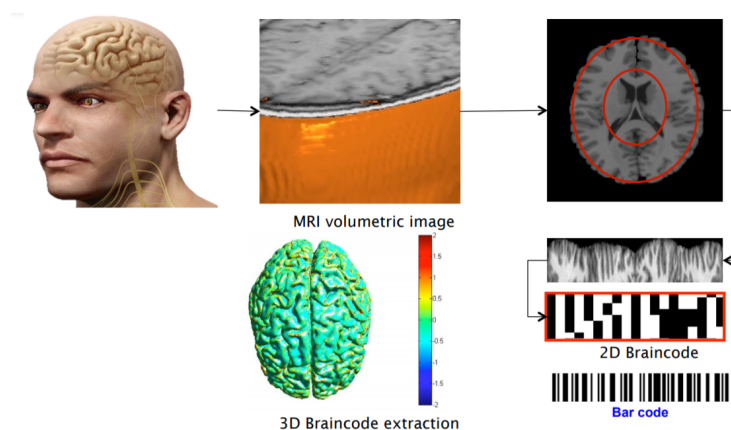


Figure I.16: Example of brain biometric modality¹⁵.

- **X-Ray:** The X-Ray is radiography based on the transmission imaging technique. It allows obtaining a whose contrast depends on both the thickness and the crossed structures attenuation coefficient. X-Ray is used in medical radiology, industrial radiology and radiotherapy.

¹⁴Image source: unt-ori2.crihan.fr/unsfp/ECG-EEG

¹⁵Image source: biometrie.sciencesconf.org/hidden-biometrics

Medical radiography allows the development of 2D images of human bones. With this type of images, bone structures are clearly accentuated [1, 21]. The application of this type of technology in biometrics is conceivable in using X-Ray images of the hand, for example (see Figure I.17a) where the aim is to characterize the phalanges using some image processing tools. Furthermore; the dental X-Ray (see Figure I.17b) composes distinctive features (crown, filling and bridge) for each individual which can be considered a biometric imprint.

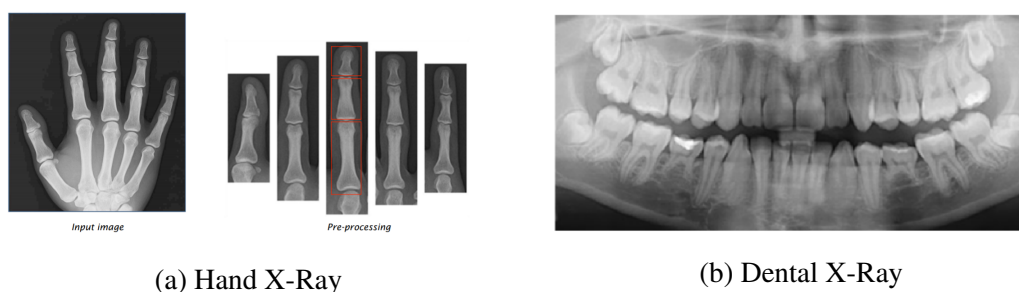


Figure I.17: Example of X-Ray biometric modalities¹⁶.

I.3.5 Comparative Study Between Different Biometrics Modalities

After going over all the various biometric modalities, it is able to see that each of the biometrics had some advantages, disadvantages and that some applications require choosing one modality over another. Each biometric modality has its own strengths and weaknesses, the choice generally depends on the area of application and sometimes on the population intended to be identified. Any characteristic to be considered as biometric modality, it must satisfy the following properties:

- **Universality:** All people to be recognized must possess it.
- **Uniqueness:** The possibility of not having correlations in various people’s measurements of the same modality.
- **Permanence:** Indicate if the trait remains unchanged over a given period.
- **Collectability:** The level of difficulty in collecting, measuring and performing the modality.
- **Acceptability:** Indicates if the individual accept to use the modality without objection.
- **Performance:** Characterizes the robustness, reliability and speed of the measurement.

Biometric modalities can exhibit some mentioned properties, but with varying levels (Low, Medium or Low). A summary of comparing biometric modalities presented in Table I.1 extracts from the work of [16, 21, 29]. The comparison shows that no modality is perfect for all applications and can be adapted to particular situations.

Rather than just comparing the performance of biometrics systems, It is necessary to consider the environment, the use, the ease of record, and the ease of analysis, storage and recognition. Each biometric technology has advantages and disadvantages, acceptable or unacceptable depending on the application, so not all solutions are competitive; they do not offer the same security levels or the same ease of use [22].

The advantages and disadvantages of different biometric techniques are presented in the following Table I.2 [22]:

¹⁶Image source: biometrie.sciencesconf.org/hidden-biometrics

Table I.1: Comparison between biometric modalities

Modality	Universality	Uniqueness	Permanence	Collectability	Acceptability	Performance
Fingerprint	Medium	High	High	Medium	Medium	High
Finger Knuckle Print	Medium	High	High	Medium	Low	High
Palmprint	Medium	High	High	High	High	High
Hand Ge-ometry	Medium	Medium	High	High	High	Medium
Face	High	Low	Medium	High	High	Low
Iris	High	High	High	Low	Medium	High
Retina	High	High	High	Low	Low	High
Ear	High	Medium	Medium	Medium	Medium	Low
Gait	Medium	Low	Low	Medium	High	Low
Voice	Medium	Low	Low	Medium	High	Low
Signature	Low	Low	Low	High	High	Medium
Keystroke Dynamics	Low	Low	Low	Medium	High	Low
DNA	High	High	High	Low	Low	High
Thermography	Low	High	Low	Medium	Medium	Low
Vascular	Medium	Medium	High	Medium	Low	High
ECG /EEG	High	High	Medium	Low	Medium	Medium
Brin	High	High	High	Low	Low	High
X-Ray	High	High	Medium	Low	Low	High

Table I.2: Advantages and disadvantages of different biometric techniques.

Modality	Advantages	Disadvantages
Fingerprint	<ul style="list-style-type: none"> -The most proven technology technically and best known of the great public; -Small size of player for easy sound integration in most mobile phones and PCs applications; -Low cost of readers due to new "Silicon chip" type sensors. 	<ul style="list-style-type: none"> -Need the cooperation of the user (correct laying of the finger on the reader); -Some systems may accept a finger copied image or cut finger (live finger detection prevents this type of spoofing); -Difficulty reading: sensitivity to alterations that may occur during the life (scratch, scar, ageing or other) and to individual variations (temperature, humidity, dirt).
Hand Geometry	<ul style="list-style-type: none"> -Good user acceptance; -Straightforward to use; -The result is independent of the humidity and cleanliness of the fingers; -Less expensive technique. 	<ul style="list-style-type: none"> -Too bulky for use on the desk, in a car or phone; -Risk of false acceptance for twins or members of the same family, - The shape of the hand where fingers change with ageing hinders long-term measurement.
Iris	<ul style="list-style-type: none"> -The iris is not modifiable even with surgery; -The irises are unique and differ even for identical twins; -The large amount of information contained in the iris; - Iris challenges to forge; - Drawing of the iris independent of the genetic code; - Iris hardly varies over a lifetime. 	<ul style="list-style-type: none"> The iris are easily visible and can be photographed; - The security issue is related to the checks performed during shooting; -The method's psychologically invasive aspect; - Problems may arise during measurement (reflection, the variation of pupil size, etc.); -A photo or contact lens reproducing the iris image may affect reliability.
Retina	<ul style="list-style-type: none"> Retinal imprint is less exposed to injury (cut, burn); -Very difficult, impossible way to copy; -Retina is different in identical twins; -The retina is stable during the life of an individual; - very effective; -Vascular map specific to each individual is different, even between twins. 	<ul style="list-style-type: none"> -Intrusive system, the eye should be placed close to the sensor; -Poor public acceptance (the eye is a sensitive organ); -Higher cost than other technologies; -Technical constraining for participants (measurement at a short distance [a few centimetres] from the sensor); -Invasive technique not widely accepted by the public; -The appearance of blood vessels may be altered by disease or age.

Face	<ul style="list-style-type: none"> - Photo camera facial-scan is known to be the most straightforward and least restrictive technique; -Its main advantage is its non-intrusive side; -Comparable to being photographed, it is relatively more socially accepted; - The only technique can be used without the consent of the person. - Easy to use. 	<ul style="list-style-type: none"> -Face recognition does not work well include low lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low-resolution images; -The distance to capture the face image is not uncomfortable; -Another serious drawback is that many systems are less effective if facial expressions vary; - Even a big smile can make the system less efficient.
Voice	<ul style="list-style-type: none"> Biometric technology is easy to implement; -Allows securing a telephone conversation; -Generally very well accepted as the voice is a natural signal to produce; - One of the only techniques to recognize someone remotely; - used for telephone recognition. 	<ul style="list-style-type: none"> -Voice is not a permanent attribute (it changes, of course, with age); -Biometric technology vulnerable to attacks; - It is straightforward to record or reproduce the voice; - Requires excellent audio quality; -Sensitive to ambient noise; -Voice changes over time and maybe impaired (cold, fatigue, high emotion, etc.); -Low level of differentiation between two voices.
Signature	<ul style="list-style-type: none"> -Written signature on a document can be kept of certain documents; -Action that involves (responsibility) the applicant; - Easy to use; -Highly accepted by users. 	<ul style="list-style-type: none"> -Need a graphic tablet; -Sensitive to the emotions of the individual; -Not used for external access control for example; - The signature is changing; -A combination of data (speed of execution or other) is required.
Vascular	<ul style="list-style-type: none"> -Very high level of security, so far no way to defraud; -Biometrics called "no trace"; -Biometrics without badges and code. 	<ul style="list-style-type: none"> -Use only indoors; -Light-sensitive sensor, however manufacturers have brought protections limiting the problem; -Proper identification of the user requires the finger to be correctly placed on the sensor.
DNA	<ul style="list-style-type: none"> -A very high precision; -It is impossible that the system made errors; -It is standardized. 	<ul style="list-style-type: none"> -Very expensive.

Keystroke Dynamics	Non-intrusive, natural gesture for an individual; -No additional hardware, simple software is enough; -Fast implementation for a large number of users; -Significantly reduces the need for password change and the solicitation of computer services; - Allow a person to be identified remotely from their computer.	-The use of a keyboard of a different format AZERTY, QWERTY, causes a refusal of its own password; -Health and fatigue can affect the way keys are struck; - Sensitivity to the difference between keyboards.
--------------------	--	---

A brief comparison of the most commonly used biometric techniques presented in both Table I.1 and Table I.2 performs that it is possible to select an appropriate approach according to the requested application constraints. The applicability of a specific biometric technique depends massively on the conditions of the biometric area of application. However, there are several biometric modalities, but there is no perfect biometric system. According to the International Biometric Group (IBG) ¹⁷, different biometric techniques called Zephyr™ Analysis have made a comparison. The results of this comparison are illustrated in Figure I.18. This comparison is based on four critical criteria [30]:

- **Intrusiveness:** level of understanding by the user of the test as intrusive;
- **Accuracy:** effectiveness of the method (the ability of person recognition);
- **Cost:** price of the technology (readers, sensors, etc.);
- **Effort:** the required effort from the user.

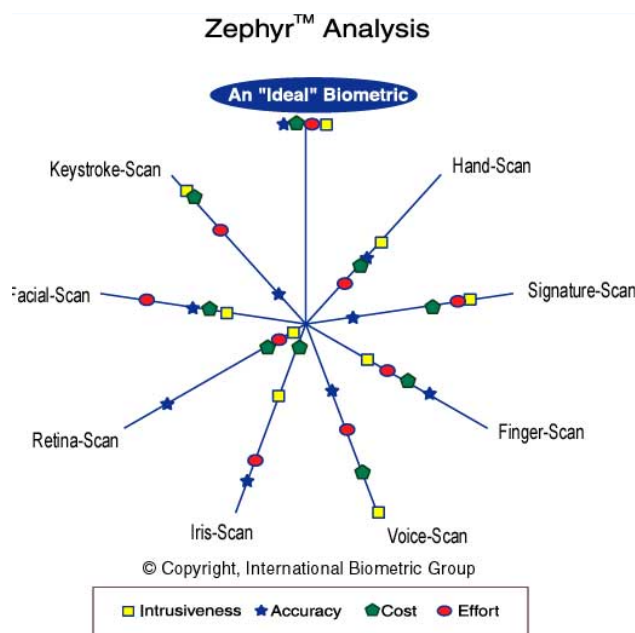


Figure I.18: Comparison of different modalities according to Zephyr™ Analysis¹⁸.

¹⁷Official IBG website, URL:<http://www.ibgweb.com/>

¹⁸Image source: biometrie-online.net/technologies/fonctionnement

I.4 Biometrics Applications

Therefore, biometric techniques bring comfort, simplicity and a high-security level to users while presenting the advantage of being coupled with existing conventional systems (badge, code, etc). Indeed, whether it is to secure physical access (a building, a room, a safe, etc.) or logical access (computer data), biometrics has already proven itself, and its use is constantly growing. Many systems are developed on the market, intended for the consumer electronics or the private sector [31]. They offer both unimodal solutions and multimodal(middleware) solutions. Figure I.19 shows the size of the current biometric adoption and trends in the markets, where the finger scanner is still most trends biometrics [31].

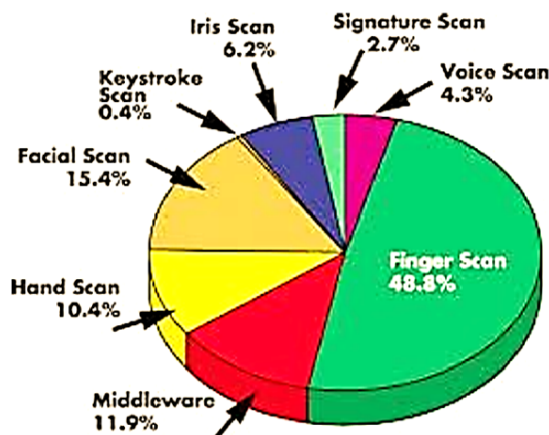


Figure I.19: Market size of different biometric technology¹⁹.

– Consumer electronics biometric market:

Biometrics are already well accepted by the general public and becoming a part of the daily life of individuals around the world due to the modernization of the authentication systems [32]. Also, Through biometrics integration for mobile devices(*smartphones*) and *tablets*, biometrics are widely known in many domains such us, social networks, home security and automotive technology (see Figure I.21).

The emergence of mobile biometrics has stimulating innovative technologies and techniques in the area of personal authentication and identification [33]. The world's first biometrics in mobile systems is fingerprint phone of a *Pantech* GI100. The phone was lanced in 2004 where the fingerprint sensor took the place of the OK button [34]. The current research for this modality embedded on the *smartphone* concerns the integration of a fingerprint sensor covering the entire *touchscreen*, making it, then able to measure this modality in a totally transparent way continuously [33]. Almost all *smartphone* have recently carried a fingerprint recognition sensor as expected by *IDEX Biometrics* [35] fingerprint sensors positioned for success in the mobile biometrics market. Figure I.20 shows the strong demand for phone fabrication companies (a billion of fingerprint sensor units are required).

Similarly, face recognition can be used by any *smartphone* because it does not require any particular sensor [33]. The world's first face recognition biometric for*smartphones* is of OKAO vision face recognition sensor. In 2005, OMRON corporation announced the ability to recognize and verify the user's authenticity through face recognition [34]. However,

¹⁹Image source: ijarce.com/biometric-technology-market-size

²⁰Image source: [IDXbiometric/IDEX Business Update](http://IDXbiometric/IDEX-Business-Update)

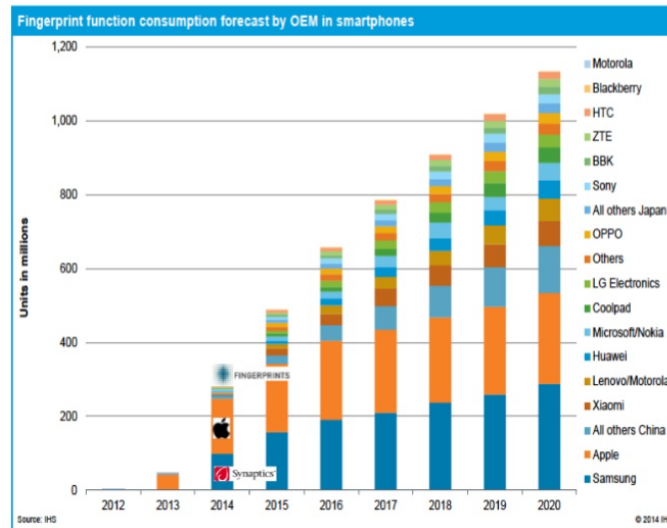


Figure I.20: Example of mobile biometrics market²⁰.

the face recognition technologies developed. In 2017, the *Apple* company proposed a significant step advancing for this modality, making it possible to perform face recognition in three dimensions with a simple *smartphone* at a distance of 20 cm (named *FaceID*) [20]. The same year (2017), the company *Samsung* proposes integrating an iris scanner on these *smartphones*. Based on multimodal biometrics principle, the fingerprint and iris recognition sensors are incorporated into the same *smartphone*. The iris sensor with an infrared camera and a single infrared LED projector, to acquire an infrared image of the eye region of the subject under any lighting condition [20]. There is, therefore, a wide range of biometric devices dedicated to the consumer electronics embedded in our *smartphones*. With mobile devices incorporating multiple solutions for different modalities, it is up to the user to consider which method seems most appropriate. Indeed, for the exponential development of biometric technology in mobile systems, LG Electronics announced in 2019 the first mobile exhibiting vascular biometric recognition [28], integrated using the palm vein modality (LG G8 hand ID). Biometrics are becoming more relevant due to the rapid growth in mobile devices and social media. The social network companies started adopting biometric technologies to attract even more users and deal with security issues that have risen recently. For example, *Facebook* social networks company has employed a tool, "tag suggestion" based on facial recognition that scans uploaded images and identifies network friends by suggesting [32].

Biometric solution available also to home security systems. As an example, the devices of the *Netatmo*, which is based on face recognition biometric [36]. The sensor is connected with objects for home monitoring communication functions using two cameras with a *smartphone*. The camera indoor identifies the family members or unidentified persons on another side the camera outdoor capture the proximity of car, people or animals [20]. Another home application, the biometric door Lock with the fingerprint. There is a range of fingerprint biometric door locks for commercial as well as domestic applications [37]. Moreover, fingerprint biometric sensors are attracted and very promising with the advancing automotive technology. There are already cars that can only be unlocked with the drivers fingerprints. Also, biometrics-based consumer electronic devices are standalone products such us time attendance device and access control systems. Companies that integrate biometric technology into existing consumer devices are included in this category. In the consumer electronic biometrics market, the *intelligence informatics solution*



Figure I.21: Example of consumer electronics biometrics market

(S2I Algeria) company offers biometric solutions for access control, to protect property and people with a simple and adaptable software named ELBASSMA; and a complete system of biometric clocking for time management of employee attendance using fingerprint or face biometrics [38].

– **Private biometric market:**

The recent years witnessed an important deployment of biometric technologies for reliable individual identification in public as well as the private (industrial) sector. Biometrics are widely known in many domains such as, defence, government, banking, and healthcare applications (see Figure 1.22).

Biometrics used in defence provide numerous applications for securing variant military tasks or activities [39]. In the main, two biometrics applications in defence seem to be essential: border control and criminal investigation (terrorist identification). Moreover, the government needs to deal with all of its citizens for their identity and demographic data to ensure security and provide other facilities [39]. So, the application of biometric technology is significantly used in the government sectors. Governments of almost all countries are using the technology to ensure fair distribution of services and resources to its citizen [39]. For example, the Algerian government using the biometric technology for subject identification in the passport, national identification card and driver's license [40].

Similarly, banking and finance is an important sector to use biometric. Banks are using biometrics to develop identification controls that combat fraud, make transactions more secure, and enhance the customer experience [32]. Biometric payment offers high security for financial institutions. For instance, the first steps towards biometric banking for payment applied for the biometric card [32]. Simply put, whenever customers want to pay via card, they have to put their fingers on the card sensor to authenticate themselves and allow the payment (see Figure 1.22). The healthcare industry is adopting various biometric technologies. Hospital systems are designed to automatically time out and force the users (doctors and nurses) to log on repeatedly between shifts [32]. Soon, healthcare industries will employ biometric technologies to identify a patient. Blood banks in the United States are starting to use fingerprints of a donor to follow the federal regulations that need precise verification of each donation [32]. Biometrics will also replace patient *wristbands* or *barcodes* currently used to identify each patient for their medication or treatment. Using biometrics like fingerprints and palmprints will also improve the ability to deal with medical emergencies

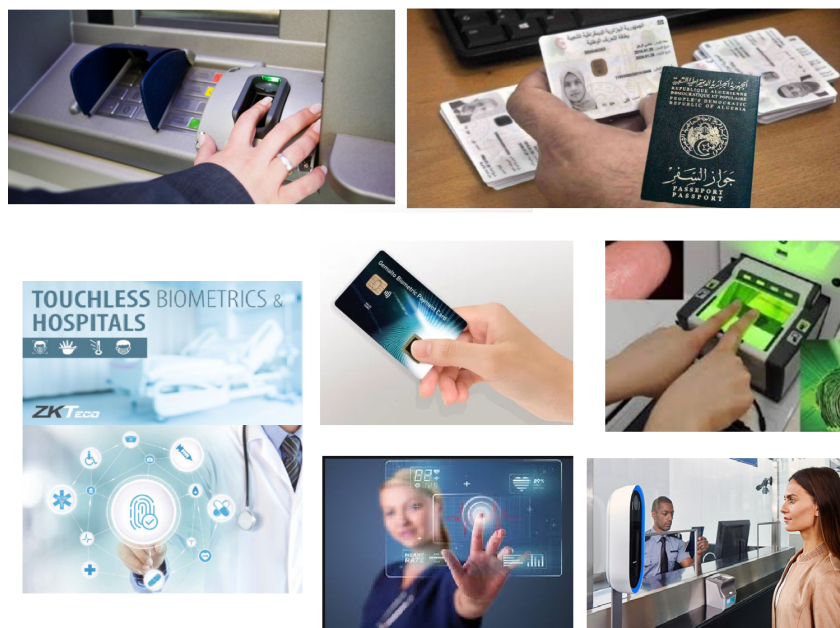


Figure I.22: Example of consumer electronics private biometrics market

where patients are unconscious by quickly checking their identities along with their medical histories [32].

Biometric technologies are rapidly becoming a part of the daily life of individuals around the world. Figure I.23 [41] shows the global biometric technology market report and estimation, where the major biometric sensors are ordered from Units State. The future of biometric trends will be increasingly used to cater to the safety and security needs.

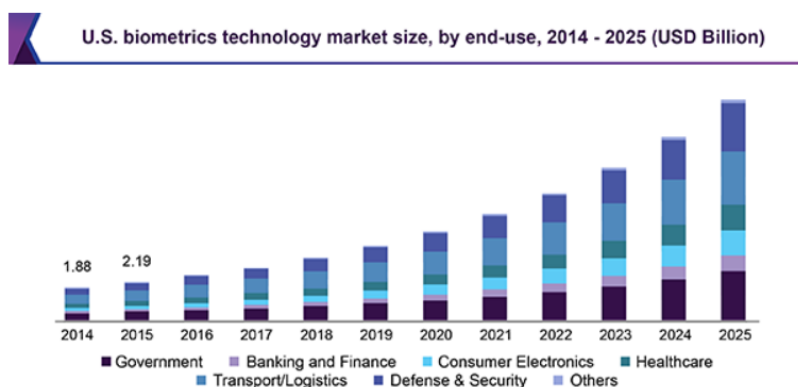


Figure I.23: Example of global biometrics technology market size²¹.

I.5 Biometrics Systems Process

I.6 Unimodal Biometrics System Architecture

The standard biometric system architecture consists of four main processes for the recognition of individuals from their biometric features, some of them are common for enrollment and Identification or Verification phases. The modules include the collection of data (data acquisition &

²¹Image source: [grandviewresearch.com/industry-analysis/biometrics-industry](https://www.grandviewresearch.com/industry-analysis/biometrics-industry)

preprocessing) followed by the extraction of the features using a function extraction algorithm. After that, the matching is then performed on the basis of the features extracted. The person shall be then accepted or rejected in using decision rule (See Figure I.24).

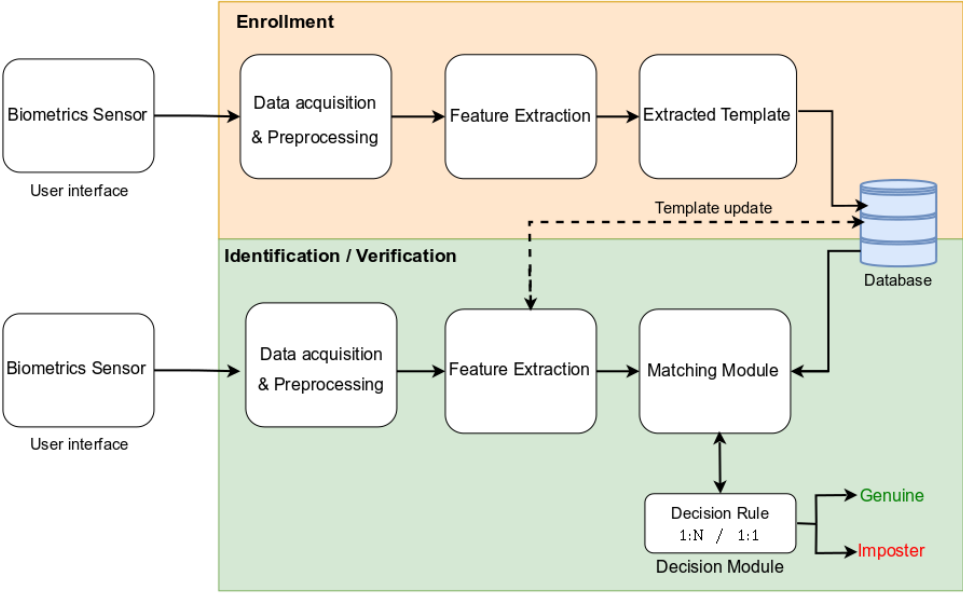


Figure I.24: Biometric systems structure

1. **Data acquisition process:** This module collects the raw biometric data using biometrics sensors and converts the information to a digital format. The quality of the data captured typically depends on the interface’s intuitiveness and the sensor’s characteristics. After that, preprocessing treatment will be used if it is necessary (eg. the ROI extraction and enhancement).
2. **Feature Extraction process:** This module is responsible for extracting feature values of a biometric trait by applying the feature extraction algorithm. For instance, if hand geometry is used as a biometric sample, then feature values would include the width of fingers at various locations, the width of the palm, the thickness of the palm, the length of fingers, etc. The outcome of this step is a biometric template that includes only the discriminatory information necessary for recognizing the person. Typically, a biometric template is unique for each individual and relative invariants. The obtained biometric template is then stored in the system database module, which the biometric system uses to store the enrolled users’ biometric templates.
3. **Matcher process:** In this step, a classifiers or matching algorithm compares the new biometric template to one or more templates kept in data storage and creates a “match score”. The matcher module also encapsulates a decision-making module, in which a user’s claimed identity is confirmed verification or a users’ identity is established identification and predicated on the matching score.
4. **Decision process:** The user’s identity is either established, or a claimed identity is accepted or rejected. This is executed based on the results of the matching modules. This can either be automated or human-assisted.

I.7 Biometrics Recognition

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual. Depending on the application context, The structure of a biometric system consists of two different phases: enrollment and verification Or identification modes, as shown in Figure I.24.

In addition, biometric recognition systems are classified into two main categories: *on-line recognition* and *off-line recognition* [16].

- **Off-line recognition:** is a system process that used biometric image modalities captured previously.
- **On-line recognition:** is a system process that used biometric image modalities acquired in real-time.

I.7.1 Enrollment Biometrics Modes:

is a common stage for both verification and identification modes. It is the initial phase where a user's biometric data is registered for the first time in the system. Over this phase, one or more biometric modalities are captured and stored as templates in the database. This phase is very essential since it impacts, later, the whole recognition process. In fact, the quality of enrolled data is essential for ulterior identification phases because acquired data are considered as references for the person. The collected information is stored in a central database where it is labelled with a user identity (e.g. name, PIN) to facilitate recognition (See Figure I.25) [42].

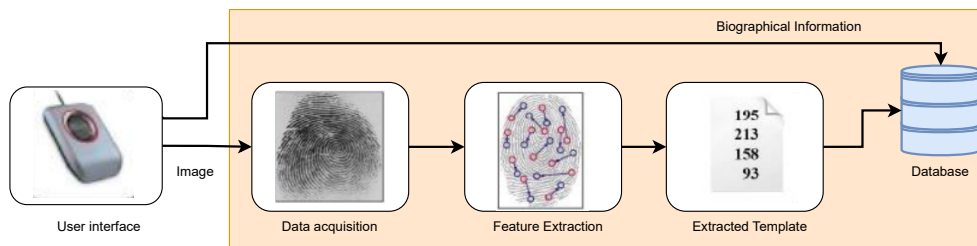


Figure I.25: Example of Enrollment biometric system

I.7.2 Verification Or Identification Biometrics Modes:

A biometric system may operate either in verification mode or identification mode.

1. **Verification Mode:** is *one – to – one* (1 : 1) matching process, the system verifies the claimed identity by comparing it with the stored one (See Figure I.26). If the matching score of the claimed identity greater than a predefined threshold $\alpha \in (0, 1)$, then the claimed identity is accepted as *genuine*, otherwise, the claimed identity is rejected as an *imposter*. Thus, authentication process able operate based on verification mode and could be implemented as a binary classification problem. The decision rule is calculated and based on the following formula [16]:

$$R(u_i) = \begin{cases} \text{Genuine} & \text{if } R(u_i) > \alpha \\ \text{Imposter} & \text{otherwise} \end{cases} \quad (I.1)$$

where $R(u_i)$ represents the authentication score for a user u_i and is calculated by the classifier, and α represents a predefined threshold $\in (0, 1)$.

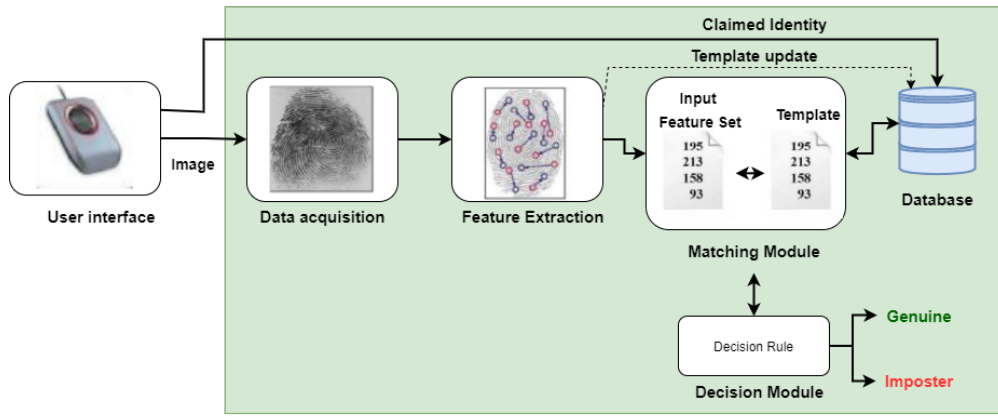


Figure I.26: Example of verification biometric system

2. **Identification Mode:** is *one – to – All* (1 : N) matching process, the system recognizes the presented biometric sample by comparing it with all or many stored templates (See Figure I.27), where the matching stage estimates the user identity based on the highest matching score and a designated threshold (i.e., there is multiple matching scores will be generated, one for each user, in which the highest score will be selected) [16].

Considering u_i the biometric features extracted by the system when a user u is in front of it. So, identification involves determining the identity of $I_k, k \in [1, 2, \dots, N]$ where I_1, I_2, \dots, I_N are user identities previously enrolled in the system, and I_0 indicates an unknown identity. The identification function f can be defined by:

$$f(u_i) = \begin{cases} I_k & \text{if } \text{Max}_k \{f(u_i)\} \geq \alpha, k = 1, 2, \dots, N \\ I_0 & \text{otherwise} \end{cases} \quad (I.2)$$

Such biometric identification system can work into two modes of identifications: *open – set*

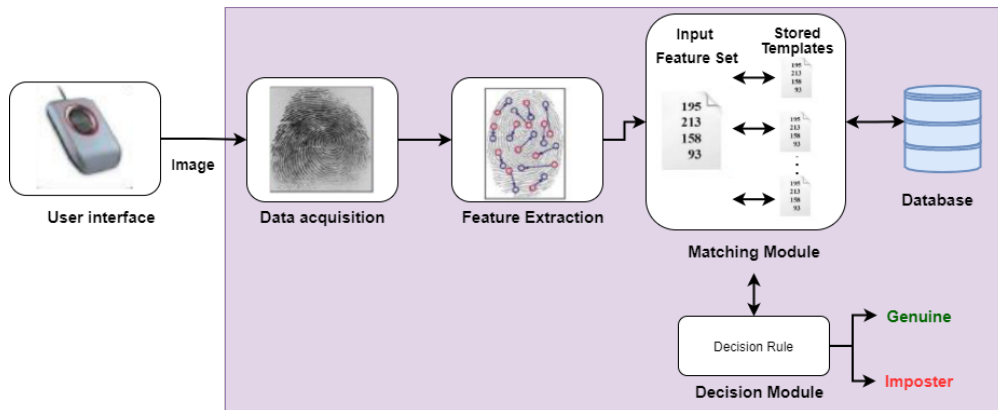


Figure I.27: Example of identification biometric system

and *closed – set* identification:

- **Open-set identification:** It is unknown whether the individual presented to the biometric system for recognition has enrolled in the system or not. Therefore, in this case, the system needs to decide whether to reject or recognize him as one of the enrolled individuals [16].
- **Closed-set identification** Any individual presented to the biometric system for recognition is known to be enrolled in the system; thus, no rejection is needed in principle unless the input biometric trait's quality is too low to process[16].

I.8 Biometrics Systems Performances Evaluation

Evaluation of the performance of a biometric system is an essential process in the architecture of a biometric recognition system. This section describes techniques for biometric analysing systems and various metrics and graphs demonstrating how biometric systems work. As previously mentioned, it is known that biometric systems divided into two mode, namely verification and identification. It makes sense to differentiate between these two mode herein as they will significantly impact performance evaluation. There are many solutions to image classification problems [5] in the field of biometrics. The methods presented can be used for classification problems with two or more classes, and the behaviour of classifiers depends on the number of samples per-class and their composition. Therefore, the selection of the most appropriate method is dependent on the constraints of the targeted application. One solution is to make an initial selection of methods, test them and then perform a series of evaluations.

Data analysis techniques usually use as a starting point an array representation, called a confusion matrix. This Table I.3 link the number of predictions $X_{i,j}$, ($X_{class,prediction}$) samples of class i assigned to a class j (among C classes). The number of samples forming class i is noted as K_i , and the total number of predictions attributed to this class is named M_i . The sum of the K_i and the sum of the M_i corresponding to the total number of samples (Σ).

Table I.3: Prediction Confusion Matrix of a C-Class Classifier

		Prediction			Total /Classes
		Class ₁	Class _{<i>i</i>}	Class _{<i>C</i>}	
Real Class	Class ₁	$X_{1,1}$	$X_{1,i}$	$X_{1,C}$	K_1
	Class ₂	$X_{i,1}$	$X_{i,i}$	$X_{i,C}$	K_i
	Class _{<i>C</i>}	$X_{C,1}$	$X_{C,i}$	$X_{C,C}$	K_C
Total Predictions		M_1	M_i	M_C	Σ

Considering the previous problem, for each of the classes i , as binary (Class i : positive; All other classes $i \neq j$: negative), or directly in the case of a two-class problem, the predictions are summarized as four main pieces of information:

- **True Positive (Tp)**: Samples of the positive class (i) correctly classified ($X_{i,i}$).
- **False Negative (Fn)**: Samples of the positive class (i) incorrectly classified ($X_{i,j}, \forall j \neq i$).
- **True Negative (Tn)**: Samples of the negative class (j) correctly classified ($X_{i,t}, \forall t \in [1, C] \neq i$).
- **False Positive (Fp)**: Samples of the negative class (j) incorrectly classified ($X_{j,i}, \forall j \neq i$).

For a problem with N classes, considered as binary for the test of each class, there are as many confusion matrices as there are classes, each representing the performance of the classification against class i . The confusion matrix for a two-class problem thus establishes the link between the total number of samples (P) of the positive class, the total number of samples (N) of the negative class, the four previous information and therefore the total number of samples classified positively (P_{pos}) and negatively (P_{neg}). This confusion matrix, Table I.4, gives an indication of the classification results. However, because the quantity of samples per class can vary between different classes and different problems, its exploitation is not always easy.

Various measures can be derived from a confusion matrix, from the problem with Two-classes we can describe the following metrics:

Table I.4: Two-class classifier prediction confusion matrix

		Prediction		Total /Classes
		Positive Class	Negative Class	
Real Class	Positive Class	Tp	Fn	P
	Negative Class	Fp	Tn	N
Total Predictions		P_{pos}	P_{neg}	Σ

- **False Acceptance Rate (FAR)**: Defined as the probability that the biometric security system mistakenly accepts an access attempt by an unauthorized user [20].

$$FAR = \frac{Fp}{Tn + Fp} = \frac{Fn}{N} \quad (I.3)$$

- **False Rejection Rate (FRR)**: Defined as the probability that the biometric security system mistakenly reject an access attempt by an authorized user name [20].

$$FRR = \frac{Fn}{Tp + Fn} = \frac{Fn}{P} \quad (I.4)$$

- **Sensitivity**: is calculated as the number of correct positive predictions divided by the total number of positives. It is also called recall or True Positive Rate or **Genuine Acceptance Rate (GAR)** witch is given by $GAR = 1 - FRR$ [16].

$$Sensitivity = \frac{Tp}{Tp + Fn} = \frac{Tp}{P} \quad (I.5)$$

- **Specificity**: is calculated as the number of correct negative predictions divided by the total number of negatives. It is also called true negative rate. It can also be calculated by $(1 - Specificity = FAR)$ [20].

$$Specificity = \frac{Tn}{Tn + Fp} = \frac{Tn}{N} \quad (I.6)$$

- **Precision**: is calculated as the number of correct positive predictions divided by the total number of positive predictions. It is also called positive predictive value [20].

$$Precision = \frac{Tp}{Tp + Fp} = \frac{Tp}{P_{pos}} \quad (I.7)$$

- **Equal Error Rate (EER)**: is calculated as the number of all incorrect predictions divided by the total number of the classes. **EER** defined also as the best compromise between **FAR** and **FRR** [20]. The best error rate is 0.0, whereas the worst is 1.0.

$$EER = \frac{Fp + Fn}{Tp + Tn + Fn + Fp} = \frac{Fp + Fn}{P + N} \quad (I.8)$$

- **Accuracy (ACC)**: is calculated as the number of all correct predictions divided by the total number of the dataset. The best accuracy is 100%, whereas the worst is 0.0 [20]. It can also be calculated by $(1 - EER)$.

$$ACC = \frac{Tp + Tn}{Tp + Tn + Fn + Fp} = \frac{P}{P + N} \quad (I.9)$$

Each of these metrics has a percentage describing a certain capability of the model. The higher the percentage value, the better the model. Sensitivity and specificity only take into account samples from the same test class (positive class for sensitivity and negative class for specificity). Thus, variations in the number of test images per class have no influence on these metrics. However, this is not the case for precision and accuracy. Indeed, precision takes into account the test samples determined as positive for both classes and the accuracy is a "global" evaluation of the model, considering all the prediction results (the whole confusion matrix).

The exploitation of previously described metrics are basic biometric performance measures such as the **FRR/FAR**, sensitivity/specificity and precision/sensitivity (or recall) pairs.

Figure I.28a illustrates match score distributions for **FRR/FAR** by the use of different thresholds. These thresholds, applied to the prediction scores, make it possible to adjust these metrics by considering a prediction as just if its associated score is higher than this threshold.

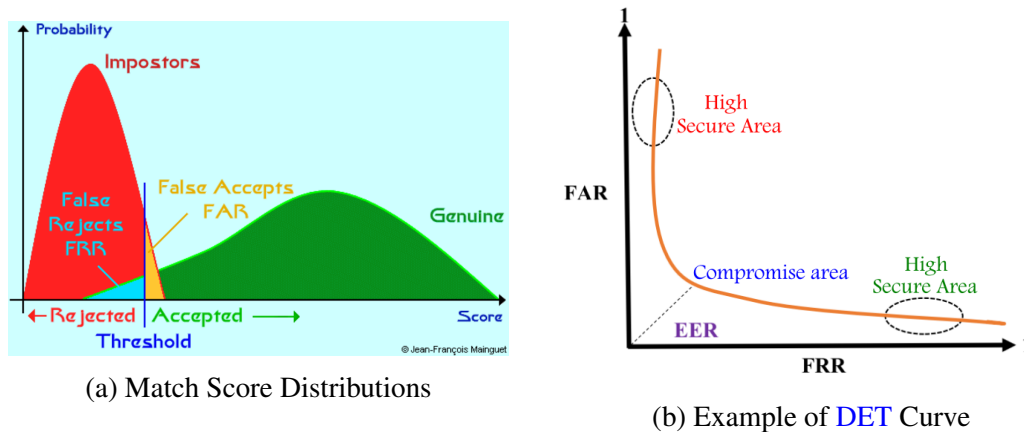


Figure I.28: Example of **FRR/FAR** Illustration²².

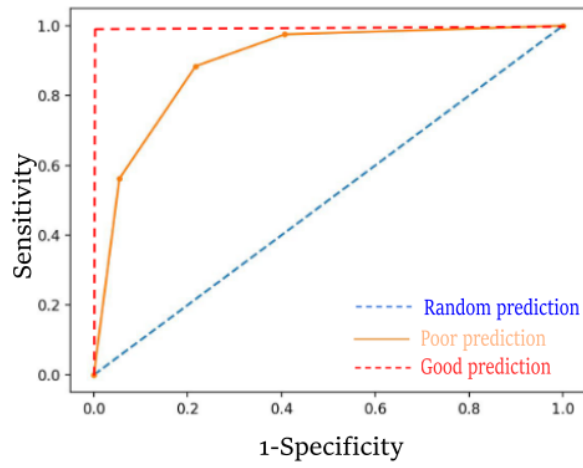
Figure I.28b illustrates the **Detection error tradeoff (DET)** curve which presents the relationship between the **FRR** and the **FAR**. It is obtained by varying the decision threshold and each time calculating the two **FRR** and the **FAR** values [43].

Figure I.29 represents the utilization of the sensitivity/specificity and precision/sensitivity pairs. Figure I.29a shows the **Receiver Operating Characteristic (ROC)** curve, which is a popular measure for evaluating classifier performance [43]. The **ROC** curve is a model-wide evaluation measure that is based on two basic evaluation measures: sensitivity/specificity. Similarly, the **Precision-Recall (PR)** curve [43] shows what happens to precision and recall as we vary the decision threshold (see Figure I.29b).

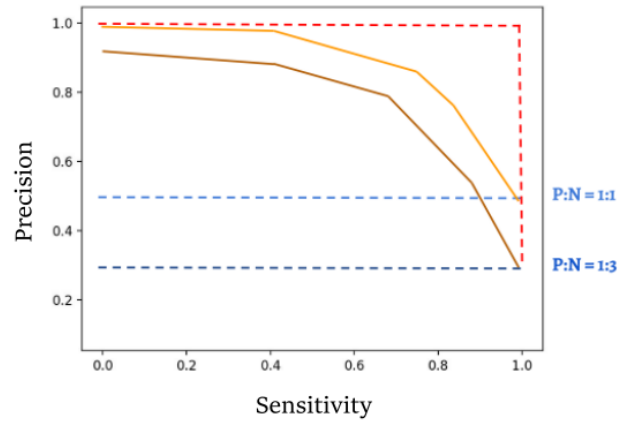
A specific metric named the **Area Under the Curve (AUC)** score is another gain of the usage of the **ROC** or **PR** curves. As the name indicates, it is an area under the curve calculated in the **ROC** or **PR** space. One of the easiest ways to calculate the **AUC** score is using the trapezoidal rule, which is adding up all trapezoids under the curve [21].

Figure I.30 represents the utilization of the **Cumulative Matching Characteristic (CMC)** curve, the graphical representation used to evaluate the performance of a biometric identification system using **Rank One Recognition (ROR)** and **Rank of Perfect Recognition (RPR)**. A **CMC** curve plot the identification rate against the rank [16].

²²Image source: <https://biblio.univ-annaba.dz/These-Hafs-Toufik.pdf>



(a) ROC curve



(b) PR curve

Figure I.29: Example of ROC and PR curves illustration

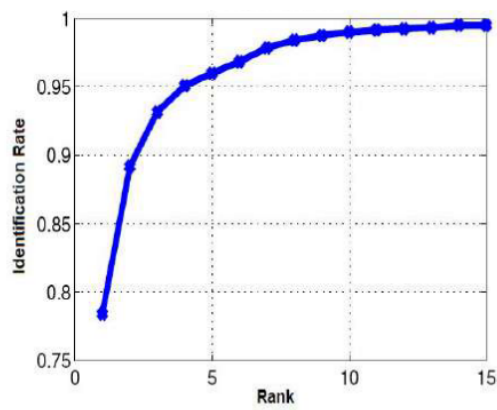


Figure I.30: Example of CMC Curve

I.9 Conclusion

Biometrics are increasingly becoming a tool for recognizing individuals in various applications. It gains its place as the best security approach of authentication. However, a number of challenges, such as attacks on biometric systems, remain to be defeat. Notwithstanding this, the future of biometrics holds promise for recognition of individuals. In this chapter, we have offered an overview of biometrics to briefly introducing and its related technology briefly. To that end, the fundamental concepts of biometrics and its principles have been described. The features of biometric modalities and their advantages and applications have been described in this chapter. Furthermore, this chapter has explained the basis of a general biometric system, including their components and the most significant biometric functions: enrollment, verification and identification. Finally, Metrics and charts which needed for the evaluation of biometric performance are presented. Where it has been possible to state that the rate of false rejections or false acceptances are performance indicators enabling the application to be adapted to the context of use of the modality biometric and that the degree of security of a biometric system can be adapted to the intended use of the system. On the other hand, the effectiveness of a particular modality depends on its relevance to the intended application. Combining or fusion of multiple modalities in the same application increases system reliability and security. The next chapter is dedicated to the presentation of the different concepts related to biometric systems fusion.

CHAPTER II

MULTIMODAL BIOMETRIC SYSTEMS

Contents

II.1 Introduction	36
II.2 Unimodal Biometrics Systems Limitations	36
II.3 Multi-modality in Biometrics	37
II.3.1 Data Fusion Concept	37
II.3.2 Multi-Biometrics Sources	38
II.3.3 Multimodal Biometrics System Architectures	39
II.4 Biometrics Fusion Levels	41
II.4.1 Fusion Pre-Classification:	41
II.4.2 Post-Classification:	43
II.5 Biometrics Fusion Methods	47
II.6 Conclusion	48

II.1 Introduction

Multimodality is defined as the use of various biometric systems. The primary purpose of fusing different biometric systems is to reduce the limitations of unimodal biometrics. Indeed, the combination of other biometric systems aims to improve recognition performances by increasing the quantity of discriminant data of each person and to decrease the risk of enrolment failure and the robustness to frauds. This chapter introduces the multimodal biometric systems, including the multibiometrics types and architectures. Eventually, we discuss biometric fusion levels.

II.2 Unimodal Biometrics Systems Limitations

Biometric systems have certain limitations that make applications unstable. The main limitation incorporates performance [44]. Indeed, biometric systems do not allow exact recognition because they are based on the degree of similarity between the two biometric data comparisons. These variations in biometric data and the lack of exact matching are due to several parameters [24, 42]:

- **Non universality:** if each individual is capable of presenting a biometric modality for a given system, then that modality is said to be universal. However, we see that many biometric modalities are not really universal. The National Institute of Standards and Technologies (NIST) reported that it was not possible to obtain a good quality fingerprint for about 2% of the population (persons with hand-related disabilities, individuals performing many repetitive manual jobs, etc.) [45]. Thus, such persons cannot be registered in a fingerprint verification system. Similarly, people with very long eyelashes and those with abnormalities of the eyes or eye diseases (such as certain glaucomas and cataracts) cannot provide images of Iris, or retina, of good quality for automatic recognition [44];
- **Noise effect:** The captured data may be noisy or damaged. A fingerprint with a scar or voice modified by a virus (Cold/flu) are examples of noisy data [16]. They could also result from a faulty or poorly managed sensor (for example, accumulation of dirt on the fingerprint sensor). The noisy data can be incorrectly compared with the models in the database resulting in incorrect user rejection [44];
- **Spoofing attacks:** An imposter may attempt to mystify a registered authorised user's biometric trait to defraud the system. This type of attack is particularly appropriate when behavioural traits such as signature and voice are used [44]. However, the physical features are also sensitive to attacks; for example, it has been shown that it is possible to build artificial fingers or fingerprints in a reasonable time to defeat the fingerprint verification system;
- **Distinctiveness:** Within a large community, unimodal biometrics are prone to inter-class similarities. Facial recognition may not work correctly for identical twins as the camera might not distinguish between the two subjects leading to inaccurate matching;
- **Intra-class variations:** The biometric data acquired from an individual during the enrolment phase may not be the same as the template used during recognition. This variation is typically caused due to incorrect interaction with the sensor, or when sensor characteristics are changed during the recognition phase.

Some types of unimodal biometric system limitations are shown in Figure II.1.



Figure II.1: Example of Unimodal Biometric System limitations.

II.3 Multi-modality in Biometrics

The need for high accuracy and reliability is also growing as biometrics witness a lot of interest from many fields. While multiple biometric solutions have been established and upgraded, there are still limitations that have to be overcome to achieve various applications' performance requirements. Nowadays, most biometric solutions deployed in real-world applications are already unimodal. Multimodal biometric systems can mitigate many biometric system limitations because the different biometric sources typically compensate for the other sources' inherent limitations [46]. Multimodal biometrics are systems able to use more than one physiological or behavioural characteristic for enrollment, verification, and identification [47]. Multimodal biometrics exploit information among different modalities based on data fusion techniques.

II.3.1 Data Fusion Concept

The general concept of data fusion consists of combining data from several sources to obtain a more significant decision than obtained from separate sources. The technologies used use different methods from different areas, such as signal processing, artificial intelligence, recognition of patterns, classification, etc. In general, data fusion is a combination process of diverse data in order to create new information which will be more representative of all the data. Data fusion was first considered to improve the quality of the answer to the military problems [48]. Today, it significantly affects areas such as weather forecasting, multimodal biometrics, remote sensing, robotics and medical application.

The integration of data fusion in the conception of the biometric system increases efficiency and accuracy. The progress of the multi-biometric systems front several challenges. The successful pursuit of these systems challenges generates significant advances and improvements. Hence, the challenges in designing biometric multimodal systems are:

- The sensors used for collecting the data should show flexibility in performance under a variety of operational environments. The sensor should be fast, low cost, and with better quality images.
- The information obtained from different biometric sources can be combined at four different levels: sensor level, feature level, score level and decision level (see Section II.4). Therefore, selecting the best level of fusion will directly impact performance and cost involved in developing a system.

- There are many techniques available for data fusion in the biometric multimodal system; the various sources of information are available. So, it is challenging to find the optimal solution for the provided application.

II.3.2 Multi-Biometrics Sources

Multimodal biometrics refers to the use of two or more separate biometric. So, the sources of information that can be considered in a multimodal biometric system are important. Figure II.2 describes the various scenarios that are possible to obtain multiple sources of data. In general, there are five types of multimodal biometric systems; in four scenarios, the information fusion is accomplished using a single trait, while in the fifth scenario, multiple traits are used [5, 17, 47].

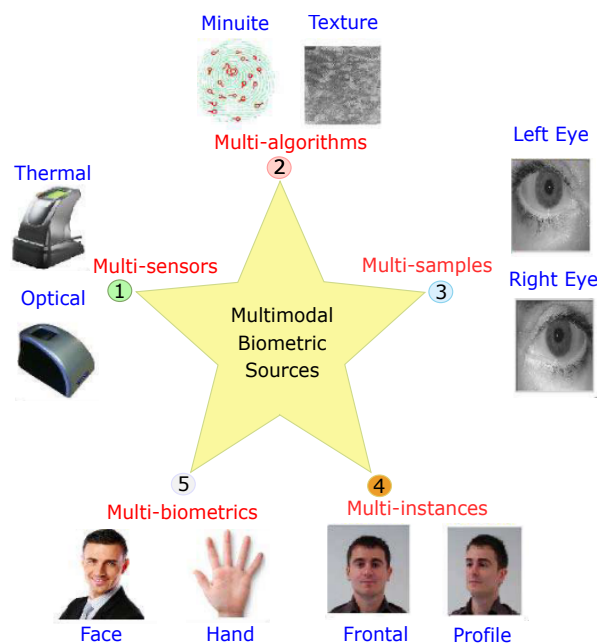


Figure II.2: Example of Multimodal Biometrics Sources.

- 1. Multi-sensor systems:** These systems use multiple sensors to capture a single biometric characteristic of an individual to extract diverse information from captured images. For example, the fingerprint systems can utilise an optical sensor and a thermal sensor to acquire the images.
- 2. Multi-algorithm systems:**

In this combination scenario, multi-algorithm systems apply different feature extraction algorithms on a single biometric trait. The extraction of the characteristics is done through different algorithms before the fusion step. For example, we can combine two algorithms to process the same fingerprint image, one that analyses the texture while the other extracts the minutia.
- 3. Multi-sample systems:** Multi-sample systems leverage multiple samples of the same biometric characteristic to recognise individuals using a single sensor for accounting for the variations that can occur in the trait to obtain a complete representation of the underlying trait. For example, the acquisition of the frontal profile of a person's face and the left and right profiles considers the facial poses variations.

4. **Multi-instance systems:** In these systems, multiple instances of the same individual body feature are deployed. The same biometric character can be acquired over several temporal intervals. The objective here is to consider the interpersonal variation of the biometric modality. Multi-instance systems are particularly beneficial for users whose biometric traits cannot be reliably captured due to inherent problems. For example, a single Eye may not be a sufficient discriminator for a person. However, the integration of evidence across left and right Eye may serve as a good discriminator in this case.
5. **Multi-biometric systems:** These systems establish an identity-based on the data of multiple biometric features. For example, a person may have to present her hand and face scan for personal identification on a multi-biometric system that uses data from both the biometric identifiers.

II.3.3 Multimodal Biometrics System Architectures

Multimodal systems combine multiple biometric systems and therefore require multiple data acquisition and processing. As a result, the acquisition and the processing can be made successively or simultaneously; we speak then of architectures in series or parallel. Fusion strategies or architectures describe all sources, how they are collected, and statistical or mathematical processing techniques.

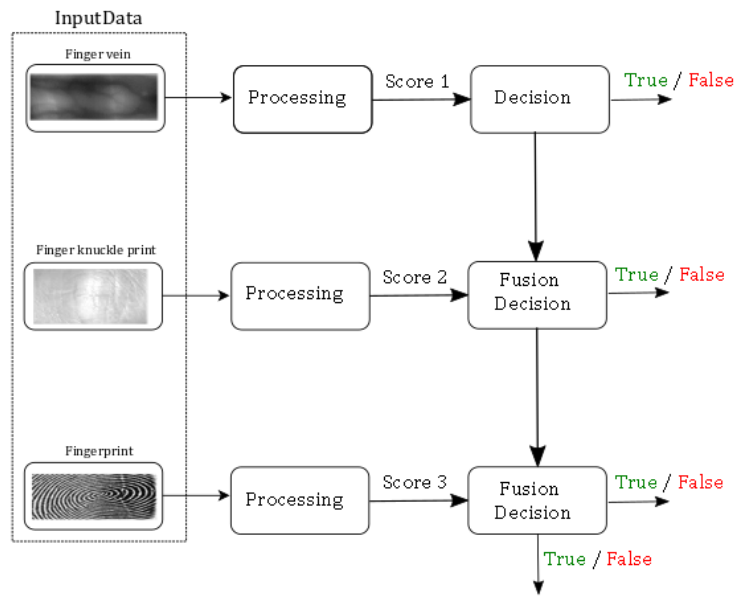
The acquisition of biometric data is generally sequential for practical reasons. It isn't easy to acquire a fingerprint and an iris image simultaneously under the right conditions. However, there are some cases where acquisitions can be made simultaneously when the different data uses the same sensor, such as the multi-finger fingerprint sensors that allow several fingers to be acquired simultaneously or even the finger knuckle prints and finger vein. A multimodal biometric system can be designed according to three architectures [25]: serial (or cascading) architecture, parallel architecture and hierarchical (or tree) architecture. The architectures are generally related to the processing and, in particular, to the decision. Indeed, the difference between multimodal systems lies in obtaining a similarity score at the end of each acquisition or performing all scans before making a decision. A graphical representation of the three categories is given in Figure II.3

In the *serial architecture* (see Figure II.3a), individual systems are requested in sequence. Some of them may be used only when a possible condition arises at the exit of the systems referred to above, which makes it possible to reach a decision without necessarily involving all of these systems. This architecture can be used as an indexing scheme to reduce the number of possible identities before using the following data. It also increases efficiency by first using low-cost and less accurate systems and then using more expensive but more accurate systems.

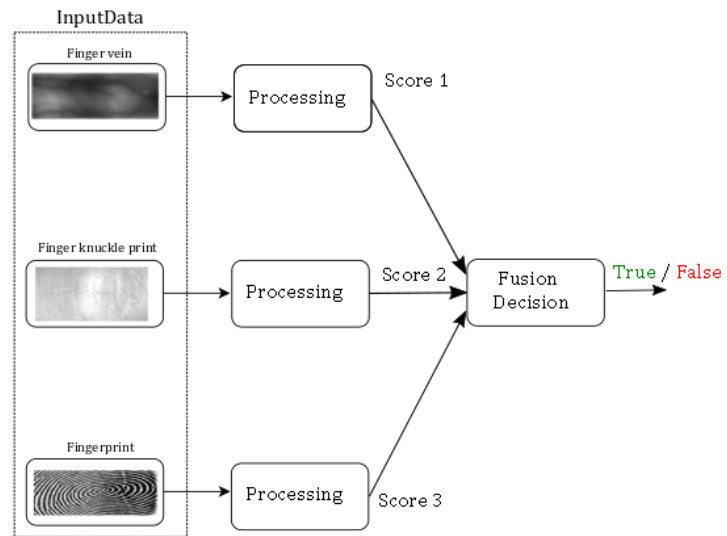
In the hierarchical architecture (see Figure II.3c), the individual systems are combined into a tree structure. This architecture is considered the most flexible and makes it possible to deal with missing or poor quality data often encountered in biometric systems.

In the *parallel architecture* (see Figure II.3b), information from different systems are used simultaneously to perform the task of reconnaissance. The use of all biometric information is then required to produce a decision, which is likely to provide more improvement than in a *serial architecture*. These advantages have meant that most of the methods proposed in the literature belong to this category of architecture, which is also the case with the methods proposed in this thesis work.

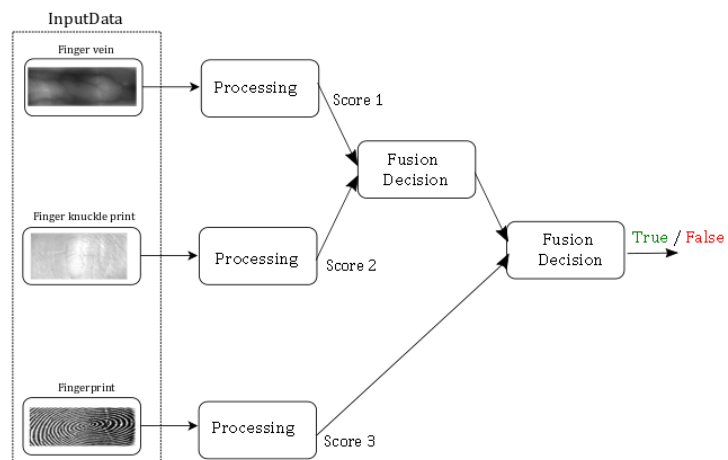
The choice of the architecture of a system depends on the needs of the application. In user-convivial and low-risk applications, *serial architecture* is preferred for its cost advantages in time and hardware over *parallel architecture* requiring the acquisition and processing of a large amount of biometric data. On the other hand, in applications where security is of paramount importance, *parallel architecture* is more appropriate. *Tree architecture* is preferred in applications where there is a greater risk of low-quality biometric data. It is also used in applications where one or the other modalities may be missing [25].



(a) In series



(b) In parallel



(c) In tree

Figure II.3: Example of fusion architectures

II.4 Biometrics Fusion Levels

During the biometric system process the amount of information available becomes compressed as one progresses through its steps, from acquisition to decision as presented in Section I.6. With respect to the type of information in each module, several levels of fusion can be defined. Indeed, the fusion process may be performed in five different levels: sensor level, features level, matching score level, rank level and decision level, as shown in Figure II.4. These five levels may be classified into two sub-sections: *fusion Pre-Classification* or *fusion Post-Classification after-matching* steps [49].

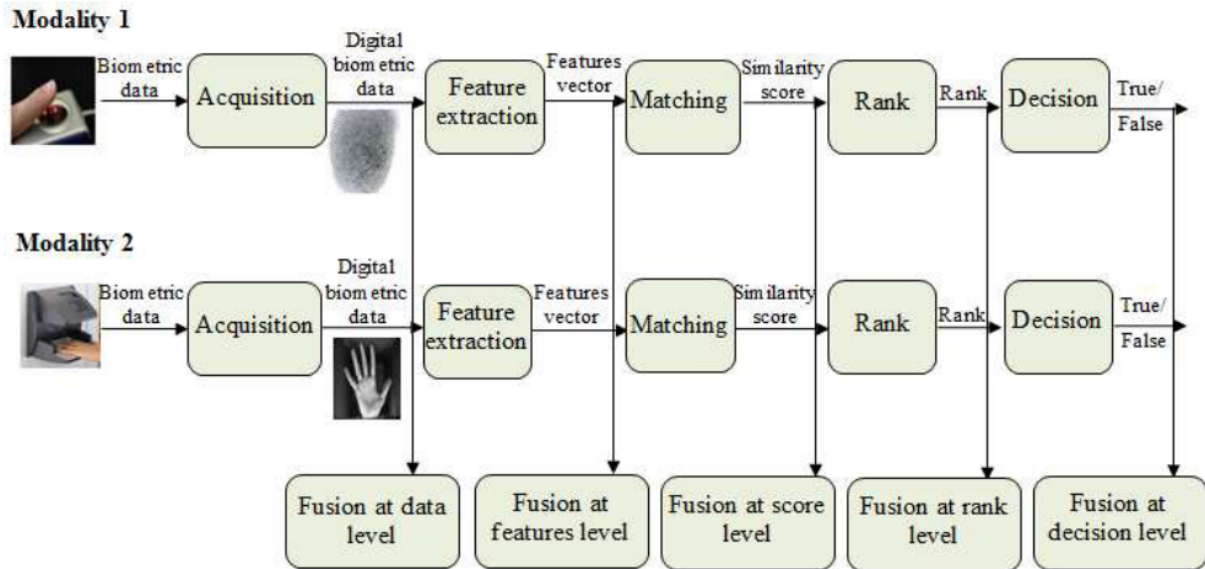


Figure II.4: Example of different fusion levels of biometric systems.

In what follows, we will detail these two sub-sections fusion families:

II.4.1 Fusion Pre-Classification:

The combination of the information at pre-classification (fusion before the matching), can occur either at the sensor or at the level of the characteristics extracted by the feature extraction module. These types of fusion require homogeneity between the data.

- **Fusion at sensor Level:** The first level of fusion is at the sensor level. This fusion aims to create a new capture of higher quality than the source captures, which will be processed before feature extraction as shown in Figure II.5 [50]. In the field of image processing, this method is referred to as image fusion or pixel fusion. Due to the need for homogeneous data, this form of fusion is used infrequently. Indeed, sensor-level fusion may be accomplished by combining several compatible captures of instances extracted from the same biometric trait or combining multiple instances of the same biometric trait identified by a single sensor [42]. In general, data fusion is not feasible if the data instances are incompatible.
- **Fusion at feature extraction Level:** Fusion at the feature extraction level consists of combining different vectors from different sensors or obtained by applying different algorithms to the same biometric data [25, 51]. The extracted characteristic obtained from one of the following sources: multiple sensors of the same biometric trait, multiple instances of the same biometric trait, multiple units of the same biometric trait, or multiple biometric traits (see Section II.3). Combining characteristic vectors from different sensors or obtained by

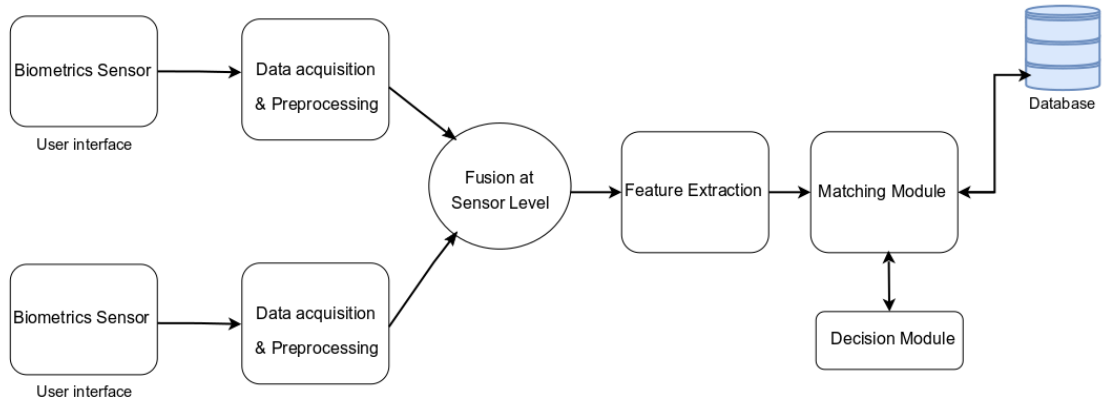


Figure II.5: Flowchart of fusion at the sensor level.

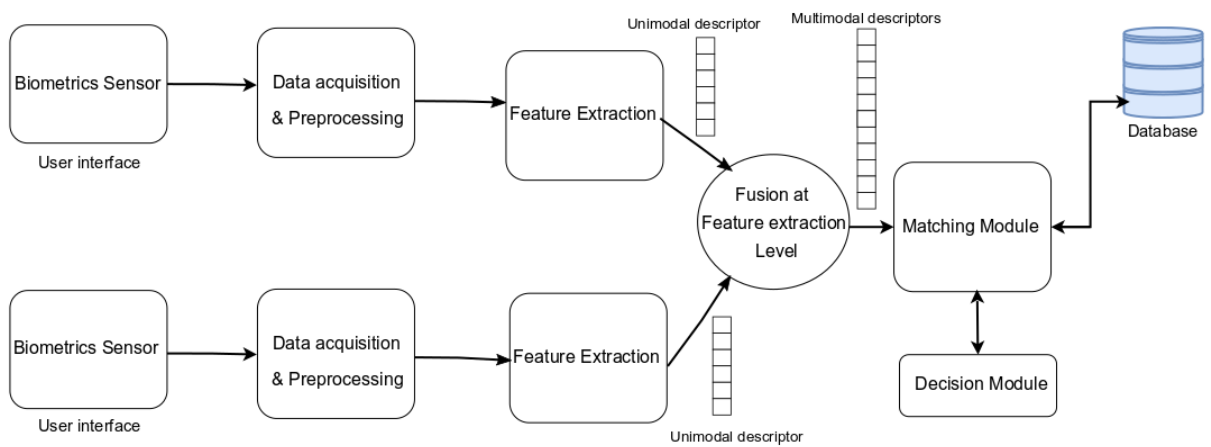


Figure II.6: Flowchart of fusion at the feature extraction level.

applying different algorithms to the same biometric data as shown in Figure II.6. The extracted features can be vertical or horizontal contour, geospatial information, grey level intensity,.. etc. There are many algorithms to extract the feature vector to and fusion theme [3, 19, 24, 52]. For instance, PCA, LDA coefficients, Gabor transformation, DCT and DWT [53, 54]. According to S.K.Bhardwaj [55], When the characteristic vectors are homogeneous (e.i, multiple fingerprint images of a user's finger), a single resulting characteristic vector can be calculated as vector of the individual characteristic vectors. When characteristic vectors are heterogeneous (e.i, vectors of features of different biometric modalities like fingerprint and finger vein), we can concatenate them to form a single vector of features. This supplies a vector of larger size, which contains more information . However, in the case of heterogeneous data, a normalization step (data standardization) should be made before vectors concatenation [44, 51]. This fusion techniques is used in our work(see Chapter V).

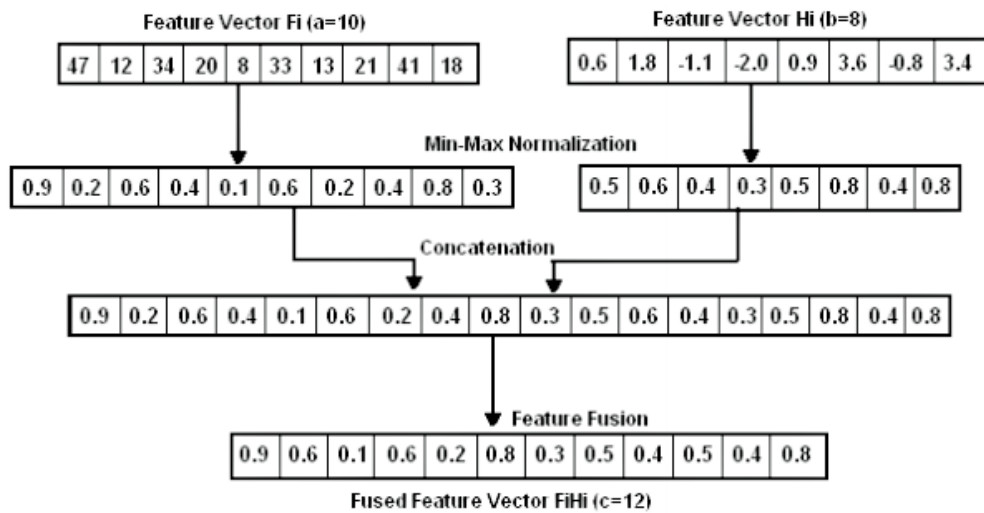


Figure II.7: Example on Feature Level Fusion of two Heterogeneous Feature Vectors.

II.4.2 Post-Classification:

The integration of multiple biometric information at the post-classification (fusion after-matching) can occur through two categories: the *dynamic classifier selection* and the *classifier fusion* [49].

- **Dynamic classifier selection:** Dynamic classifier selection, also known as the "*winner-take-all*" approach, requires consideration of partitioning of input data [49]. These can be defined by the individual decisions of each classifier or by the characteristics of the input samples. For each partition, the classifier providing optimal results on learning or validation data is selected. For classification, an unknown sample is assigned to a partition. The classifier's decision, associated with that partition, is most likely to give a correct decision, which is used in the final decision. In summary, dynamic classifier selection attempts to predict which classifier is most likely to provide a correct result for a given sample [20].
- **Classifier fusion:** Classifier fusion uses individual classifiers in parallel, and their outputs are combined to obtain a "group consensus". There are three levels of fusion for this second category, namely fusion at the score level, fusion at the rank level and fusion at the decision level [20, 49].
 - **Fusion at score Level:** Fusion at score level is referred to as the combination of similarity scores obtained from different classifiers as shown in Figure II.8. This type of

fusion is the most usually used one since it may be applied to all types of systems , in a small dimension space (the size of the vector of scores signifies the number of subsystems) [56], using approximately simple and effective methods and treating more information than decision fusion. Indeed, the fusion at level score offers the best trade-off between information richness and ease of implementation [42, 56]. There are two

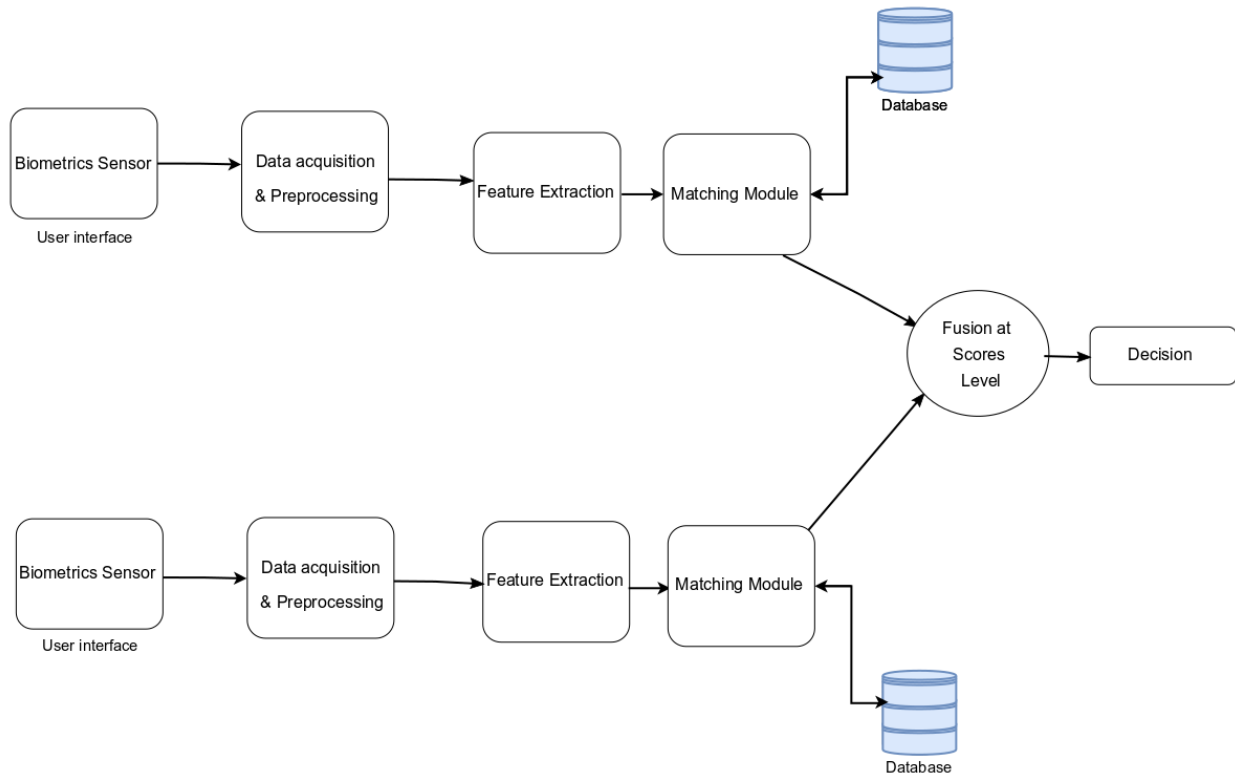


Figure II.8: Flowchart of fusion at the score level.

approaches to combining scores from different matches. The first approach is to see it as a *classification* problem. The second approach is to treat the subject as a *combination* problem [42, 49].

– **Score fusion based on Classification approaches :**

is to see the fusion as a *Classification* problem that searches to separate the two classes *Genuine* and *Impostor* in the N -dimensional space of scores.

A characteristic vector formed by individual matcher scores is assigned to one of the *accepted* (also called authorized / authentic / client) or *rejected* (*imposter*) classes. Generally, the classifier used can make such a decision regardless of how the characteristic vector of scores was generated, which makes it possible to merge non-homogeneous scores on the output of the different matchers (distance or similarity, different score intervals, etc.) without any prior processing before passing them to the classifier. Several classifiers were used to consolidate individual matcher scores and arrive at a final decision. We can cite, as an example, LDA [57], multi-SVM [58], Neural Network [53] and Multi-ELM [59].

– **Score fusion based on combination approaches :** in this approach, individual match scores are combined to form a single score to make the final decision [46, 52]. Two steps are required to establish the fusion of scores: *Normalization of scores*, the *combination of standardized scores*.

Normalization makes it possible to make the score distributions of the different authentication subsystems compatible, indicating that modifying the parameters

of the distribution of correspondence, scores (mean and standard deviation), so that they are in the same interval.

- **Normalization:** makes it possible to make the score distributions of the different authentication subsystems compatible, indicating that modifying the parameters of the distribution of correspondence, scores (mean and standard deviation), so that they are in the same interval. In the literature, there are several methods of normalization of scores. The three most known methods of normalization [21, 60], are the *Min-Max*, the *Z-score* and *TanH* methods. According to Vishi et al. [60], the *Hyperbolic Tangent Normalisation (TanH)* is the more robust and efficient normalisation method comparing with the fundamental normalisation concepts. The *TanH* offer respectively normalized score in the range [0, 1] according to the described Equation (II.1). Where, S_{Mean} and S_{SD} are the mean and standard deviation estimation of the score distribution, respectively.

$$s_{TanH} = \frac{0.01 \times (S - S_{Mean})}{S_{SD}} \quad (II.1)$$

- **Combination of standardized score:** The set of rules for combining scores was developed by Kittler et al [61]. The goal is to obtain a single classification score using several combination schemes such as the rule (sum rule), the *product rule*, the *maximum rule (max rule)*, the *minimum rule (min rule)* and the *median rule* [62]. Among the different score fusion techniques recommended by ISO standards ISO/IECTR 24,722:2015 [46], only *weighted sum* (Equation (II.2)), *weighted product* (Equation (II.3)), *Bayesian rule* (Equation (II.4)) fusion techniques are used in our work (see Chapter V).

$$s_{ws} = w_i \times S_1 + (1 - w_i) \times S_2 \quad (II.2)$$

$$s_{wp} = S_1^{w_i} \times S_2^{w_i} \quad (II.3)$$

$$s_B = \frac{S_1 \times S_2}{(1 - S_1) \times (1 - S_2) + S_1 \times S_2} \quad (II.4)$$

Here S_1 and S_2 are the recognition scores of unimodal systems, w_i is a weight value and computed as following:

$$w_i = \frac{EER_i}{\sum_i EER_i} \quad (II.5)$$

where EER_i is the *Equal Error Rate* of each unimodal biometric system and $\sum_i EER_i = 1, 0 \leq w_i \leq 1$. The final decision is obtained according to the *threshold* score.

- **Fusion at rank Level:** Rank-level fusion the method that consolidates more than two identification results to improve the reliability of individual identification [20, 63]. When a system uses several classifiers and their output has several classes, it is possible to sort them in descending order according to their confidence score associated with the prediction, thus allowing to perform a fusion at the rank of the prediction. For this type of fusion, *Ho et al.*[64] distinguish three techniques allowing the combination of these ranks:
 - **Highest Rank Method:** Each possible match is assigned the best (minimum) rank calculated by different matches in this method. In the case of equalisation, only one is chosen at random to arrive at a strict rank order, and the final decision is made according to the combined ranks.

- **Borda Count Method:** This method uses the sum of the rank assigned by the individual matches to calculate the combined ranks.
- **Logistic regression:** It generalises the "Borda count" method where a weighted sum of individual ranks calculated and weights are determined by logistic regression.

"Highest Rank Method", "Borda Count Method" and "Logistic regression" [64].

- **Fusion at decision Level:** this involves combining the decisions of the biometric systems as shown in Figure II.9, which each give a response (*accepted:1* or *rejected: 0*, in the case of verification) according to the entry presented to them [50]. This level of fusion can be achieved by simple rules such as:

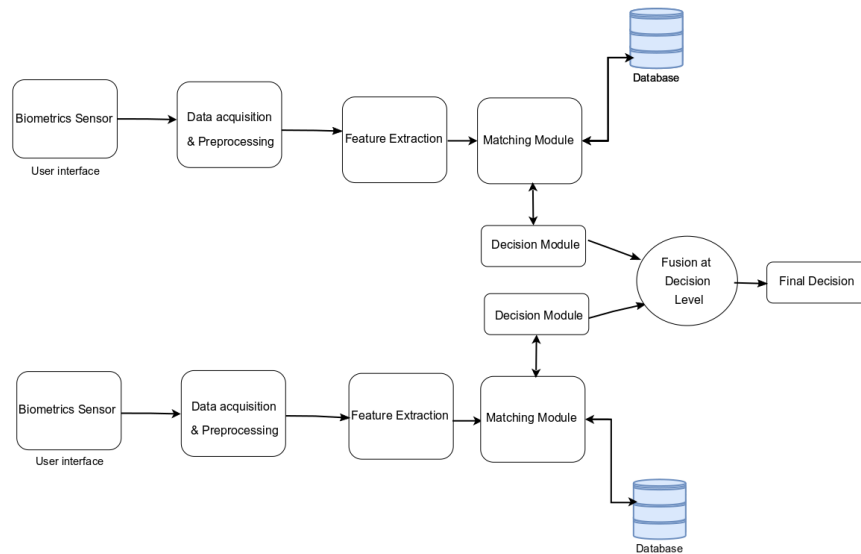


Figure II.9: Flowchart of fusion at the decision level.

- **Majority voting:** Voting methods consist of interpreting each output of a classifier as a vote for one of the possible classes. The class with a majority number of votes or more than a predetermined threshold is chosen as the final decision [44, 61].
- **Weighted vote:** These voting methods consist of interpreting each output of a classifier as a majority vote. The classifiers' votes are weighted, and each class receives as many votes as there are classifiers to combine is chosen as the final decision [25].
- **And and OR rules:** The final decision consists of accepting the user "if and only" if or "all, if at least" the subsystems have recognized one used modality [44].

Other complex methods based on prior information regarding the performances of various biometric sub-systems exist. For instance, we can cite methods based on *Bayes theory*, the evidence theory of *Dempster-Shafer*, *the behaviour knowledge space*, etc [62]. Fusion at the decision level has the advantage of being simple. However, the information it uses is very limited (0 or 1) [25].

Above, many fusion techniques are presented, which could be used in any biometric modalities (see CHAPTER 2. Section I.3). Figure II.10, resume most of them use fusion at a single level, whichever level it is. Fusion at more than two levels can be done, or at all five levels. This might create a very complex system, but with the advancement in the efficiency of computational resources, it is possible. Also, the research in multimodal biometric authentication systems and the observation of various proposed systems leads us to believe that a biometric system using multiple

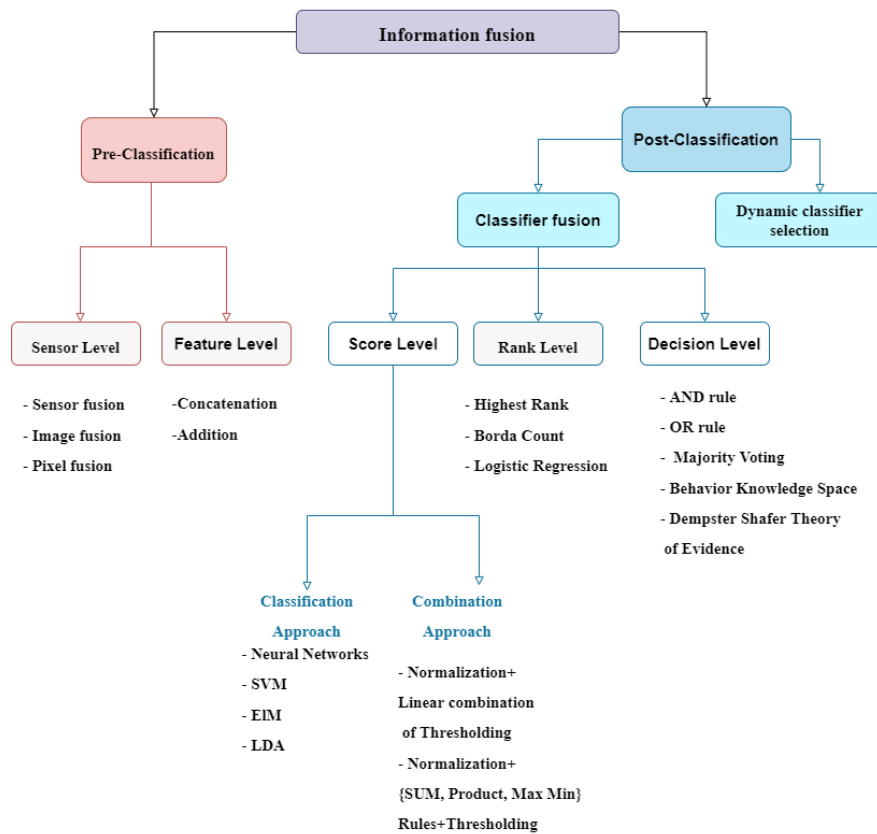


Figure II.10: A diagram of the various levels of biometric fusion.

modalities gives high accuracy, robustness and good overall performance where the *feature* and *score* levels are the most popular because they are more stable and prove effective recognition performance. There are several topologies and levels of fusion, which depends on the nature of the sources and information.

II.5 Biometrics Fusion Methods

In literature [49, 52], there are a vast number of techniques for different fusion level. On that point are certain techniques for multimodal fusion, as given in Figure II.11, that can be categorized into three types: *Rule-based techniques*, *classification based techniques* and *estimation-based techniques* [49, 65]. This classification of methods depends on the basic structure of these techniques. It essentially means categorising problem areas, like parameter estimation, can be solved using estimation-based techniques. On the other hand, the problems based on obtaining a result depending on a certain observation is solved using rule-based or classification based technique. However, if varying types of modalities are observed, then a fusion of all observation scores is required before a classification decision or estimation is made [49].

– Rule-based fusion techniques:

The rule-based fusion techniques include an array of some basic rules that combine multimodal information. Some statistical rule-based techniques are used in this case, such as *product* and *sum* based fusion (*linear weighted*), *MIN*, *MAX*, *majority voting*, *OR*, *AND*. All these rules are custom-defined, and their structure is specifically based on the application perspective. The rule-based technique, in general, performs well if the temporal alignment amongst different modalities has good quality [49, 65].

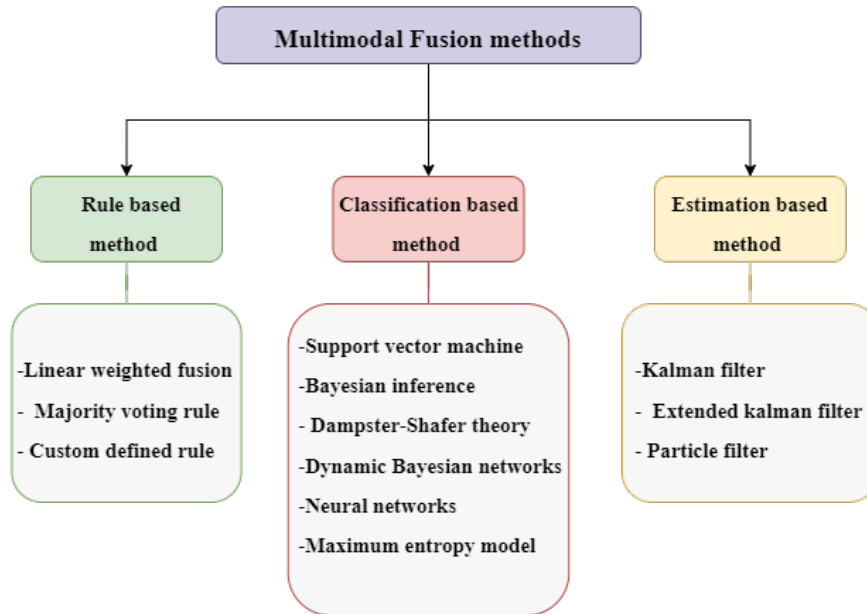


Figure II.11: Fusion methods types example.

- **Classification based fusion techniques:** These techniques include a wide array of classification methods used to classify the multimodal observations into one of the pre-defined classes. For instance, the techniques in this category are *maximum entropy models*, *neural networks*, *dynamic Bayesian network*, *Dempster–Shafer theory*, *Bayesian inference* and *Support vector machine* [49, 65]. These techniques can be noticeably more divided into two methods: discriminative and generative models, from machine learning.
- **Estimation-based fusion techniques:** This estimation based category will include particle filter fusion techniques, such as: *extended Kalman filter* techniques and the *Kalman filter* method [49, 65]. These described techniques are mostly used to estimate better any moving entity's state based on multimodal information. For instance, tracking an object requires the fusion of multiple modalities such as video and audio to estimate the final object position.

II.6 Conclusion

In this chapter, we have discussed the principle of multi-biometric systems and fusion techniques. There are different types of architecture as well as different levels of fusion throughout the progression through the biometric system, from the biometric sensor to the final decision to accept or reject an individual. Multi-biometrics can effectively improve the performance and robustness of the authentication process by combining different information. There are several topologies and levels of fusion, which depends on the nature of the sources and information. Therefore, in the next chapter, we will outline the used information sources, which is based on finger biometrics.

CHAPTER III

FINGER-BASED BIOMETRICS

Contents

III.1 Introduction	50
III.2 Bibliometric Analysis of Finger-Based Biometrics	50
III.2.1 Research process	50
III.2.2 Preliminary Search Results	51
III.2.3 Exploratory Data Highlights	54
III.2.4 Deductions from Bibliometric Analysis	59
III.3 Fingerprint Biometrics	59
III.3.1 Fingerprint Imaging Principe	60
III.3.2 Fingerprint Databases	60
III.4 Finger Vein Biometrics	62
III.4.1 Finger Vein Imaging Principe	63
III.4.2 Finger Vein Databases	63
III.5 Finger Knuckle Print Biometrics	65
III.5.1 Finger Knuckle Print Imaging Principe	65
III.5.2 Finger Knuckle Print Databases	66
III.6 Conclusion	67

III.1 Introduction

Bibliometric analysis is a popular and rigorous method for exploring and analysing large volumes of scientific data. It refers to the cross science of quantitative analysis of all knowledge carriers with mathematical and statistical methods. Bibliometric analysis is a comprehensive knowledge system that enables researchers to unpack the evolutionary nuances of a specific field while shedding light on the emerging areas and for detecting the state of art for a particular field. This chapter presents a bibliometric analysis of finger-based biometrics. The research process respects bibliometric analysis's vital aspects, such as documents fetched by significant keywords, language, source, subject area, type, and year. The information is then related to each other with the help of network diagrams for the appearance of data like- authors and source titles, authors and keywords, authors linked by co-publication etc. Eventually, we present an overview of the biometrics of the finger.

III.2 Bibliometric Analysis of Finger-Based Biometrics

The study aims to investigate the evaluation of finger-based biometric systems. The stud's objectives are to identify the various biometrics and features proposed in the literature, as well as the fusion levels, datasets and approaches that they have employed, and suggest future directions to empower knowledge in the area. Based on these objectives, the study focuses on analysing how the literature covers finger-based multimodal biometric systems, what can be learned, and what is missing to advance research in the field.

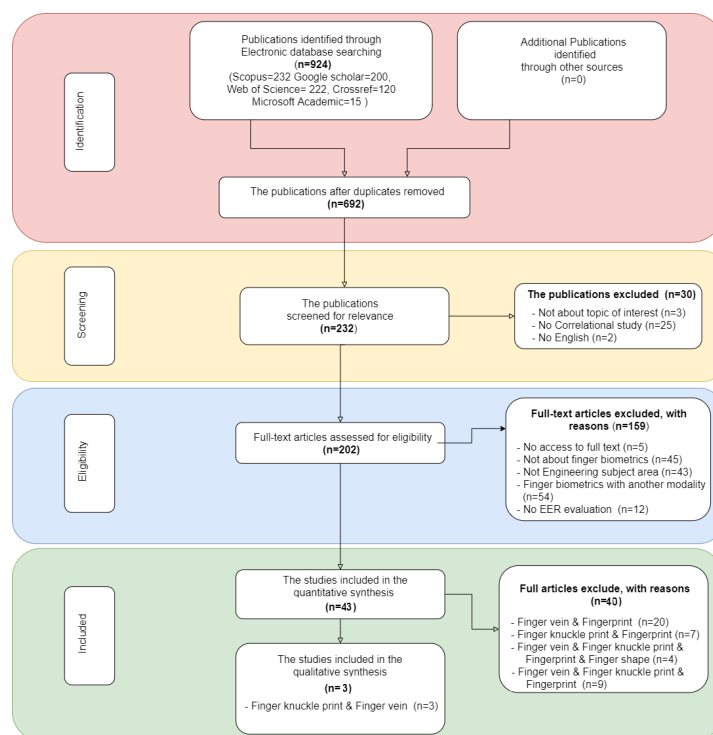


Figure III.1: Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Flowchart of the research process

III.2.1 Research process

– Research Question & data collection

The first phase of bibliometric recherche is to formulate the main research questions. As presented in Table III.1, the research question(RQ1)is the main guidance and direction of this

study to identify the various finger-based biometrics. Then we define the research question RQ2,RQ3 and RQ4 to get more details about the used fusion levels, datasets and approaches. After that, we get information about the problem of multimodal finger-based biometric systems.

Table III.1: The Main Research Questions

	Question	Motivation
RQ1	- What are the fused finger-based modalities?	To identify the various biometrics features that are used.
RQ2	In which fusion level are combined?	-To identify the best biometric fusion level.
RQ3	- What are the techniques or approaches used?	-To identify the dominantly used algorithms and how they perform.
RQ4	-What is the dataset used?	-To identify the available dataset for experiments.

We conduct a systematic review based on **PRISMA** guidelines [66] and the Biometrics research evaluation book [67] to ensure a comprehensive and unbiased a systematic review (see Figure III.1). We identify relevant studies on finger-based multimodal biometric systems as described in Figure III.1. Based on the research question, a search protocol is developed to guide the process to reduce the researcher’s biases in study selection.

- **Data sources:** The search process started with the identification of data sources. There are many popular datasets available to access the research data and articles, publication resources such as Research Gate, SCI Imago, Google Scholar, Mendeley, Scopus, Clarivate, ScienceDirect, Institute of Electrical and Electronics Engineers (IEEE) Xplore and Web of Science (WOS). We conducted initial browsing in the four major repositories Scopus [68], Crossref[69], Google Scholar[70], and Microsoft Academic[71], to cover various information technology literature. There are a lot of tools freely available can be used to measure scientific research performance. **Publish or Perish** is a software application intended for the analysis of the citations. This software is available from *Professor Anne Wil Harzing*, a specialist in international management at Melbourne University from Australia [72, 73](see Appendix A).
- **The used keywords:** The preliminary processing in any bibliometric study is to build a valid search query. In contrast, the quality of the outcome will depend on the goodness of the data in this step. To restrict the important articles on this research, many articles published as “*systematic reviews*” or “*bibliometric analyses*” are reviewed to build a search question. In this step, the keywords used are divided into two types: Primary and Secondary keywords. Primary keywords include finger and biometrics, and secondary keywords include multimodal biometrics, fusion, fingerprint, finger vein, finger knuckle print. Various combination using *Boolean operators* (‘AND’, ‘OR’ and ‘NOT’) [74] are used between the keywords and the results were analysed (See Table III.2). Where, the research is limited to publication years from 2000 to 2020.

III.2.2 Preliminary Search Results

The query, which is indicated in Section III.2.1, with the relevant search keywords used as a search strategy, found an important number of publications as presented in *Identification part* in a **PRISMA** flowchart see Figure III.1. According to the preliminary analysis of the obtained data (924 *publication*) ,692 duplicates of publication are removed. As results, we focus on the analysis of those 232 *publication* existing in the Scopus database.

Table III.2: Significant keyword and their combinations (i.e Using Scopus dataset)

	Keywords	Publication Count
Primary	"finger" AND " multimodal biometrics"	231
Secondary	"finger" AND " multimodal biometrics" AND "fusion"	160
	"fingerprint" AND " multimodal biometrics" AND "finger vein"	46
	"fingerprint" AND " multimodal biometrics" AND "finger knuckle print"	18
	finger vein" AND " multimodal biometrics" AND "finger knuckle print "	12
	"fingerprint" AND "finger vein" AND " multimodal biometrics" AND "finger knuckle print "	10
	"fingerprint" and "finger vein" and " multimodal biometrics" and "finger knuckle print "	12

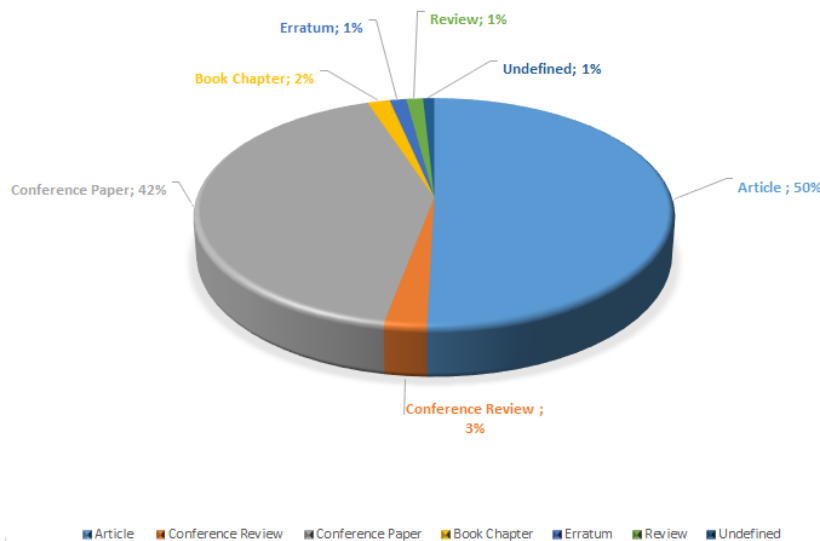
- **Language Based Analysis:** The result from the search analyses the type of language used for publishing the documents. Figure III.2.2 summarises the contribution based on the language of published documents for multimodal finger biometrics. In Figure III.2.2 , it is observed that English is the main language used by the researchers to publish their manuscripts and articles. Very few manuscripts are written in the Chinese language.



Language	Publication Count
English	229
Chinese	2

Figure III.2: Language wise trend analysis

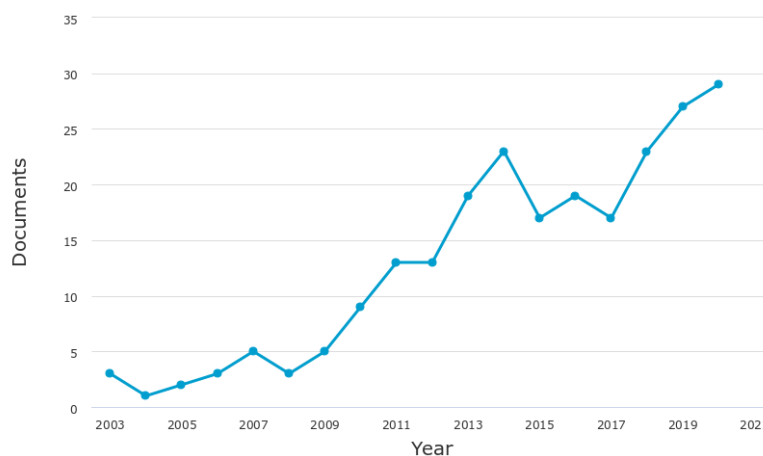
- **Document type-wise publication trend analysis:** Document type-wise list of documents that have been published for multimodal finger biometrics as shown in next Table. From the various document types, the maximum number of publications has been Articles, Conference papers and review papers also have been a substantial amount of publications but lesser than that of article publications. By drawing a pie chart we find a clear picture regarding the publication in various document types. The chart in Figure III.2 shows that maximum contribution is made in Articles followed by Conference papers and review papers. Others in the pi-chart include editorial, short review and book chapter, where the publications are not that significant.



Document Type	Publication Count
Article	115
Conference Paper	98
Conference Review	6
Book Chapter	4
Review	3
Erratum	3
Undefined	2

Figure III.3: Documents Source wise type analysis¹.

- **Documents by year Based Analysis:** Year wise publication in the recent years have been analysed. Next Table shows the number of publications that have been published from 2000 to 2020 for 231 *publication* using Scopus databases. There an flatness in the pervious yers followed by upward trend. We find that research have been gradually increasing over the years mostly during 2014 and has been a decrease in the 2015,2016 and 2017 years though a consistency has been maintained. Figure III.3 shows the graph which tells us about the publications in the last years. The publications have increasing trend over the recent years .The maximum publications was seen in the year 2020.



Year	Documents
2020	28
2019	27
2018	23
2017	17
2016	19
2015	17
2014	23
2013	19
2012	13
2011	13
2010	9
2009	5
2008	3
2007	5
2006	3
2005	2
2004	1
2003	3

Figure III.4: Documents by Year

¹Image source: <https://www.scopus.com/>(Accessed on February 5, 2020)

Some keywords that often appear in good currency papers are divided into five clusters (see Figure III.7), namely:

1. Cluster 1 (teal) consists of 8 keywords: biometrics, multimodal biometrics, finger knuckle print, fingerprint, finger vein, multimodal fusion, multibiometrics systems, and multimodal feature fusions.
2. Cluster 2 (purple) consists of 8 keywords: score level fusion, feature fusion, multimodal, features level fusion, multibiometrics, fusion, finger vein recognition and recognition accuracy.
3. Cluster 3 (yellow) consists of 7 keywords: feature expression, fusion recognition, finger biometrics, human, finger features, biometric recognition system and data fusion.
4. Cluster 4 (green) consists of 2 keywords: signal processing, biometry systems.
5. Cluster 5 (cornflower blue) consists of 3 keywords: finger, fingerprint and finger knuckle print.

The keywords that are divided into five clusters are arranged in coloured circles that show cluster indicators. This data can be used to find out the trend of keywords in the last year. The bibliometric analysis shows several widely used keywords in the papers, which are the object of research. The more keywords that appear, the wider the circle is shown. Meanwhile, the line relationship between keywords shows how much they are related to other keywords.

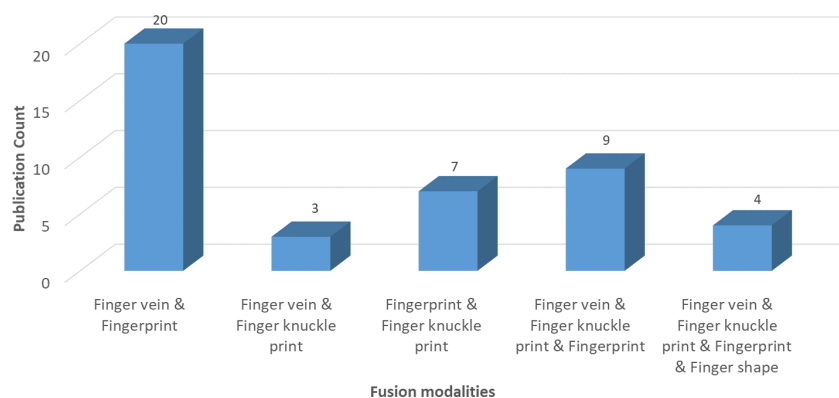


Figure III.8: Fused finger-based modalities of trend analysis

– Publication trend data Analysis

According to the PRISMA, the analysis of finger-based biometric papers after excluding the non-eligible documents (see Figure III.1). The selected documents included 43 papers for the qualitative synthesis. The documents are classified based on the biometrics used fused modalities (see Figure III.9) and their fusion levels (see Figure III.8). As shown in Figure III.9, based on finger biometrics, there are five modalities combinations which are: the fingerprint & finger vein, finger vein & finger knuckle print, fingerprint & finger knuckle print, finger vein & finger knuckle print & fingerprint and finger vein & finger knuckle print & fingerprint & finger shape. The fusion of fingerprint & finger vein is the most used combination in 20 documents, and the fusion of fingerprint & finger knuckle print is not widely used. The fusion of fingerprint & finger vein is the most used combination in 20 documents, and in the fusion of fingerprint & finger knuckle print, there are only 3 documents.

Using the same included data (43 documents), the analyses based on the fusion level-wise of the trend are present in Figure III.9. As presented in the wise, the fusion in the score level is the most used with 44% followed by the fusion in feature level with 37%. Besides that, the fusion in the fusion in rank level is not usually used with only 3%.

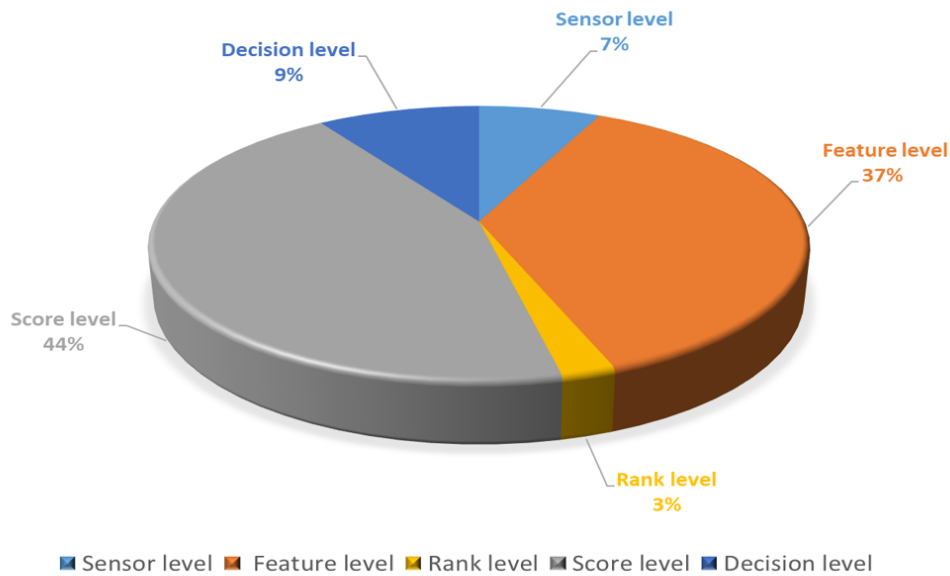


Figure III.9: Fusion level wise of trend analysis

– Citation Analysis

The data analysis of the most cited article is essential to identify the dominantly used algorithms and how they perform and get information about the performance and problem in the domain.

The analysis of finger-based biometric cited papers before excluding the non-eligible documents (see Figure III.1) are presented in Appendix A.3

The Top Ten documents are in descending order of citation; the count is shown in Table III.3 below, representing the years from 2013 to 2019. The analysis of the top citation paper provides us with an important clue about the used technique to focus on for starting the initial work and defining objectives. The maximum citation [75] count of 94 is obtained for paper used finger vein and finger knuckle print modalities where matching learning method is used. Table III.3, the analysis states that among the top ten cited papers, maximum papers are based on the machine learning method, and few articles have used the CNN/deep learning approach.

Table III.3: Top ten documents in the related field from the data collected from the Scopus database.

	Cites	Authors	Title	Year	Source
1	94	W Yang, X Huang, F Zhou, Q Liao	Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion	2014	Information sciences
2	75	Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C.	A fingerprint and finger-vein based cancelable multi-biometric system	2018	Pattern Recognition
3	58	Peng, J., El-Latif, A.A.A., Li, Q., Niu, X.	Multimodal biometric authentication based on score level fusion of finger biometrics	2014	Optik
4	41	S Veluchamy, LR Karlmarx	System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier	2017	IET Biometrics
5	36	Khellat-Kihel, S., Abrishambaf, R., Monteiro, J.L., Benyettou, M.	Multimodal fusion of the finger vein, fingerprint and the finger-knuckle-print using Kernel Fisher analysis	2016	Applied Soft Computing Journal
6	17	Peng, J., Li, Q., Abd El-Latif, A.A., Niu, X.	Linear discriminant multi-set canonical correlations analysis (LDMCCA): an efficient approach for feature fusion of finger biometrics	2015	Multimedia Tools and Applications
7	15	Arunachalam, M., Subramanian, K.	AES based multimodal biometric authentication using cryptographic level fusion with Fingerprint and Finger Knuckle Print	2015	Lecture Notes in Computer Science
8	9	Zhang, H., Li, S., Shi, Y., Yang, J.	Graph fusion for finger multimodal biometrics	2019	IEEE Access
9	7	Peng, J., Li, Q., Abd El-Latif, A.A., Niu, X.	Finger multibiometric cryptosystems: Fusion strategy and template security	2014	Journal of Electronic Imaging
10	5	Shanmugasundaram, K., Mohamed, A.S.A., Ruhaiyem, N.I.R.	An overview of hand-based multimodal biometric system using multi-classifier score fusion with score normalization	2018	Proceedings of IEEE International Conference on Signal Processing and Communication, ICSPC 2017

III.2.4 Deductions from Bibliometric Analysis

This section describes the research outcomes obtained after the overall analysis done on the core keyword, i.e. finger-based biometrics. The outcomes will provide some research goals and objectives that can be explored further to advance researcher in the field. As per the analysis done, we can answer the main Researcher Question presented in Table III.1. There is four biometrics in the finger: fingerprint, finger vein, finger knuckle print, and finger shape. Each of the four-finger biometrics has its own set of intrinsic weaknesses. The multibiometrics fusion and combination could be then the best solution to improve the biometric system performance. As detailed, there are 5 different combinations where the analysis indicate that fusion of finger vein and finger knuckle print is not wedly used. There are few works, but it is an important combination. The features level and scores level are the best levels for the fusion. A good number of papers used machine learning techniques, and few numbers used deep learning techniques. The analyses of ten top-cited article indicate that in literature there is two know popularly used data based SDUMLA-HMT [76] and PolyU [77].

III.3 Fingerprint Biometrics

The fingerprints are found at the tips of the fingers, on the palmer side of the last phalanx. They are formed of curved lines in relief on the skin, also called "ridges". These fingerprints are different on each finger and unique for each individual. The information provided by fingerprints, allowing to authenticate or identify an individual, is distinguished through three levels of precision as shown in the Figure III.10.

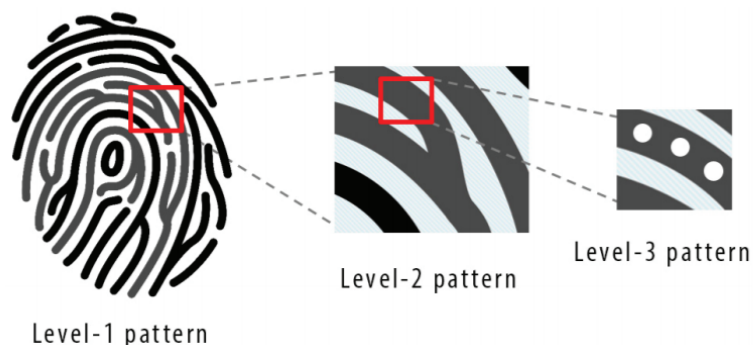


Figure III.10: Illustration of taxonomy of fingerprint feature levels ².

(Level-1 represents global fingerprint patterns, Level-2 represents local ridge details, Level-3 are fine details at microscopic scale like sweat pores)

- **Level-1** is the highest level of abstraction of pattern and represents overall fingerprint ridge flow. It is made up of general shapes, also called singularities. These patterns are usually divided into three categories (loops, whorls and arches). Each of these categories has various variations, as shown in Figure III.10. These singularities are approximated by estimating the local orientation of the ridges and can be detected from low-resolution images [78].
- **Level-2** is features or minutiae are local ridge characteristics that make every fingerprint a unique pattern (see Figure III.10). The premise of fingerprint uniqueness has been generally accepted, but still lacks proper scientific validation [78].

²Image source: FINGERPRINT RECOGNITION SYSTEM USING ARTIFICIAL NEURAL NETWORK AS FEATURE EXTRACTOR: DESIGN AND PERFORMANCE EVALUATION

- **Level-3** features are microscopic level patterns that are almost exclusively used by forensic examiners (see Figure III.10). They consist of sweat pore locations, ridge geometric details, scars and other very small characteristics. Lately, their computer automated extraction has been seriously considered as more and more biometric system vendors begin to adopt 1000 PPI (pixels per inch) sensing resolution of fingerprint images in their recognition systems [78].

III.3.1 Fingerprint Imaging Principle

In a fingerprint authentication system, the acquisition of the fingerprint image performs a key role. The imaging is a primary step in a recognition system involving the initial fingerprint image to support the different possible recognition treatments [21]. There are four types of fingerprint scanners: the optical scanner, the capacitance scanner, the ultrasonic scanner, and the thermal scanner. The essential function of every kind of scanner is to obtain an image of a person's fingerprint and find a match for it in its database [79].

- **Optical scanners:** take a visual image of the fingerprint using a digital camera.
- **Capacitive or CMOS scanners:** use capacitors and thus electrical current to form an image of the fingerprint. This type of scanner tends to excel in terms of precision.
- **Ultrasonic fingerprint scanners:** use high-frequency sound waves to penetrate the epidermal (outer) layer of the skin. Ultrasonic fingerprint scanners use high-frequency sound waves to penetrate the epidermal (outer) layer of the skin.
- **Thermal scanners:** sense the temperature differences on the contact surface, in between fingerprint ridges and valleys.

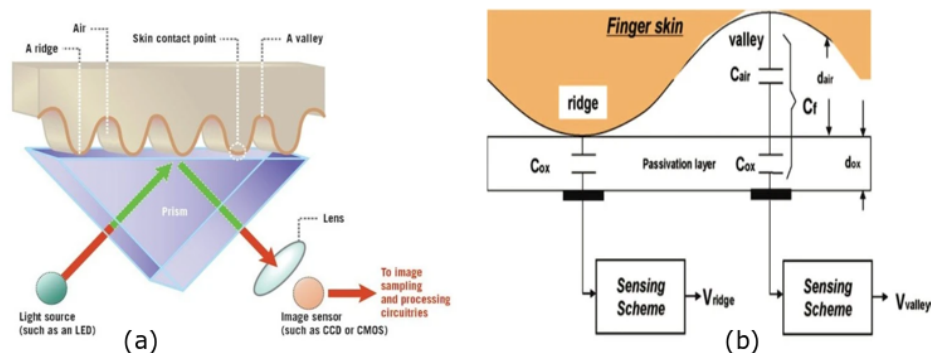


Figure III.11: Principle of fingerprint imaging:(a) Optical Fingerprint Scanners, (b) Capacitive Fingerprint Scanners ³.

III.3.2 Fingerprint Databases

In general, there are three types of fingerprint databases; latent fingerprints, Rolled fingerprints and Plain fingerprints [80, 81].

- **Latent fingerprints** are lifted from the surfaces of objects that are inadvertently touched or handled by a person through various means ranging from simply photographing the print to more complex dusting or chemical processing.

³Image source: <https://techpp.com/2019/03/26/types-of-fingerprint-scanners-explained/>

- **Rolled fingerprints** are achieved by moving a finger from nail to nail to capture the complete ridge finger details.
- **Plain or slap fingerprints** are obtained by pressing a finger onto a flat surface without movement.

Rolled and plain impressions are obtained by scanning the inked print on paper or directly using Livescan devices. Compared to rolled and plain fingerprints, the latent fingerprints have poor ridge clarity and complex background noise and consist of only a tiny part of a finger and sizeable non-linear skin distortion [80, 81]. Examples of the three types of fingerprints are shown in Figure III.12



Figure III.12: Example of Fingerprint acquisition; Left: Rolled print, Middle: plain or slap print and Right: latent print.⁴

There are a large number of fingerprint publicly available datasets; Among these, we can mention: SDUMLA-HMT Multi-sensor Fingerprint Database [76] and FVC2004 databases [82].

- **SDUMLA-HM fingerprint database** includes fingerprint images captured from the thumb finger, index finger and middle finger of both hands. To explore the sensor interoperability, they captured each of the 6 fingers with 5 different types of sensors, i.e., AES2501 swipe fingerprint scanner developed by Authentec Inc, FPR620 optical fingerprint scanner and FT-2BU Capacitive fingerprint scanner, both produced by Zhongzheng Inc, URU4000 optical fingerprint scanner designed by Zhongkong Inc and ZY202-B optical fingerprint scanner designed by Changchun Institute of Optics, Fine Mechanics and Physics, China Academy of Sciences. It is to be noted that 8 impressions were captured for each of the 6 fingers using each of the 5 sensors. SDUMLA-HM fingerprint database contains $6 \times 5 \times 8 \times 106 = 25,440$ fingerprint images in total. Every fingerprint image is saved in 256 grey-level “BMP” format, but the size varies according to the capturing sensors [76]. Some sample images of the fingerprint database are shown in Figure III.13.
- **FVC 2004 fingerprint database** for the third international Fingerprint Verification Competition. the database includes Four different databases that were collected by using the following sensors/technologies: DB1: optical sensor "V300" by CrossMatch, DB2: optical sensor "U.are.U 4000" by Digital Persona, DB3: thermal sweeping sensor "FingerChip FCD4B14CB" by Atmel and DB4: synthetic fingerprint generation. The images were acquired as fingerprints from thirty student volunteers (average age 24). Each volunteer was asked to present their fingerprint in three separate sessions, with at least two weeks separating each session. At the end of the data collection, a total of 120 fingers and 12 impressions per finger (1440 impressions) were gathered for each database (DB1, DB2, DB3 and DB4) [82]. Some sample images of the fingerprint database are shown in Figure III.14.

⁴Image source: <http://citeseerx.ist.psu.edu/viewdoc>

⁵Image source: <https://link.springer.com/content/pdf/10.1007%2F978-3-642-25449-9.pdf>

⁶Image source: <http://bias.csr.unibo.it/fvc2004/databases.asp>

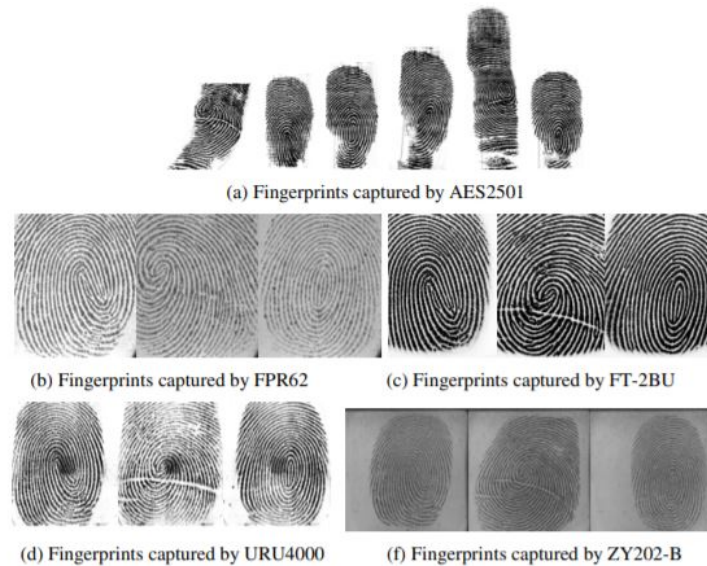


Figure III.13: Samples of images SDUMLA-HM fingerprint database.⁵

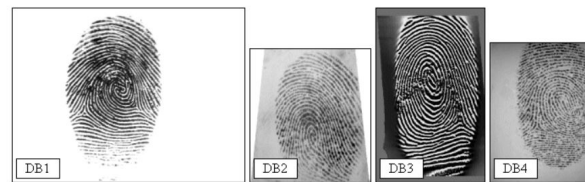


Figure III.14: Samples of images FVC 2004 fingerprint database.⁶

III.4 Finger Vein Biometrics

Recently in the literature [6, 47], a biometric method based on vascular patterns such as hand vein and peculiarly finger vein has interested the researchers. A finger vein biometric system came into existence after the invention of finger print. The veins are within of the human finger. Finger vein features offering varied other favourite advantages and these include [13, 83]:

- The finger-vein patterns are unique for every person, even identical twins. So, it offers good distinction between each individual.
- The patterns of finger vein are permanent, they does not change with time.
- The finger vein patterns are invisible to human's eyes. Consequently, they are not obscured and difficult to be replicated because it is located underneath the human's skin.
- The finger-vein patterns acquisition is considered to be very user-friendly. The vein pattern images captured non invasive. The finger vein device is contactless sensors, so his concept ensuring hygiene and convenience hygiene for the user.
- The human has ten fingers, if something incident happens to any one of the fingers, other fingers can be used as replacement for authentication.
- Finger-veins can only be captured from a living body. Hence, if a person is dead, it is impossible to steal his identity.

Regardless of the advantages mentioned above, there are defy that still need to be treated in order to achieve the higher performance wanted in real world deployments of finger vein biometric recognition [26].

III.4.1 Finger Vein Imaging Principe

The finger vein patterns are not visible for human eyes. However, they captured by sensors of **Near-infrared** camera which is sensitive to **NIR** light. There is two ways have introduced for finger vein image acquisition: light transmission method and light reflection method [47]. The main divergence between the approaches is the **Near-infrared (NIR)** position.

– Light reflection method

is a method where the **NIR** light source and the **NIR** camera situated along a similar position of the finger, the light source placed in palmer side of the finger, the reflected light from the finger will be acquired by the **NIR** camera as illustrated in Figure III.15. The vein pattern image formed by the differences in the intensity minutiae of the reflected light. After the vein absorbs the **NIR** light rays, the image shows poor light from the veins and bright light from the other parts surrounding the veins. The design of the finger vein capturing device is the significant advantages of the light reflection method, the **NIR** illuminating source, and the **NIR** camera are grouped to make the device more compact. The capturing devices easy to use and there is no blockage between the user and the device. Unfortunately, the image captured has a low contrast; this caused by strong reflection from the skin's surface and the poor penetration of **NIR** light rays under the skin. Moreover, the quality if the unevenness and grooves greatly influence the finger-vein pattern image on the skin's surface and thus it will meddle with the verification process. This phenomenon is known as the effect of reflection [15].

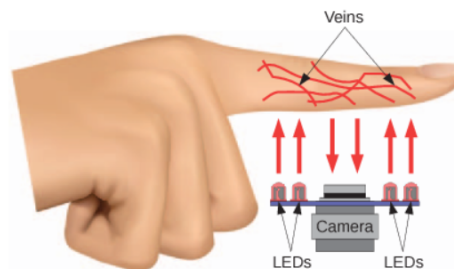


Figure III.15: Finger-vein pattern imaging : light reflection methods.⁷

– Light transmission method

is a method where the finger will place in between the **NIR** light source and the **NIR** camera; the light sources positioned in the dorsal side of the finger, the **NIR** light will penetrate across the finger and captured by the **NIR** camera such as shown in Figure III.16. Since the **NIR** light emits in the dorsal side of the finger, the haemoglobin in the blood absorbed the **NIR** light directly, the absorbed light to appear as a dark area and then captured by the **NIR** camera. Thus, the impact of reflection does not exist, and high-contrast vein pattern image can produce. Because of its advantages, compared to the light reflection method, light transmission is chosen to be the most suitable method for this project [15].

III.4.2 Finger Vein Databases

One of the greatest challenges to researchers is to get high image quality, so there are varied public finger vein databases, the five typical databases are as follows:

⁷Image source: <https://www.semanticscholar.org/paper/Contact-Less-Palm%2FFinger-Vein-Biometrics>

⁸Image source: <https://www.semanticscholar.org/paper/Contact-Less-Palm%2FFinger-Vein-Biometrics>

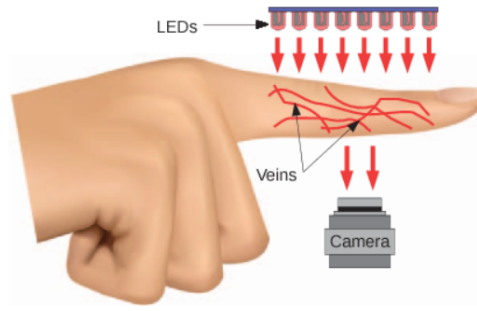


Figure III.16: Finger-vein pattern imaging : light transmission methods.⁸

The first one is named SDUMLA-HMT database, and it was a part of homologous multimodal databases [76]. Another finger vein database which is also a homologous multimodal databases known as HKPU-FV proposed by Ajay and Zhou [84]. The third database abbreviated as UTFV database was realized by B.T. Ton, R.N.J. Veldhuis from University of Twente [85]. The two finger vein databases were recently published at Chonbuk Ntion University [86] and Tsinghua University [87]. The previous database are named respectively MMCBNU-6000 database and THU-FVFDT database. The Table III.4 summarize mentioned databases all of them uses light transmission based image acquisition device. But the number of subject/finger is limited, also the image size, contrast, backgrounds and quality are different. Some of the samples are terribly skewed (misaligned) [13].

Table III.4: Comparison between finger vein databases

Database	dated	Image numbers	Subject numbers	Finger numbers pre subject	Image Size (Pixels)	Format	Typical Image
SDUMLA-HMT[76]	2010	3816	106	Index, Ring, middle of both hands	320 × 240	.bmp	
HKPU-FV [84]	2010	6264	156	Index, Ring, middle of both hands	513 × 256	.bmp	
UTFV [85]	2013	1440	60	Index, Ring, middle of both hands	672 × 380	8 bit gray scale .png	
MMCBNU-6000 [86]	2013	6000	100	Index, Ring, middle of both hands	672 × 480	.bmp	
THU-FVFDT [87]	2014	440	220	Index, Ring	200 × 100	.bmp	

III.5 Finger Knuckle Print Biometrics

The fingers of human hand has three bone segments and three joints as shown in Figure III.17. The joints named Metacarpophalangeal (MCP), proximal interphalangeal (PIP) and distal interphalangeal (DIP). The major finger knuckle position of (PIP) is the more useful part of the finger in biometric. In any knuckle print (see Figure III.17), there are lines like (i.e., knuckle lines) rich pattern structures in vertical as well as horizontal directions. These horizontal and vertical pattern formations are believed to be very discriminative. The main reason for using them is their unique anatomy; they are also non-invasive in nature and are quite stable which can be captured at low cost without any overhead of installing new hardware device [88].

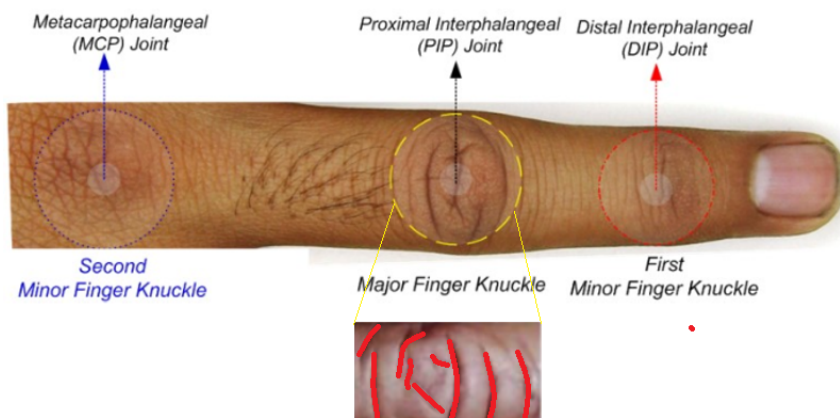


Figure III.17: Sample finger dorsal image to illustrate prior work in finger knuckle identification.⁹

III.5.1 Finger Knuckle Print Imaging Principle

The **Finger knuckle Print (FKP)** image acquisition module comprises a finger holder, an **LED** light source in the form of a ring, a lens, a **CCD** camera and an acquisition card. The **LED** light source and **CCD** camera are enclosed in a box to almost constant the luminance. A basal block and a triangular block are used to fix the position of the finger joint (see Figure III.18) [89].

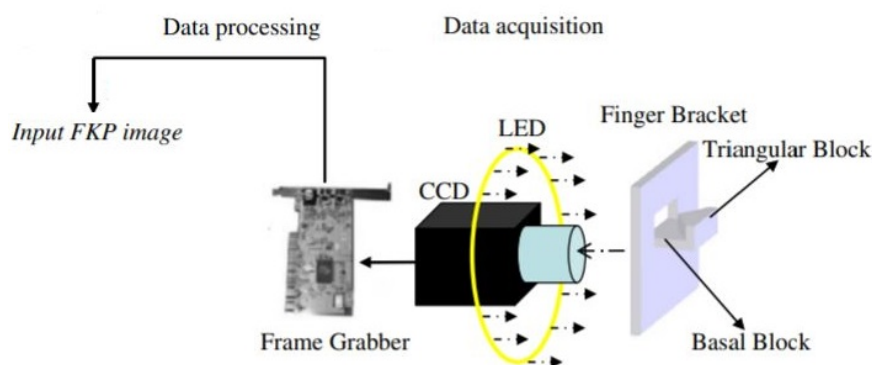


Figure III.18: Finger knuckle print data acquisition module.¹⁰

For the data acquisition, the user puts his finger on the base block by touching the two slopes of the triangular block (see Figure III.19).

⁹Image source: <https://web.comp.polyu.edu.hk>

¹⁰Image source: <https://www.sciencedirect.com/science/article>

¹¹Image source: <https://www.sciencedirect.com/science/article>




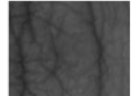


Figure III.19: Finger Knuckle Print (FKP) Acquisition Device.¹¹

III.5.2 Finger Knuckle Print Databases

There exist four publicly available well-known finger knuckle print databases Table III.5, namely, PolyU FKP database [77], IITD FKP database [90], The Hong Kong Polytechnic University Contactless Finger Knuckle Images Database [91] and The Hong Kong Polytechnic University Contactless Hand Dorsal Images Database [92].

- **The PolyU Finger Knuckle Print Database [77]** is collected from 165 individuals that include 125 males and 40 females using an automated low-resolution camera in a peg free environment. This finger knuckle image capturing system collects the knuckle images from persons in two different sessions. In each session, a person submits 6 images of his/ her four different finger knuckle surfaces. The four finger knuckle images were captured from left index finger knuckle, left middle finger knuckle, right index finger knuckle and the right middle finger knuckle regions. Therefore, 24 images were collected from each person in one session. Totally, each person submitted 48 images in two sessions. The database of the finger knuckle surface images consists of totally 7920 images. These images were obtained from 660 different finger knuckle surfaces.
- **IIT Delhi Finger Knuckle Database [90]** this database has been created by capturing finger back knuckle region using low resolution digital camera in a contact less manner. This database consists of finger knuckle images collected from 158 users belonging to the age group from 16 to 55 years. Totally, there are 790 finger knuckle images present in the database. These images are sequentially numbered using integer identification for each and every user. Since the entire finger back region has been captured.
- **The Hong Kong Polytechnic University Contactless Finger Knuckle Images Database (HKPU FKP) [91]** is contactless finger knuckle images database contributed from the male and female volunteers. This database has been largely acquired in The Hong Kong Polytechnic University campus and IIT Delhi Campus using a contactless setup that simply uses a handheld camera. This database has 2515 finger dorsal images from the middle finger of 503 subjects, all the images are in bitmap (*.bmp) format.
- **The Hong Kong Polytechnic University Contactless Hand Dorsal Images Database (HKPU HDI) [92]** is contributed from the male and female volunteers. This database has been largely acquired in IIT Delhi Campus, in The Hong Kong Polytechnic University campus by using a mobile and hand held camera. This database has 2505 hand dorsal images from the right hand of 501 different subjects that illustrate three knuckle patterns in each of the four fingers from the individual subject. All the images are in bitmap (*.bmp) format. The combined database from 712 different subjects hand dorsal images is made publicly available.

Table III.5: Finger Knuckle Print Databases

Database	Dated	Subjects	Total Images	Images Size	Typical Image
PolyU FKP [77]	2009	165	7920	110 x 220	
IIT FKP [90]	2009	158	790	80 x 100	
HKPU FKP [91]	2014	503	2515	160 x 180	
HKPU HDI [92]	2016	501	2505	100 x 100	

III.6 Conclusion

The Bibliometric analysis done in this chapter tends to provide some future research directions in finger-based biometrics to analyse the research trends. From the bibliometric study and analysis, it is observed that there are several researchers involved in the field of finger based biometrics. The information retrieved has four biometrics in the finger: fingerprint, finger vein, finger knuckle print, and finger shape. The multimodal systems are based on different combinations where the analysis indicates that fusion of finger vein and finger knuckle print is not widely used. There are few works, but it is an essential combination. The research shows that machine learning techniques and deep learning techniques are used for recognition and treatment. Therefore, in the next chapter, we will outline the deep learning and machine learning domain.

CHAPTER IV

DEEP LEARNING OVERVIEW

Contents

IV.1 Introduction	69
IV.2 Machine learning Overview	69
IV.2.1 Machine Learning types	70
IV.2.2 Machine Learning "Classic"	71
IV.3 Artificial Neural Network	75
IV.4 Deep Learning and Convolutional Neural Networks overview	76
IV.4.1 Convolution Neural Network (CNN)	77
IV.4.2 Convolution Neural Network (CNN) trend Architectures	79
IV.5 CNN training workflow and Transfer Learning concept	82
IV.5.1 Training workflow	82
IV.5.2 Data augmentation and transfer learning	83
IV.6 Conclusion	83

IV.1 Introduction

Artificial intelligence is becoming an important tool that has an impact on our daily life, especially in the field of security systems and biometrics. We are witnessing the success and advancement of artificial intelligence in various domains every day. Nowadays, we are using intelligent algorithms to unlock smartphones just by showing them our faces or using fingerprint characteristics. Also, AI allows us to perform E-shopping easily and with high flexibility by speaking to a virtual assistant, like Amazon's Alexa, that can understand natural language. All the aforementioned amazing applications are based on deep learning algorithms, such as **Convolution Neural Network (CNN)**, **Recurrent Neural Networks (RNN)**, **Generative Adversarial Networks (GAN)**, among others. Over the last few years, deep learning architectures have increasingly been adopted to perform many tasks in a wide range of applications, including computer vision, **Natural Language Processing (NLP)**, biometrics, fraud detection, to name a few. These algorithms provide better results than traditional techniques achieving impressive results that bypass the human level. In the present chapter, we aim to introduce the concept of one of the most powerful deep learning-based algorithms, which is **Convolution Neural Network (CNN)**, as well as introducing its most known architectures, including *AlexNet*, *VGGnet*, and *ResNet*. Also, the **CNN** training workflow all along with transfer learning and fine-tuning techniques are presented.

IV.2 Machine learning Overview

We are living in the era of big data, where we need efficient and advanced tools to handle such an amount of information.

As described in Figure IV.1, machine learning (Machine Learning) is a subset of artificial intelligence. The particularity of Machine Learning is that the methods used allow the machine to learn to perform a task based on large input datasets. Machine learning has emerged as an effective solution for data analytics, which has become an indispensable tool for various applications in different domains, from medical diagnosis to electronic payment. Machine learning could be defined as a subset of artificial intelligence that aims to give computers the ability to learn from data without being explicitly programmed by extracting patterns [93]. Deep learning is a subset of machine learning. In the form of layers, Deep Learning implements a sequence of algorithmic treatments specific to Machine Learning to respond to a complex problem cut into several tasks, each layer using the output of the previous layer as input data[94].

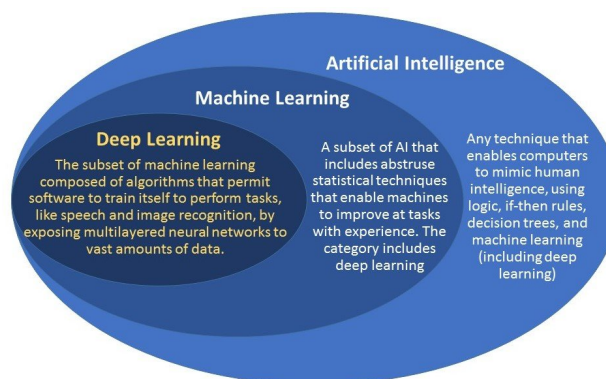


Figure IV.1: Relations between "Artificial intelligence", "Machine learning" and "Deep learning"¹.

In traditional programming methods, the computers follow the instructions given by the programmer to process the input data, and according to them, they give us answers (see Figure IV.2

¹Image source: geospatialworld.net/machine-learning-and-deep-learning

(Top)). Whereas, in the case of machine learning, we fed to the model the data and the corresponding output and it returns the rules to solve a specific task by exploring the relationship between the pair (data, answers) (see Figure IV.2(Bottom)). Thus, we begin this chapter with an overview of the different machine learning types followed by their limitations and challenges.



Figure IV.2: Traditional programming (Top) VS Machine learning (Bottom).

IV.2.1 Machine Learning types

The power of machine learning is the ability to generate strong rules from training data to perform complex tasks that were impossible using traditional programming techniques, such as object detection, fraud detection, recommendation engines, and speech recognition. Machine learning algorithms are divided into three main categories; supervised, unsupervised, and reinforcement learning (see Figure IV.3).

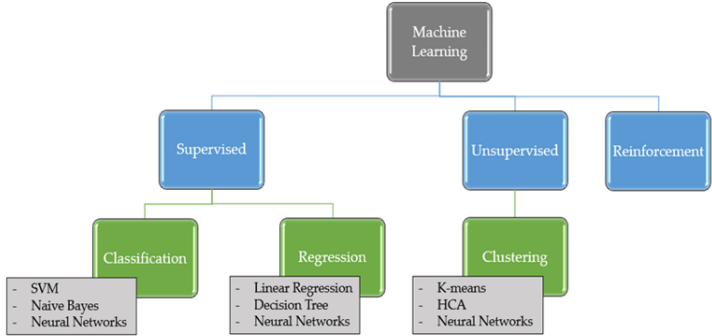


Figure IV.3: Machine learning types.

- **Supervised learning** is the most known and used machine learning category, which aims to map an input to its corresponding output according to the input-output pairs. These types of algorithms require labeled datasets to be fed to the machine learning model for the training process. The trained model is used to perform prediction on new unseen data, where it could be categorized into classification and regression according to the deserved output. The classification task goal is to predict the category of new input data based on the past acquired knowledge, where the model output is a discrete value. E-mail filtering is a well-known classification example that aims to classify incoming emails into a spam or not spam. Also, person identification through fingerprints or facial recognition is another example of a supervised classification task. On the other hand, the regression models aim to predict a numerical output value from an input value. Houses prices prediction and stock market forecasting are some examples of supervised regression applications. However, in supervised machine learning, we need to do the labeling task manually, which is a hard and tedious operation that takes a lot of time. K-Nearest Neighbors, Linear Regression, Logistic Regression, Support

Vector Machine (SVM), Decision Trees, Random Forests, and Neural Networks are among the most used supervised learning algorithms.

- **Unsupervised learning** is another machine learning type that aims to handle unlabeled data. In unsupervised learning, we feed to the model raw data without any labels, where the model performs some processing to extract similarities in the input data. According to the extracted similarities, the model will group the input data into different clusters. The unsupervised learning algorithms are usually used for clustering, anomaly detection, and dimensionality reduction, where K-means, **Hierarchical Cluster Analysis**, One-class **SVM**, **Principal Component Analysis**, and Neural Networks are the most known unsupervised learning algorithms [95, 96].
- **Reinforcement learning** takes its name from the fact that learning is enhanced with each iteration of the process by feedback. The algorithm’s performance is maximized as it makes decisions based on its training data. The algorithm is immersed in an environment, and makes its decisions based on its current state. After each learning step, the environment returns a reward, which can be positive or negative, depending on the outcome of the previous step. Thus, through iterated experiments, the algorithm seeks optimal decision-making behavior, so that it maximizes the sum of the rewards over time.

IV.2.2 Machine Learning "Classic"

As described above, the Learning machine is a sub-family of artificial intelligence. What we consider as "classical" Learning machine or "traditional" corresponds to this family to which we exclude the sub-family of Deep Learning. Thus, classical Machine Learning corresponds to the algorithms and methods now developed of state of the art and have proven their reliability of many problems [93].

As shown in Figure IV.4, in machine learning, the general processing chain has several essential steps such as **Region Of Interest (ROI)** detection and cropping, preprocessing to improve the image enhancement in the desired direction followed by a potential normalisation, the extraction of characteristics or features as well as their selection. Then the classification performing either learning of a model or a prediction from the training model. This prediction gives rise to a decision that, based on multiple results averaged on an image database, provides a specific amount of information to evaluate the model’s performance.



Figure IV.4: Process of image classification steps common to most applications.

- **Region Of Interest (ROI)**: The first step is to extract the area of interest where the elements you want to classify are located. This step (see Figure IV.4), while optional, helps reduce the influence of unnecessary data in the image. For example, in the case of finger vein recognition, it is essential to isolate the finger vein from the image’s background. On the other hand, in multiple detections (pedestrians, cars, signs, etc.), the information is distributed throughout the image.

- **Preprocessing:** or pretreatment is a significant step in the image classification process (see Figure IV.4). Manipulation of the image (filtering, segmentation, enhancement, etc.) makes it possible to reinforce or appear the essential elements in the images. Also, they while reducing the useless contributions. The normalisation phase keeps the images used for learning homogeneous. The images are resized to the same dimension or rotated, which maintain a similar orientation of the subject.
- **Features Extraction:** Feature extraction allows visual information to be transcribed into more stable and understandable information by the training algorithm. Based on the statistical distribution of data, specific algorithms make it possible to find the characteristics common to the images of a single class or to detect the features that best discriminate one class from another while seeking to reduce the impact of the characteristics common to several classes [20]. Feature extraction is a crucial step in the image classification processing chain (see Figure IV.4), and the methods used in the literature can be grouped into two main categories [97], as shown in Figure IV.5, global and local methods.

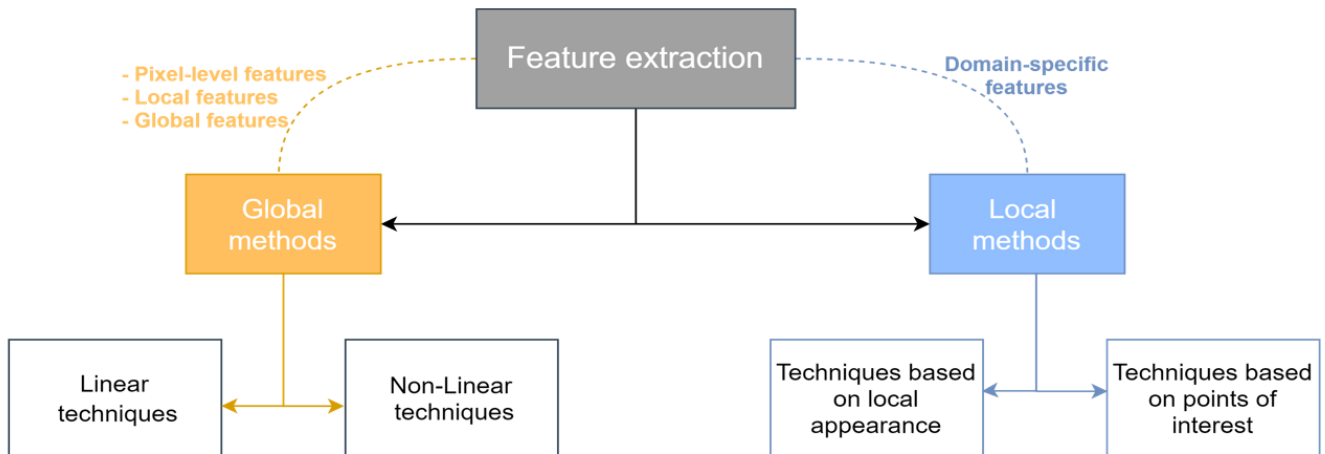


Figure IV.5: Categories of feature extraction methods in the image.

The global methods are based on independent features and focus on characteristics such as textures, colour or even shapes. Three levels of abstraction can be considered for these characteristics: the pixel level (colour, coordinates in the image, etc.), the local level (features resulting from image subdivision, segmentation, or other) and the level global (characteristics derived from the entire image or a single region of the image). The global methods used the whole section of the image. The used image is represented as a matrix of pixels, transformed into a vector of pixels for ease of handling. These approaches are sensitive to acquisition changes (orientation, lighting, etc). Considering the used methods, this category groups together two types of techniques: *linear* and *nonlinear*.

Linear techniques perform a linear projection of the input data, represented in a very large space (depending on the number of pixels and channels of the image), in a new relatively small space dedicated to the "subject". This space is made up of characteristics specific to the types of elements observed. Many techniques can be classified as linear: **Principal Component Analysis (PCA)** [98, 99], **Independent Component Analysis (ICA)** [100], **Linear Discriminant Analysis (LDA)** [101], Gabor wavelets and many other approaches. When the structure of the input data is *nonlinear*, one solution is to use a kernel function. In this case, a large-dimensional space is created in which the representation of the problem becomes linear. We can adapt linear methods to address this problem by adding a kernel [102]. Thus,

we find the [Principal Component Analysis \(PCA\)](#) with kernel [103], [Independent Component Analysis \(ICA\)](#) with kernel [104], [Exponential Discriminant Analysis \(EDA\)](#) [105] and many other approaches.

Local methods, dealing only with characteristics very specific to the type of information observed in the image, can be divided into two categories: techniques based on local appearance and techniques based on points of interest. Local appearance based techniques divide the image into small regions or "patches" from which local features are directly extracted. Once these regions have been defined, the next step is to choose the best way to represent the information of each region. The characteristics most generally used in the literature are the Gabor coefficients [106], Haar wavelets [107], [Scale-Invariant Feature Transform \(SIFT\)](#) [108], [\(Local Binary Pattern \(LBP\)](#) [109], [\(Local Ternary Pattern \(LTP\)](#) [110], and many other approaches. Point of interest based techniques first detect these specific points, subsequently allowing the extraction of features representing the various relationships between these points, such as their distance or angle. This type of extraction is performed with approaches such as [\(Dynamic Link Architecture \(DLA\)](#) [111], Gabor filter extraction [112], etc.

A third category could be defined as hybrid methods combining techniques from the Local methods, the global methods and new methods based on statistical models [97].

– **Classification:**

The feature extraction thus provides a vector composed of elements representing its characteristics. The next step in the chain is classification (see Figure IV.4).

There are two categories for classification the feature-based and distance-based classification.

The distance-based classification purpose is to calculate the degree of similarity between two vectors (target and measured characteristics) or between one vector (measured characteristic) and a set of vectors (forming a class). This comparison can be made in different ways, more or less effective depending on the complexity of the data (vector dimensions, interclass variance, class separation, etc) [20]. In literature [20] there are several number of distance based classifier au example Euclidean distance and Mahalanobis distance.

Let be two vectors x (target characteristics) and y (measured characteristics) of n elements $\vec{x}(x_1, \dots, x_i, \dots, x_n)$ and belonging to a normalized vector space E , such that $\vec{y}(y_1, \dots, y_i, \dots, y_n)$ are both elements of \mathcal{R}^n .

The distance between these vectors denoted $d(x, y)$, is a measure between each of their components i two by two $1 < i < n$ and can be defined in several ways:

- **Euclidean distance:** Euclidean distance is the shortest distance between two vectors, also known as the bird's-eye distance. It derives from the Minkowski distance [20].

$$d(\vec{x}, \vec{y}) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \quad (IV.1)$$

- **Mahalanobis distance:** it differs from the *Euclidean* distance [20] in that it considers the variance and correlation of the data series. Thus, unlike the *Euclidean distance*, where all the components of the vectors are treated independently and in the same way, the spread of *Mahalanobis* grants a less critical weight to the most dispersed elements.

$$d(\vec{x}, \vec{y}) = \sqrt{(\vec{x} - \vec{y})^T \Sigma^{-1} (\vec{x} - \vec{y})} \quad (IV.2)$$

Where Σ^{-1} is the inverse of the covariance matrix between the vectors x and y .

The feature-based classification is divided into two phases: training and testing. During learning, the classifier uses the characteristics of the training images to build a model based on rules that best separate classes. Depending on the application and the images used, it is necessary to adjust the classification parameters. Learning can be improved using a cross-validation technique, allowing images to be split into several groups and learn about each of these groups of varying parameters.

The use phase allows, from the characteristics of an unknown image, to determine the membership of the sample to a particular class using the classification model. Thus this model provides the label of the predicted class and the associated score attesting to the probability of a good prediction. The decision step is to define whether or not the prediction of the model is correct. The predicted class is used directly, or a threshold can be defined and adjusted on the prediction score to consider a prediction only if the score is higher than the threshold set. Finally, the evaluation allows quantifying the model's performance with metrics calculated from information from prediction results on test images. These metrics make it possible to compare models between them and thus select the optimal model in a given case.

When learning, bad distribution of input data and a poor configuration of classification can lead to "over-learning" or "under-learning". Over-learning corresponds to a model that considers details and noise essential data, leading to excellent performance during learning but very bad on new unknown images. Under-learning refers to a model that is unable to provide good learning performance or new data.

There are several features-based classifiers; the relative comparison between widely used and most popular supervised classification algorithms is made [20, 113, 114]. Among the linear classifiers, we find the Decision tree, Naive Bayes, [K-NN](#), [SVM](#). Table IV.1 present a comparative study on a widely used supervised classification algorithm.

Table IV.1: A comparative study on widely used four supervised classification algorithm

Comparison parameters	Decision tree	Naive Bayes	K-NN	SVM
Learning speed	Average	Best	Best	Worst
Classification speed	Best	Best	Worst	Best
Performance with presence of missing value	Average	Best	Worst	Good
Performance with non-relevant features	Average	Good	Good	Best
Noise tolerance	Good	Average	Average	Good
Performance on discrete/binary attribute	Good	Average	Average	Worst
Tolerance with parity problems	Good	Worst	Worst	Average
Clarity on Classification prediction	Best	Best	Average	Worst
Handling of model parameter	Average	Best	Average	Worst
Overall accuracy	Good	Worst	Good	Best

The comparative study of the above-mentioned shows that the [Support Vector Machine \(SVM\)](#) is the significant classifier. [Support Vector Machine \(SVM\)](#) are not new but are still a powerful tool for classification due to their tendency not to overfit, but to perform well in many cases.

Support Vector Machine (SVM) also known as Support Vector Networks is mainly used in machine learning, especially in the deep of learning process. SVM is a kind of linear classifier, which can classify the data extracted in advance and give each data specific score as the basis of evaluation. And the classification of the extracted data is one of the most important aspects in deep learning. The extracted data is generally in the form of N-dimensional vectors, so that's why it is called Vector Machine [115, 116].

IV.3 Artificial Neural Network

Artificial Neural Network (ANN) are special classes of machine learning algorithms that are inspired by the structure of the biological human brain. They consist of artificial neurons that receive signals from other neurons and perform some basic mathematic operations like addition and multiplication to generate an output that will be transferred to other neurons. The neuron is a linear transformation of an input value followed by a nonlinear function, commonly known as the activation function (see Figure IV.6). The activation functions are a fundamental key to artificial neural networks, which are mathematical equations used to determine the output of each neuron. For example, the ReLU activation function takes the positive values and gets rid of the negative ones.

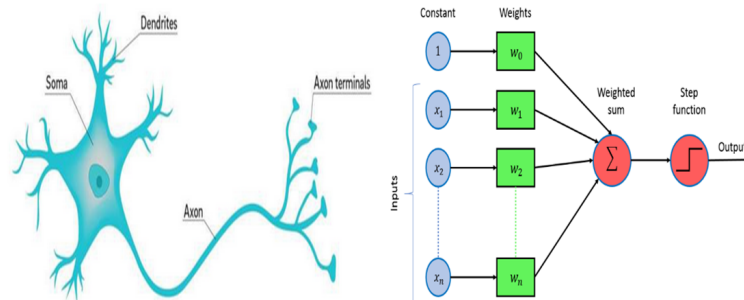


Figure IV.6: Biological (left) vs Artificial neuron (right).²

The output of an artificial neuron can be represented by the following equation: $f(\sum_{i=1}^n w_i x_i + b)$, where f is the activation function (for example *ReLU*, *tanh*, *sigmoid*), w_i are the associated weights to each input, x_i are the inputs (for example pixels values in the case of image) and b is the bias. Figure IV.7 shows examples of the most known activation functions.

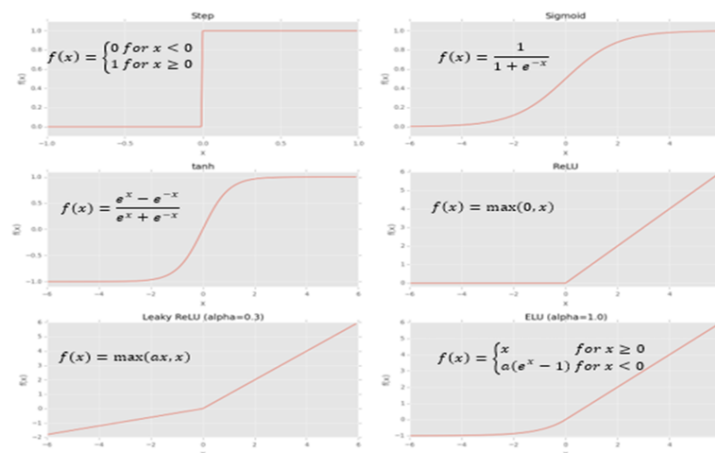


Figure IV.7: Examples of activation functions.

²Image source: educba.com/perceptron-learning-algorithm/

Any ANN consists of three main types of layers: the input layer, the hidden layer, and the output layer (See Figure IV.8). The input and output layers receive all the inputs to give the desired output respectively. Whereas, the hidden layers perform the processing to extract the relevant features. When we have more than two hidden layers, the artificial neural network is called Deep Neural Networks (DNN) or Multi-Layer Perceptron (MLP) (See Figure IV.8).

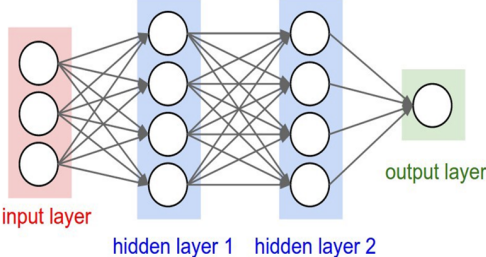


Figure IV.8: Example of Multi-Layer Perceptron.³

IV.4 Deep Learning and Convolutional Neural Networks overview

Single-layer and shallow neural networks perform very well to solve some basic problems, such as predicting house prices. However, they are insufficient to handle complex problems because they cannot extract enough information from the input data. Recent advances that have occurred in the processing power and the availability of a huge amount of data have made it possible to train and execute complex and deep neural networks in a faster and more accurate way.

Deep learning is a special type of machine learning that is based on neural networks. The main difference between traditional machine learning and deep learning algorithms is the ability of automatic feature extraction. In traditional machine learning techniques, we need to extract relevant features manually, which is a very difficult task and has low performance on complex problems like self-driving cars. However, deep learning architectures can extract more valuable features automatically (See Figure IV.9) [95, 117]. Table IV.2 shows the main differences between traditional machine learning algorithms and deep learning algorithms in terms of performance, required data, and feature extraction methods.

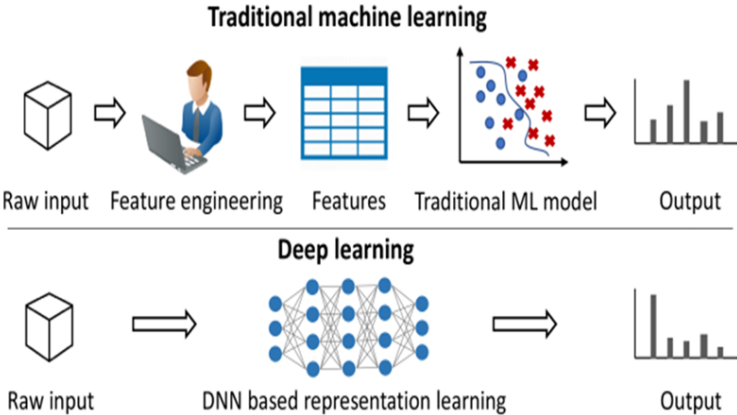


Figure IV.9: Traditional machine learning vs deep learning pipelines.⁴

³Image source: pianalytix.com/perceptronmultilayer-neural-network-algorithm/

⁴Image source: cacm.acm.org/magazines/241703-techniques-for-interpretable-machine-learning

Table IV.2: Comparison between biometric modalities

	Data	Accuracy	Training time	Hardware	Feature Extraction
Machine learning	Small datasets	Relatively low	Relatively low	CPU	Manually
Deep Learning	Large datasets	High	Very long	Powerful GPUs	Automatically

Deep learning can build powerful systems that are capable of solving complex problems that were impossible a few years ago. Nowadays, we can develop systems that can identify peoples with a very high accuracy either through facial, fingerprint, or other individual characteristics.

Deep learning is a branch of machine learning algorithms that is based on deep neural networks, including [MLP](#), [RNN](#), Autoencoders, Generative Adversarial Networks, among others. In this study, we are interested in one of the most powerful deep learning algorithms to solve computer vision-related problems, which is [Convolution Neural Network \(CNN\)](#). [CNN](#) applications are not limited to image analysis and computer vision tasks, but they could be used for speech recognition and recommender systems achieving remarkable results. Therefore, in this section, we will present the fundamentals of [CNN](#) architectures [96].

IV.4.1 Convolution Neural Network (CNN)

Convolutional Neural Network is a special type of deep neural networks. Due to the technological advancement in terms of computational power, efficient software, and a large amount of training datasets, [CNN](#) architectures achieved state-of-the-art results in computer vision and image processing applications, including image classification and object detection [118, 119]. A typical [CNN](#) architecture consists of three main components (layers), which are the convolutional layer, pooling layer, and dense layer (see Figure IV.10). In the following subsections, we are going to provide a detailed description of each layer and its main role.

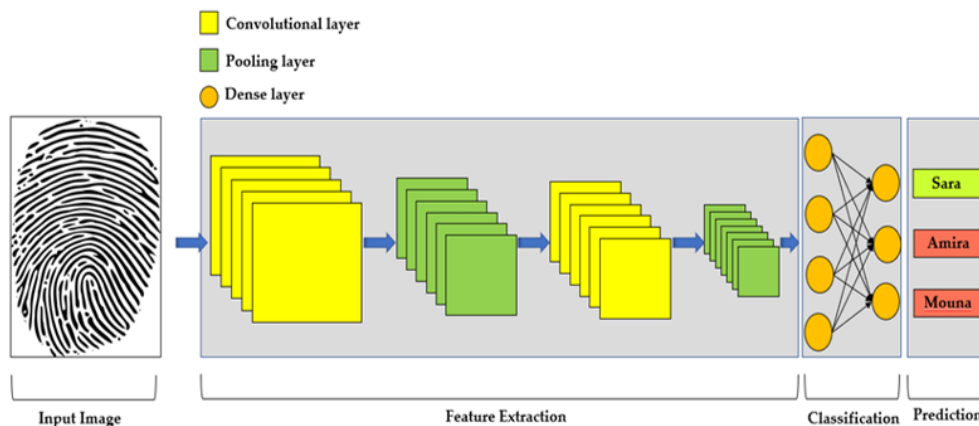


Figure IV.10: Standard [CNN](#) architecture.

- **Convolutional layer:** It is considered as the fundamental building block of any [CNN](#) architecture, which aims to extract automatically the most effective features from an input image. The convolutional layer generates feature maps by applying different sets of trainable filters, also called kernels, at each layer that could be hundreds or even thousands, where each of these filters is responsible for detecting a specific feature. The convolutional layers are

always followed by non-linear activation functions, such as *ReLU*, to introduce the nonlinearity in the network. Figure IV.11 shows how convolution operation is applied on input 2D data to generate a feature map, where we have a (6×6) input image convolved with a (3×3) kernel to generate a feature map of size (4×4) .

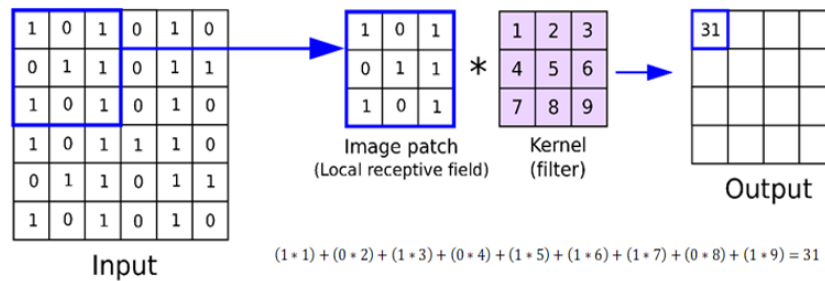


Figure IV.11: Convolution operation⁵.

There are four fundamental hyperparameters that we should take care of to define a convolutional layer. The first hyperparameter is the number of convolutional filters in each layer that represents the depth of the output feature map, where the number of the feature maps equal to the number of filters. The convolutional filter size is another crucial hyperparameter that determines the height and width of the output feature map. The choice of filter sizes depends on the details that we want to capture, where small filters can capture fine details while the bigger ones can miss these details that could be very important in some cases. In convolution, the stride and padding hyperparameters control the shape of the output feature map, where they refer to the operations that control the number of steps we take in each phase and the size of the output image/feature map, respectively. Thus, their main role is to keep all the important details of the image before transferring them to the next layer.

– **Pooling layer:**

After the generation of the feature maps, a pooling operation will be applied to each feature map. The main role of the pooling layers, also called subsampling layers, is to reduce the dimensionality of the generated feature maps, thus, reducing the overall number of learnable parameters, while keeping the most relevant and important features. Also, it could prevent or reduce the overfitting issue. There are two types of pooling operation; *max-pooling* and *average pooling*. The latter takes the average value in an image or feature map patch (See Figure IV.12). However, the *max-pooling* operation, which is the most used type, takes the maximum value among the image/feature map patch (See Figure IV.12).

- **Dense layer:** After extracting the features from the input image using convolutional and pooling layers, dense layers use these features to classify the input image into the corresponding category. The dense layer is just a regular feedforward neural network, where each neuron in a specific layer is fully connected to the neurons in the previous layer. The dense layer is always placed at the end of the CNN architecture, just after the last pooling layer. It performs the classification task using the *sigmoid* or *softmax* activation function for binary or multiclass classification, respectively.

Batch normalization and dropout could be considered as other types of layers that could be used to speed up the training process and improve the model performance.

⁵Image source: <https://anhreynolds.com/blogs/cnn.html>

⁶Image source:



Figure IV.12: Max-pooling vs average pooling operations.⁶

IV.4.2 Convolution Neural Network (CNN) trend Architectures

Yann Lecun developed one of the early successful CNN architectures called **LeNet-5** [120], which is a five-layer neural network used for handwritten digits recognition. At that time, it was adopted by *US* post to automatically identify *ZIP* codes. However, LeNet architecture was not able to perform complex tasks due to the low processing power and data scarcity. In the following subsections, we are going to present more advanced and efficient CNN architectures.

- **AlexNet:** Krizhevsky et al. [121] brought the main breakthrough of computer vision applications, where they proposed an efficient CNN architecture that can classify high-resolution images with impressive precision. *AlexNet* architecture won the 2012 *ImageNet* competition with a top-5 error rate of 16.4% outperforming the 2011 winner that achieved a top-5 error rate of only 25.8%. *AlexNet* architecture consists of five convolutional layers followed by Rectified Linear Unit (*ReLU*) activation function, where the first, second, and the fifth convolutional layers are followed by max-pooling layers. The outputs of the last max-pooling layer are flattened and fed to three dense layers to classify the extracted features into their corresponding classes (See Figure IV.13).

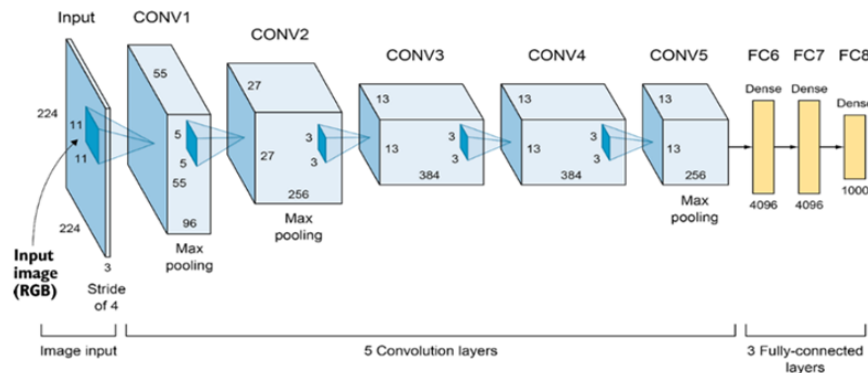


Figure IV.13: AlexNet architecture⁷.

- **VGGnet:** In 2014, the Visual Geometry Group at Oxford University [8, 122] developed a CNN architecture that has the same building blocks as its predecessors *LeNet* and *AlexNet*, but with more layers and a slightly different structure. Also, *VGGnet* used multiple smaller filter sizes of (3x3) instead of (11x11) and (5x5) adopted in *AlexNet*. Thus, unlike *AlexNet* that uses larger kernel sizes, *VGGnet* can extract finer features providing better results, where it achieved a top-5 error rate of 7.3% in the *ImageNet* competition.

⁷Image source: ivebook.manning.com/book/AlexNet

There are two main types of VGGnet architectures, where the first one consists of 16 layers and the second one consists of 19 layers. The 16 layers version (*VGG-16*) is the most adopted architecture in the literature. *VGG-16* architecture consists of 13 convolutional layers and 3 dense layers organized as shown in Figure IV.14.

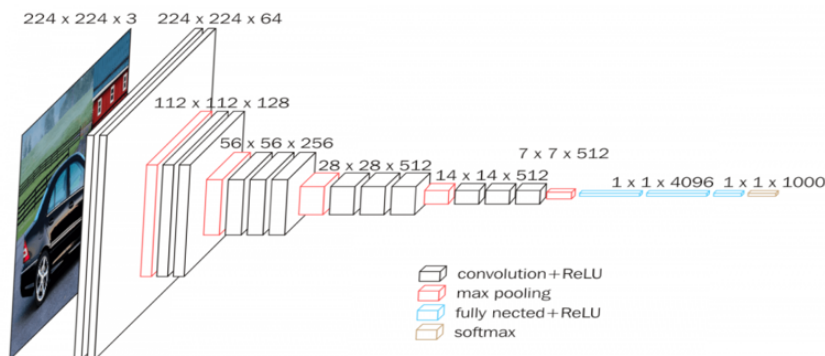


Figure IV.14: AlexNet architecture ⁸.

– **GoogLeNet (Inception):**

Szegedy et al.[123] developed another deep CNN architecture called *GoogLeNet* (or Inception later) that consists of 22 layers. Unlike traditional CNN architectures that are based on stacking convolutional and pooling layers on top of each other, *GoogLeNet* introduced a new concept called "inception module" to perform the different operations in parallel, where each module consists of convolution filters of sizes (1×1) , (3×3) , and (5×5) and (1×1) max-pooling layer Figure IV.15.

GoogLeNet architecture stacked the inception modules one after the other to build a deeper CNN (See Figure IV.16) that can optimize the utilization of the computing resources and reduce the number of trainable parameters inside the network while providing better results than the previous architectures achieving a top-5 error rate of 6.7% that allowed it to win the 2014 *ImageNet* competition[124]. Other versions of Inception architecture were developed achieving even better results, such as *Inception v3*, *Inception v4*, and *Inception-ResNet* that achieved a top-5 error of 5.6%, 4.01%, and 3.08% respectively on the *ImageNet* dataset[125].

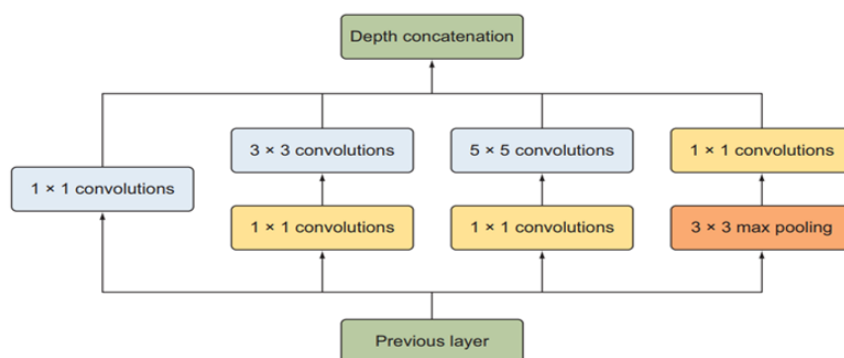


Figure IV.15: Inception module.⁹

– **ResNet:**

⁸Image source: neurohive.io/popular-networks/vgg16

⁹Image source:

¹⁰Image source:

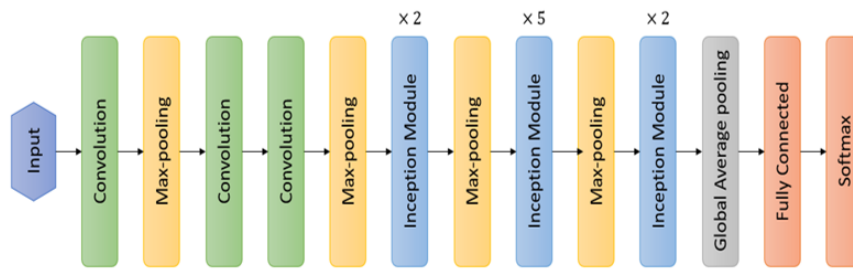


Figure IV.16: GoogLeNet architecture.¹⁰

In 2015, a Microsoft research team developed the **Residual Neural Network (ResNet)** [126] that is based on skip connections allowing to train deeper networks that can achieve up to 152 layers. The adopted technique is capable of overcoming the vanishing gradient problem while keeping a low number of trainable parameters compared to *VGGnet*. *ResNet* won the 2015 *ILSVRC* competition achieving a top-5 error rate of 3.57%, which is outperformed the human ability of just 5%. Skip connections are shortcuts that allow the flow of information from earlier layers to another layer located later in the network allowing to overcome the vanishing gradient problem (See Figure IV.17). ResNet architecture stacks residual blocks on top of each other as shown in Figure IV.18.

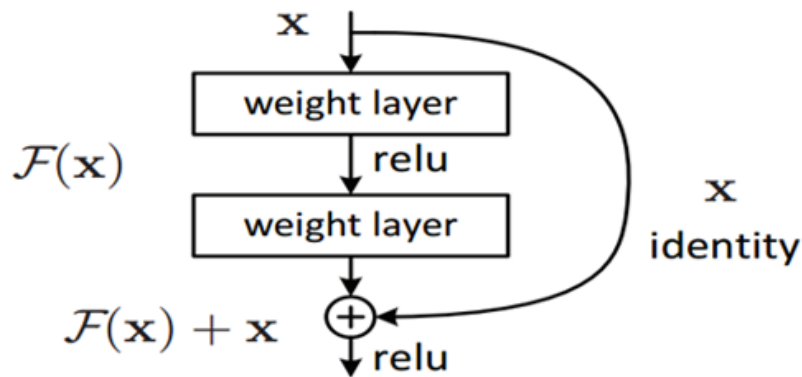


Figure IV.17: Residual block.¹¹

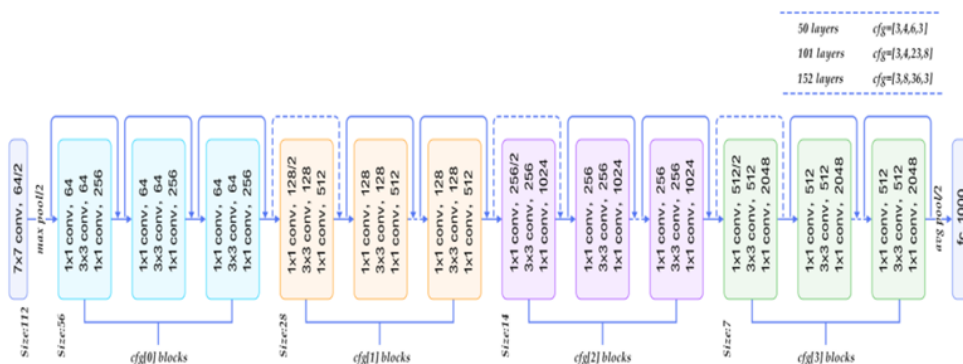


Figure IV.18: ResNet architecture.¹²

¹¹Image source:

¹²Image source:

- **Other CNN types:** Many other CNN architectures have been proposed since 2015 achieving better results to solve image analysis-related problems. Some of these networks were deeper and some others were lighter. Huang et al. [127] proposed a deep CNN architecture that was inspired by *ResNet* architecture, which is called *DenseNet*. Also, to adapt CNN architectures with small devices that have low computation powers, many researchers proposed lightweight CNN versions that achieved acceptable accuracy while improving inference speed, especially on embedded systems. Different versions of *MobileNet*, *SqueezeNet*, *PeleeNet*, and *ShuffleNet* are some famous lightweight CNN architectures [128].

IV.5 CNN training workflow and Transfer Learning concept

In this section, we introduce the training workflow and different techniques that could solve the lack of data and training time problems to improve the trained model performance, including data augmentation and transfer learning.

IV.5.1 Training workflow

In order to train an efficient CNN architecture, we need to follow a certain workflow from determining the goal to the model deployment (See Figure IV.19). After specifying the targeted goal, the first step to build a CNN-based deep learning model is the collection and preparation of the data before the training, evaluation, and deployment of the model. The collected data depends on the targeted application. Then, to prepare the dataset, we need to perform some preprocessing operations on the collected data, such as data cleaning, resizing, splitting, among others. Also, we need to only select data that is relevant to solve the targeted problem. The collected data is divided into two main sets, which are the training set and the testing set. In some cases, we need to divide it into three parts instead of two by adding a part called the validation set. Once the data is prepared, we need to select the adequate CNN model to be trained to achieve the targeted task. The right architecture selection depends on the problem to be solved. For example, we need shallow networks for small object identification, and deeper networks to extract more details. After the training of the selected model, we need to evaluate the model to see how it performs on new unseen data. If the model performs badly on new data, we need to improve the model performance by changing some hyperparameters, adding more data, or even change the whole architecture. However, if we are satisfied with obtained results, then we can deploy the model to be used on the web, mobile, or any other platforms [95, 129, 130].

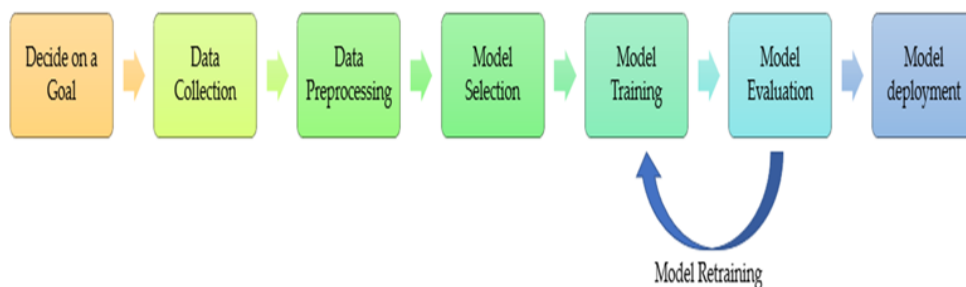


Figure IV.19: CNN training workflow.

IV.5.2 Data augmentation and transfer learning

In order to build any deep learning model; including [CNN](#), we usually need a huge amount of data in the training process. However, collecting and labeling such a large dataset is very difficult and time-consuming. Also, in some cases, we cannot find much data to achieve acceptable results. Thus, in this section, we introduce two fundamental techniques that could help to avoid overfitting and improve the deep learning model performance just with little data and less training time. These techniques are data augmentation and transfer learning[95, 130–132].

- **Data augmentation:** Having a large amount of data is not always feasible, and data augmentation could be an effective and inexpensive solution to reduce or avoid overfitting resulting in an accuracy improvement. Data augmentation is about generating new instances of data from the available data applying some geometric transformation or generating new unseen data using generative models[95, 117, 130].

Many techniques could be used to increase the dataset size like applying some geometric operations, including rotating, flipping, mirroring, lighting conditions, zooming, to name a few (Figure IV.20 (left)). Also, we can train special kinds of deep learning models that can generate new instances of data. [Generative Adversarial Networks \(GAN\)](#) and autoencoders are the most used deep learning models to increase the size of data (Figure IV.20 (right)).

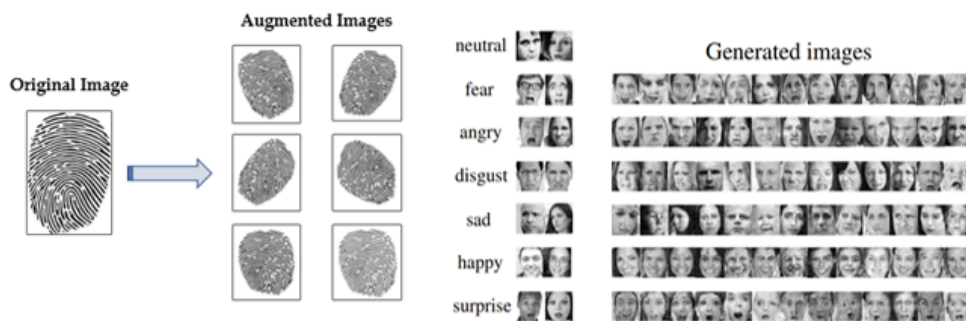


Figure IV.20: : Data augmentation techniques, geometric transformation (left), GAN (right) ¹³.

- **Transfer learning:** Transfer learning is a very popular deep learning technique that provides the ability to use a pre-trained model and adopt it to solve other types of problems. In addition to overfitting avoidance, it comes to solve big problems facing the deep learning community, which are lack of data and computation power. Instead of training a model from scratch; which requires a very large number of labeled data, transfer learning is used to transfer knowledge from a pre-trained model and use its optimized weights and parameters as a starting point. Even if we can get a large dataset to solve our problem, it still very hard, time-consuming, and computationally very expensive to train deep and complex neural networks on such huge datasets. Usually, the training process takes days, or even weeks, on powerful *GPUs* to accomplish the training. Therefore, transfer learning makes the training process much faster and achieves better results in fewer iterations with fewer data [95, 130–132].

IV.6 Conclusion

In this chapter, we presented the concept of machine learning and its different types, including neural networks. A special kind of deep neural networks called [Convolution Neural Network](#)

(CNN) was presented in detail all along with its fundamental building blocks and state-of-the-art architectures. Also, the concepts of transfer learning and data augmentation were introduced showing their importance to solve some problems related to the processing power and the size of datasets. Transfer learning is considered the fastest and easiest way that gives us the possibility to build a deep learning model without worrying about the size of data that we have. Usually, training deep CNN models requires high computational resources and a lot of data. However, transfer learning has emerged as an effective solution to such a problem.

CHAPTER V

FINGER-BASED MULTIMODAL BIOMETRICS RECOGNITION SYSTEMS USING DEEP LEARNING

Contents

V.1	Introduction	86
V.2	Multimodal Biometric Recognition Systems Using Deep Learning based on the Finger vein and Finger knuckle print Fusion	86
V.2.1	Related Work	86
V.3	The Proposed Architectures	87
V.3.1	Unimodal System	88
V.3.2	Multimodal system	89
V.3.3	Used Databases	90
V.4	Results and Discussion	92
V.4.1	Training of deep learning architectures	92
V.5	Performances Evaluation	93
V.5.1	Test and analysis of the proposed biometrics recognition systems	93
V.5.2	Unimodal Recognition	93
V.5.3	Multimodal Recognition	95
V.5.4	Comparative Study	96
V.6	The proposed Finger Vein Biometric Scanner	99
V.6.1	Related work	99
V.6.2	Finger vein designed device	100
V.6.3	Near-infrared light controlling	101
V.6.4	Finger vein acquisition and control system	102
V.7	Results and discussion	104
V.8	Conclusion	107

V.1 Introduction

Recognition systems using multimodal biometrics attracts attention because they improve recognition efficiency and high-security level compared to the unimodal biometrics system. So, Based on the obtained results of the bibliometrics analysis presented in Chapter III.

In the first part of this chapter, we perform a secure multimodal biometrics recognition system using **Finger Vein (FV)** and **Finger knuckle Print (FKP)** biometrics. The originality of this proposition is that the deep learning technique based on convolutional neural networks and transfer learning has never been applied for multimodal finger modalities fusion, especially in the case of **FV** and **FKP** fusion. Consciously, we propose two multimodal architectures using the **Finger knuckle Print (FKP)** and the **Finger Vein (FV)** biometrics with different levels of fusion: a features level fusion and scores level fusion. The features extraction for **FKP** and **FV** are performed using transfer learning **CNN** architectures: AlexNet, VGG16 and ResNet50. The key step aims to select distinct features descriptors from each unimodal biometrics modality. After that, we combine them using the proposed fusion approaches were **Support Vector Machine (SVM)** or Softmax applies as classifiers to increase the proposed system security.

The second part of this chapter presents the design of a finger vein scanner because most existing finger vein capturing devices are not suitable for any research or development. For that reason, this work focuses on designing and developing a finger vein biometric system based on an Arduino and Raspberry Pi board. In the aim to implement the proposed architect in real-time application in future work, we present the design finger vein scanner.

V.2 Multimodal Biometric Recognition Systems Using Deep Learning based on the Finger vein and Finger knuckle print Fusion

V.2.1 Related Work

The fusion between the finger vein and finger knuckle print is a promising finger-based biometric combination. However, in the literature, few works employ them (see Chapter III).

- **Veluchamy et al. [133]** proposed a multimodal biometrics recognition system (based of finger vein and finger knuckle print) using at the feature level two methods: the first one is the firefly algorithm and the second one (called fractional firefly or FFF optimization algorithm) which consists of a combination between fractional theory and firefly algorithm. In this work, authors performed preprocessing (SDUMLA-HMT [76] and PolyU FKP [77] databases), features extraction and classification using repeated line tracking, FFF and multi-SVM methods, respectively. Based on the experimental results, this fusion method has high computational complexity.
- **Yang et al. [134]** designed a multimodal biometric system based on feature level fusion of finger vein and finger dorsal texture. In this work, preprocessing (Region Of Interest or ROI extraction) was achieved using Gabor filters and winner-take-all techniques to extract unimodal features orientation of line-like patterns, and a likelihood-based to find the most correlated features. Features level fusion was performed using the orientation code (OriCode^k) based on magnitude preserved competitive code scheme and the comparative competitive code (C² Code), and performance of these two methods were compared. Although the obtained results are acceptable, the fusion strategy and fusion algorithms are complex and not reliable for real-time recognition.

- **Softmax:** known as Multinomial Logistic Regression [115, 116]. It is applied to fully connected layer output for N classes. The Softmax shown in Equation (V.1) where $0 \leq y_i \leq 1$ and $\sum_{i=1}^N y_i = 1$.

$$y_i = \frac{\exp(e_i)}{\sum_{j=1}^N \exp(e_j)} \quad e_i = \sum_k z_k w_{ki} \quad (\text{V.1})$$

The total input into a Softmax layer function is given by e_i . The parameters z and w are the activations and weight of a fully connected layer, respectively.

- **Multi-class Support Vector Machine (SVM):** known as Support Vector Networks, which uses the one-vs-all approach [115, 116]. For K class problems, K linear SVM algorithm is based on the concept of maximal margin hyperplane, which depicts the decision boundary of different categories. The output hyperplane is explicitly formulated as (see Equation (V.2)):

$$a(x) = \mathbf{w}^T x \quad (\text{V.2})$$

Where \mathbf{w} is the vector of hyperplane coefficients of Multi-class SVM, and x is the features vector of the fully connected layer.

V.3.1 Unimodal System

The biometric systems are based on training and testing phases (see Chapter I). Figure V.2 shows the diagram of the proposed unimodal biometric system based on finger vein and finger knuckle biometrics. In the training phase, database (images) quality is critical to the recognition systems. Many enhancement techniques exist such as Contrast Limited Adaptive Histogram Equalization (CLAHE) [137] which is used as a preprocessing block to obtain more informative data (improved images quality). The main block of the biometric system is those dedicated to features extraction step, which allows to get the pertinent information from finger vein and finger knuckle print modalities. In our unimodal proposed method, after preprocessing (with the same technique) in both training and testing phases, features extraction is achieved using deep networks architectures (AlexNet, VGG16 and ResNet50). Training features and testing (genuine and imposter) ones are compared using Softmax or Multi-class SVM classifier.

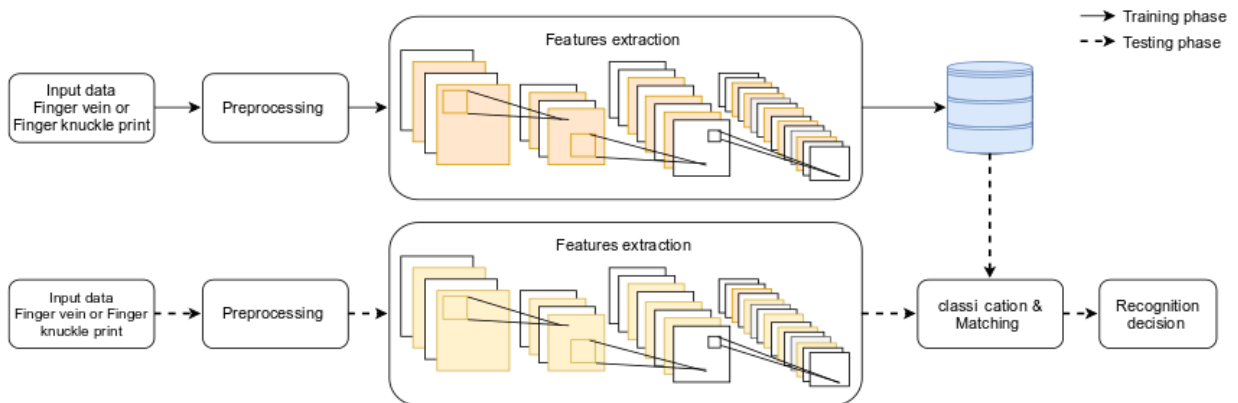


Figure V.2: Unimodal recognition system

V.3.2 Multimodal system

The unimodal system often contends with a variety of problems during algorithm designing, such as noisy data, intra-class variation, non-universality, spoof attacks, etc (see Chapter I). Combining multiple biometric traits, algorithms, sensors and/or fusing of various modalities have been the tendency in the development of better biometrics systems when compared to unimodal methods. Recognition or identification of human using multiple modalities is a very challenging problem (see Chapter II).

Let be a database D with N persons and every person have number of finger vein and finger knuckle print images. The major challenge is to recognize each of which of the N persons through their above-mentioned finger modalities.

We propose also in our work two multimodal methods using finger vein and finger knuckle print images. The first multimodal recognition system is based on features level fusion, and the second multimodal recognition system is based on scores level fusion.

- **Multimodal System Based on Feature Level fusion:** After preprocessing with the same technique used in unimodal proposed method (CLAHE)[137], we used deep networks architectures (AlexNet, VGG16 and ResNet50) to extract informative features from both **FV** and **FKP** modalities. The last layer (Fully Connected layer or FC) aims to calculate the new features fusion from FV and FKP. Indeed, normalized features of **FV** and **FKP** (using batch normalization function, see Eq.(V.3), [132]) are inputs of the FC, and its output is computed using concatenation or addition methods. In Equation.(V.3), x_i is the input features map, μ_B and σ_B^2 depict FC features map mean and variance values for a mini batch, respectively. In order to avoid division by zero, ϵ is added for numerical stability.

$$\hat{x}_i = \frac{x_i - \mu_B}{\sqrt{\sigma_B^2 + \epsilon}} \quad (\text{V.3})$$

- **Concatenation method:** The two sets of extracted features FC-FV with N_{FV} dimensional and FC-FKP with N_{FKP} dimensional are concatenated to acquire the $N_{FV} + N_{FKP}$ dimensional fused features vector FC_{FV}^{FKP} .
- **Addition method:** The two sets of extracted features FC-FV and FC-FKP are added elementwise. The fused vector FC_{FV+FKP} dimension is $Max\{N_{FV}; N_{FKP}\}$.

Figure V.3 presents the process of finger recognition based on features level fusion which also known as fusion prior to matching. The fusion is achieved by combining different feature sets extracted from multiple biometric sources before the classification step. In Figure V.3, contrary to training phase (represented with blocs), only output of testing phase (which involves the same blocs) is depicted.

- **Multimodal System Based on Score Level Fusion:** Figure V.4 represents the process of finger recognition based on score level fusion recognized also as fusion after matching. The fusion is achieved by the combination of scores from different modalities generated after the classification step. This multimodal system is based on the above proposed unimodal method (features extraction with only ResNet50) for both modalities (**FV** and **FKP**). Score level fusion consists of two steps: normalization and fusion. In the first step the **FV** and **FKP** unimodal scores (see Chapitre II) are normalized to get the same range (between 0 et 1). According to Kumer Vishi et al. [138], the **Hyperbolic Tangent Normalisation (TanH)** is the more robust and efficient normalization method comparing with the fundamental normalization concepts [139]. **Hyperbolic Tangent Normalisation (TanH)** is discarded in Chapter I.

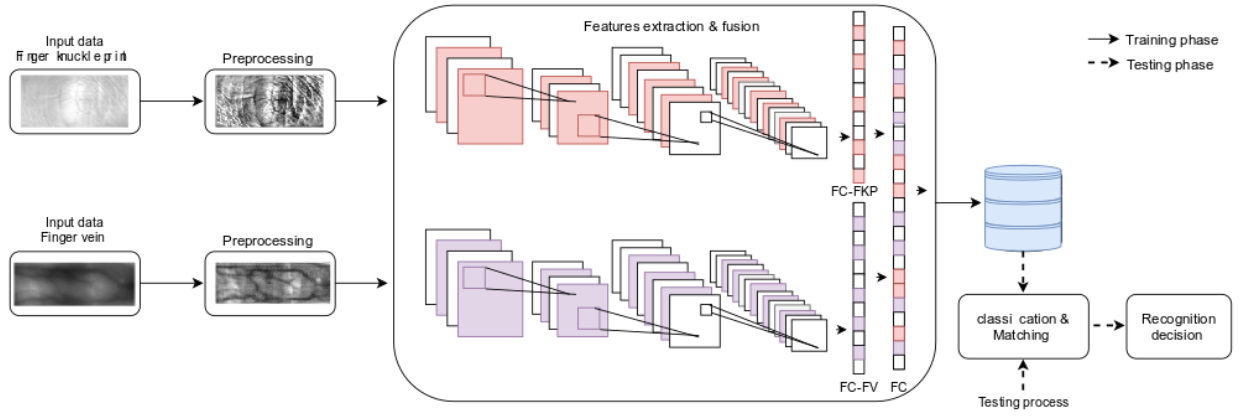


Figure V.3: Multimodal recognition system based on feature level fusion

In the second step, among the different score fusion techniques recommended by ISO standards ISO/ IECTR 24722:2015 [139], only weighted sum, weighted sum Equation.(V.4), weighted product Equation.(V.5), bayesian rule Equation.(V.6) fusion techniques were used in our work.

$$S_{ws} = w_i \times S_{FV} + (1 - w_i) \times S_{FKP} \quad (V.4)$$

$$S_{wp} = S_{FV}^{w_i} \times S_{FKP}^{w_i} \quad (V.5)$$

$$S_B = \frac{S_{FV} \times S_{FKP}}{(1 - S_{FV}) \times (1 - S_{FKP}) + S_{FV} \times S_{FKP}} \quad (V.6)$$

Here, S_{FV} and S_{FKP} are the recognition scores of FV and FKP respectively, w_i is a weight value and computed as following:

$$w_i = \frac{EER_i}{\sum_{i=1}^k EER_i} \quad (V.7)$$

Whither, EER_i denote the Equal Error Rate (EER) of each biometric system and $\sum w_i = 1$, $0 \leq w_i \leq 1$. The final decision is obtained according to the threshold score S_T and final fused scores S : if the $S > S_T$ it is considered as an imposter and if $S < S_T$ it is considered as a genuine.

V.3.3 Used Databases

To check the robustness of the proposed recognition methods, the following two open databases were used:

- **The Finger Vein (FV) database** (called humongous multimodal traits or SDULMA-HMT) was acquired by Shandong University (see Chapter III). The device used to capture images was designed by Joint Lab Intelligent Computing and Intelligent Systems. The capturing database has a total of 3816 images consisting of 106 people with 2 hands and 6 images from the fingers index, ring and middle (3816 images = 106 people \times 2 hands \times 6 images \times 3 fingers). Every image is stored in 'BMP' format (320 \times 240) pixels in size [76].
- **The Finger knuckle Print (FKP) database** is the Hong Kong Polytechnic university database (PolyU FKP database)(see Chapter III). This database is composed of 12 images from the fingers index and middle of both hands of 165 people resulting in a total of 7920 images (7920 images = 165 people \times 2 hands \times 2 fingers \times 12 images) [77].

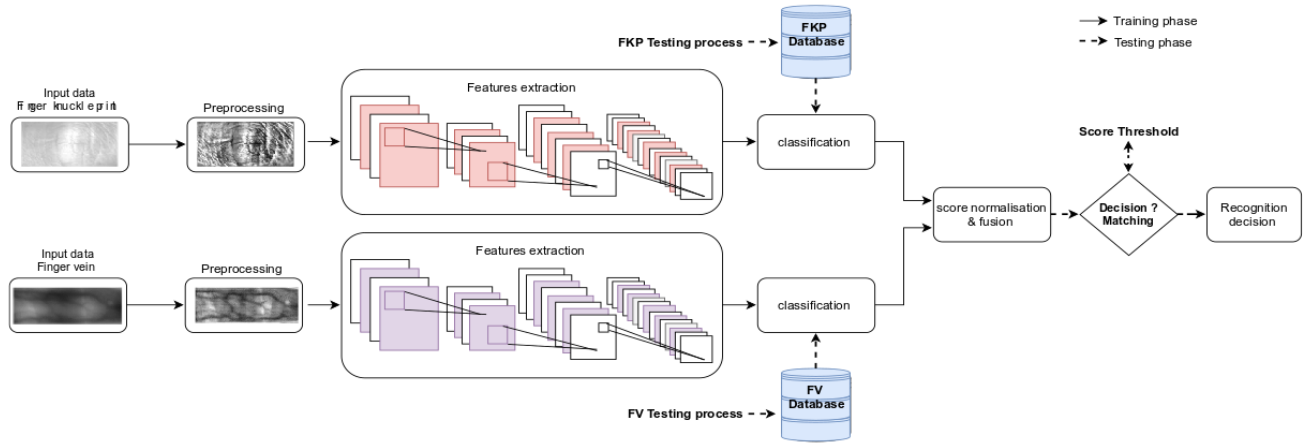


Figure V.4: Multimodal recognition system based on score level fusion

Because People number in **FKP** database is greater than in **FV** database ($165 > 106$), we took only 106 people from PolyU FKP database considering the **FV** and **FKP** people as the same ones. This assumption is necessary to perform **FV** and **FKP** modalities fusion for training and testing phases. The description of the used **FV** and **FKP** databases shown in Table V.2.

In our proposed unimodal and multimodal systems, **FKP** classes are then equal to 424 ($156 \times 2 \times 2$), and **FV** classes are equal to 636 ($106 \times 2 \times 3$). The classes from each database were divided into two sub-databases, which 60% (382 **FV** classes and/or 254 **FKP** classes) were used for training phase and 40% (254 **FV** classes and/or 170 **FKP** classes) for testing phase.

Figure V.5(a) shows an example of finger knuckle print (FKP) and finger vein (FV) images used in this study, region of interest (ROI) extraction (Fig. V.5 (b)) using algorithms found in [140, 141], and preprocessing result (Figure V.5(c)) using CLAHE algorithm [137].

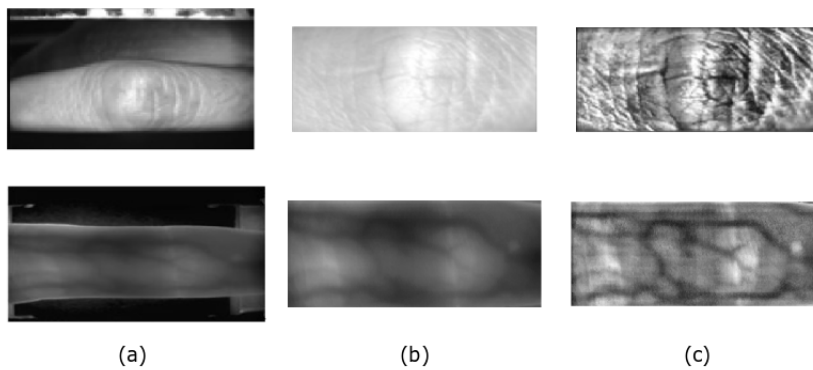


Figure V.5: Example of input images of different recognition systems: (a) Original databases images, (b) ROI images and (c) Images after preprocessing

The number of training data is insufficient for learning the parameters and weights of the deep learning architectures presented in Chapter IV. To solve the problem of over fitting, the number of training data was increased through data augmentation approach. The number of classes of each database was converted using translation and cropping to generate an artificial data sample from the original ones. To do so, the training classes are divided into two groups: genuine and

Table V.2: Finger vein and Finger knuckle print used databases description

		Finger Vein SDUMLA-HMT [76]	Finger Knuckle Print PolyU FKP [77]
Original images	#of images	3816	7920
	#of people	106	106* / 165**
	#of hands	2	2
	#of fingers	3 (index, middle and ring fingers)	2 (index, middle fingers)
	#of classes	636	424* / 660**
	#of images per class	6	12
Data augmentation for training	#of images	59592	79248
	#of images for genuine matching	29796(382 <i>classes</i> × 6 <i>image</i> × 13 <i>times</i>)	29796(382 <i>classes</i> × 6 <i>image</i> × 13 <i>times</i>)
	#of images for imposter matching (Random selection)	29796	39624

#of : Number of , *: Number of people used in our work, **: Number of people in original database.

imposter matchings. In the **FV** SDUMLA-HMT training images, the 6 images of each class are translated and cropped by 1-4 pixels randomly in the up, down, left and right directions based on the coordinates of the original images. As a result, each original image induced 13 images (original image + 12 new images). The process reiterated for all training 382 classes gave 29796 (382 classes × 6 images × 13 times) training image. The 29796 training images are used as genuine matching. Images subset is selected randomly from these 29796 images and defined as imposter matching.

In PolyU FKP database, the same data augmentation method used in **FV** case is performed, resulting in 39624 (254 classes × 12 images × 13 times) training images and defined as genuine matching. Imposter matching subsets is selected using the same procedure used in the **FV** case. This data augmentation process was used for only training phase (testing phase data non-augmented)(see Table V.2).

V.4 Results and Discussion

In this work, training and testing phases were performed using a system with Intel[®] Core™ i7-64720 HQ CPU @ 2.60 GHz (4 cores) and NVIDIA GeForce GTX 1650. All methods have been implemented using Microsoft Windows 10 Pro 64-bit and MATLAB[®] R2019a.

V.4.1 Training of deep learning architectures

All the proposed biometric recognition architectures based on **CNN** are using transfer learning. Fine-tuning was applied to the pretrained models AlexNet, VGG16 and Resnet. The **CNN** layers are retrained with augmented **Finger Vein (FV)** and **Finger knuckle Print (FKP)** images resulting

from 106 person. The stochastic gradient descent with momentum (SGDM) method was used for CNN training to accelerate the convergence of the training model. In our experiment, a high convergence rate is obtained for a learning rate of 0.001, a momentum of 0.95, a gamma of 0.1, a Mini Batch size (MB) of 128 for AlexNet (64 for VGG16 and 20 for Resnet), and a maximum Epoch (Ep) of 10. Therefore, the total number of training (T) is calculated according to $T = Itr \times Ep; Itr = \frac{I}{MB}$, where Itr is the number of iterations and I is the entire augmented data for training. The initial parameters used for CNN training are detailed in the Table V.3.

Table V.3: Description of initial parameters for training of various CNN models

Databases	Networks	Max Number of Iteration (Epoch)	Mini Batch size
Finger vein (FV)	AlexNet	465 (10)	128
	VGG16	9311 (10)	64
	ResNet50	29796 (10)	20
Finger knuckle print (FKP)	AlexNet	619 (10)	128
	VGG16	1238 (10)	64
	ResNet50	39624 (10)	20

V.5 Performances Evaluation

V.5.1 Test and analysis of the proposed biometrics recognition systems

The main objective of this work is to propose a secure and accurate multimodal recognition system using **Finger Vein (FV)** and **Finger knuckle Print (FKP)** modalities. To evaluate the performance of the proposed biometric recognition architectures, we have used **FAR**, **FRR**, **EER** and Accuracy metrics (see Chapter I). The matching time is also a critical parameter in biometric recognition systems.

V.5.2 Unimodal Recognition

Using CNN networks (AlexNet, vgg16 and ResNet50) pre-training presented in Chapter IV aims to extract informative features. Softmax or SVM were used to classify the extracted data. For the **FV** and **FKP**, a biometric system was performed using SDUMLA-HMT and PolyU FKP datasets, respectively.

Table V.4 summarizes the performance results of the proposed **FV** unimodal recognition systems. ResNet50 and Softmax or SVM classifier gave higher accuracy when compared to AlexNet and VGG16 results (with the same classifiers). Indeed, ResNet50-Softmax gave high accuracy of 80.05% (low **EER** of 0.19%) and ResNet50-SVM gave high accuracy of 80.03% as well (with **EER** of 0.29%). Besides that, the matching time using AlexNet was lower when compared with ResNet50 and VGG16. This is due to ResNet50 and VGG16 architectures deepness (more layers then more parameters) which allows to extract informative features.

Figure. V.6 and Figure V.7 show the **ROC** curves of **FV** and **FKP** unimodal recognition systems with the whole CNNs combined with Softmax (a) and SVM (b), respectively. These figures exhibit the good performance of deep learning architectures based on CNN with a better accuracy when using ResNet50 network.

Table V.5 summarizes the performance results of the proposed **FKP** unimodal recognition systems. Similarly, the obtained results when using ResNet50 architecture are better than those with AlexNet and VGG16. ResNet50-Softmax gave an accuracy of 99.42% (low **EER** of 0.112%) and

Table V.4: Performance of unimodal finger vein (FV) recognition

Networks	Accuracy (%)		EER(%)		Matching time(s)	
	Softmax	SVM	Softmax	SVM	Softmax	SVM
AlexNet	53.61	53.12	0.45	0.46	0.100	1.03
VGG16	68.81	68.85	0.319	0.31	1.39	1.40
ResNet50	80.05	80.03	0.19	0.29	2.34	2.50

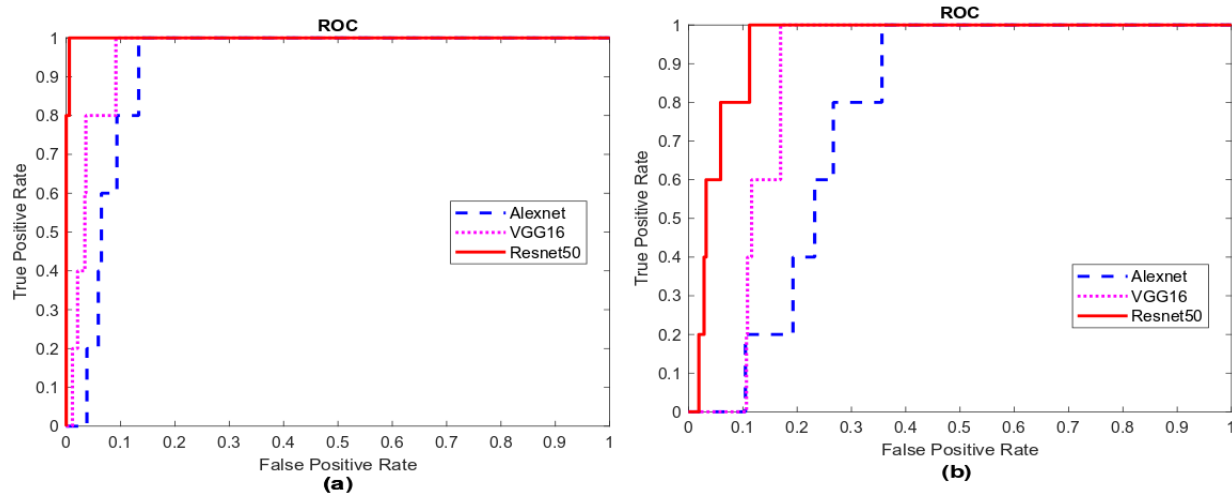


Figure V.6: Unimodal Finger vein recognition system: (a) Using Softmax, (b) Using SVM

ResNet50-SVM gave an accuracy of 88.73% (very low EER of 0.005%). As well, the matching time using AlexNet was lower when compared with ResNet50 and VGG16.

Table V.5: Performance of unimodal finger knuckle print (FKP) recognition

Networks	Accuracy (%)		EER(%)		Matching time(s)	
	Softmax	SVM	Softmax	SVM	Softmax	SVM
AlexNet	86.65	73.22	0.2678	0.1335	0.120	0.139
VGG16	90.08	82.99	1.170	0.092	1.56	1.69
ResNet50	99.42	88.73	0.112	0.005	2.36	2.55

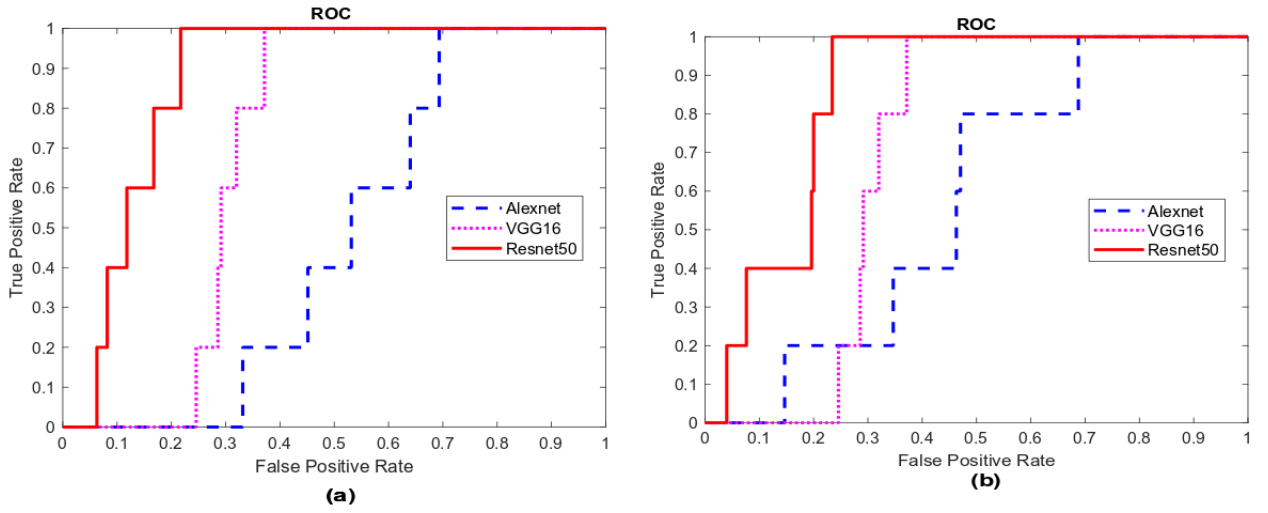


Figure V.7: Unimodal finger knuckle print (FKP) recognition system: (a) Using Softmax, (b) Using SVM

V.5.3 Multimodal Recognition

Such methods are expected to give better performance when compared to unimodal recognition systems. We proposed in this work two multimodal systems based on combining the **FV** and **FKP** modalities. In the first system, this combination (concatenation or addition) is realized in the feature level (feature level fusion technique). In the second system, this combination (weighted product, weighted sum or bayesian rule) is realized in the score level (score level fusion technique).

Table V.6 summarizes feature level fusion technique results. AlexNet, VGG16 and Rsent50 models were used to extract the informative features, and Softmax or SVM where used as classifiers after features combination (concatenation or addition).

In the case of concatenation fusion, ResNet50-Softmax gave the best accuracy of 95.77% (EER=0.0532%), and ResNet50-SVM gave 90.92% accuracy (EER=0.0532%).

In the case of addition fusion, the higher accuracy is 98.58% with the lower EER of 0.0142% were obtained for ResNet50-Softmax combination as well. In this case, ResNet50 is more accurate than AlexNet and VGG16 and slower than AlexNet in terms of matching time.

Table V.6: Performance of finger vein(FV) and finger knuckle print (FKP) multimodal feature level fusion

	Networks	Accuracy (%)		EER(%)		Matching time(s)	
		Softmax	SVM	Softmax	SVM	Softmax	SVM
Conc fusion	AlexNet	78.73	73.28	0.257	0.267	1.29	1.90
	VGG16	80.01	86.67	0.1926	0.133	2.24	2.55
	ResNet50	95.77	90.92	0.0532	0.133	2.555	2.55
Add fusion	AlexNet	79.03	76.77	0.2925	0.322	1.25	1.85
	VGG16	85.04	79.96	0.149	0.204	2.33	2.45
	ResNet50	98.58	93.34	0.0142	0.066	3.24	3.29

Conc : Concatenation , Add : Addition

In Figure. V.8 (ROC curves), ResNet50-Softmax using addition fusion seems to be the best multimodal fusion technique in the case of feature level fusion technique.

In the case of unimodal technique, Resnet50 gave the better accuracy when compared to AlexNet and VGG16 models. Score level fusion being performed after features extraction blocs (where Resnet50 is the best one), it became than obvious that in the multimodal fusion technique , Resnet50-Softmax will give the better accuracies among all the combinations (weighted product, weighted sum or bayesian rule). Table V.7 summarizes score level fusion results. In this case,

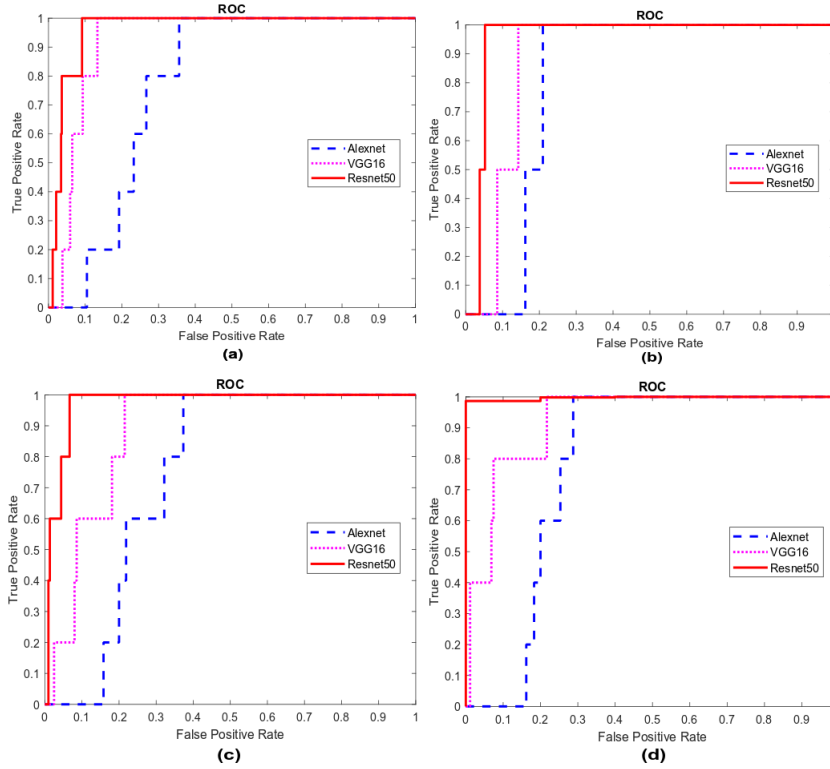


Figure V.8: multimodal recognition system feature level fusion: (a) Concatination methode using SVM , (b) Concatination methode using Softmax , (c) Addition methode using SVM ,(d) Addition methode using Softmax

Resnet50-Softmax with weighted sum fusion gave the best accuracy of 99.89% (EER of 0.005%).

Table V.7: Performance of finger vein (FV) and finger knuckle print (FKP) multimodal score level fusion.

Methods	Accuracy (%)	EER(%)	Matching time(s)
Weighted sum	99.89	0.005	3.20
Weighted product	98.31	0.017	3.29
Bayesian Rule	80.06	0.194	4.00

In Figure. V.9 (ROC curves), it can be observed that weighted sum fusion performances are better than those of weighted product and bayesian rule fusions.

V.5.4 Comparative Study

Our proposed methods are compared with previous ones (from the state of the art). Indeed, our FV unimodal recognition system is compared with J.Zeng et al. method (Squeezenet) [7], Y.Fang et.al method (selective network) [9], and H.Gil Hong et al method (VGG16) [8]. Similarly, the FKP unimodal recognition system is compared with Y.Zhai et al methods (AlexNet and Batch-normalized CNN) [10], R.Chlaoua et al. methods (PCANet and SVM)[11], and L.Fei et al. method (DDBFL algorithm) [12]. Table V.8 summarizes the performances comparison results in the case of unimodal systems. It can be observed that ResNet50-Softmax achieve the best results for both FV and FKP unimodal systems. Also, Our proposed feature level fusion technique is compared to S.veluchamy et al. work (Multi-SVM with FFF and Multi- SVM with firefl algorithms) [133], and with W.Yang et al. proposed OriCode^k and C² Code algorithms [134].

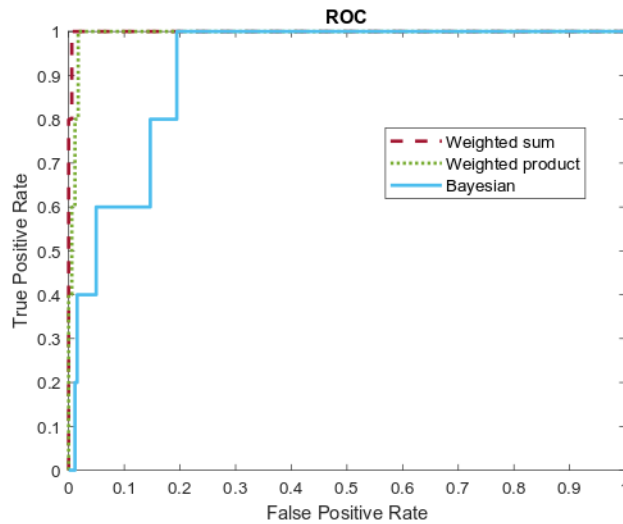


Figure V.9: Multimodal recognition system score level fusion

Table V.9 summarizes the performances comparison results in the case of multimodal systems. Our ResNet50-Softmax architecture in the case of feature level fusion technique achieves better performances when compared to previous works. The proposed scores level fusion technique is also compared to W.Yang et al. proposed Weighted fusion and Cross section binary coding methods [135]. Weighted sum fusion achieves the better results than those of previous works, thus the proposed methods are more performant. In view of its accuracy, this technique could be deployed in real time applications by using performant GPU to reduce matching time.

Table V.8: Performance comparison of the proposed unimodal recognition with the state of the art systems

	Reference	Year	Methods	Performance		
				Accuracy (%)	EER(%)	Matching time(s)
(FV)	J.Zeng et al.	2019	Squeezenet	-	4.91	-
	Y.Fang et.al	2018	Selective network	-	0.47	140
	H.Gil Hong et al.	2017	VGG16	-	0.396	-
	Proposed method		ResNet50 - Softmax	80.05	0.196	2.50
(FKP)	Y.Zhai et al.	2018	AlexNet	85.6	-	-
			Batch-normalized CNN	99.1	-	-
	R.Chlaoua et al.	2018	PCANet and SVM	-	0.919	-
	L.Fei et al.	2019	DDBFL	92.21	-	-
	Proposed method		ResNet50 - Softmax	99.42	0.005	2.55

Table V.9: Performance of multimodal recognition

	Reference	Year	Methods	Performance		
				Accuracy (%)	EER(%)	Matching time(s)
Multimodal feature level fusion	S.veluchamy et al.	2017	Multi- SVM withe FFF	95	0.35	5.1
			Multi- SVM withe firefly	94	0.7	5.1
	W.Yang et al.	2014	OriCode K	-	0.889	-
			C 2 Code	-	0.435	-
	Proposed methods		Addition fusion (ResNet50-Softmax)	98.84	0.0142	3.24
			Concatenation fusion (ResNet50-Softmax)	95.77	0.0523	3.13
Multimodal score level fusion	W.Yang et al.	2016	Weighted fusion	99.84	0.16	-
			Cross section binary coding	99.67	0.31	-
	Proposed method		Weighted sum	99.89	0.005	3.20
			Weighted product	98.31	0.017	3.29

V.6 The proposed Finger Vein Biometric Scanner

Finger vein biometric systems gained a lot of attention in recent years due to the increasing demand for high-security systems. The Finger vein recognition technology has several important features that make it distinctive from other forms of biometrics (see Chapter III). The biometric device captured the human finger vein image and used it for security such as authentication, verification and identification. Most of the existing finger vein capturing devices are not suitable for any research, development because of their private verification software. For that reason, this work focuses on designing and developing a finger vein biometric system.

The **Finger Vein (FV)** patterns are not visible to human eyes. However, they are captured by the sensors of the **NIR** camera, which is sensitive to **NIR** light. Two ways have been introduced for finger-vein image acquisition: light transmission method and light reflection method. Compared to the light reflection method, light transmission is chosen to be the most suitable method for this work because of its advantages (see Chapter III). Figure V.10 shows the finger-vein pattern imaging light transmission principle.

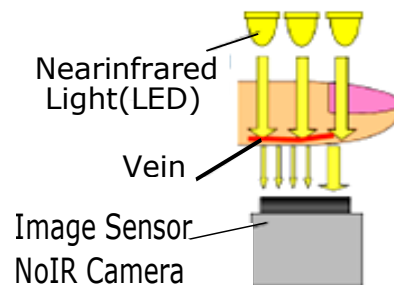


Figure V.10: Finger-vein pattern imaging : light transmission methods

V.6.1 Related work

Finger vein scanner devices are already used in commercial products as an alternative to fingerprint-based authentication systems. Almost all commercial finger vein scanner devices do not allow access to the captured finger vein images. Nevertheless, These biometric templates neither permit the development of biometric template protection nor enable a systematic evaluation of the template's properties regarding external influences and changes in the commercial vein scanners are only of little use in biometric research.

In the literature review, researchers have proposed several finger vein capturing device, such as presented in Table V.10.

- A Digital Signal Processor (DSP)-based finger-vein capturing device has been proposed by [142]. This system qualified only for authentication on mobile devices.
- [143] have proposed the finger vein recognition system. This system consists of four hardware modules: radio frequency identification system, image acquisition module, embedded mainboard, and human-machine communication module. This system used a PC, and it is heavy.
- [144] developed a low-cost finger vein capturing device using **NIR** diodes and a **Charge Coupled Device (CCD)** image sensor. To capture the finger vein images, they used MATLAB based Graphical User Interface (GUI). This proposed system using a **CCD** camera and PC, so the system provides low image quality and is heavy.

- [145] are designing and developing a finger vein capturing device by using Arduino Microcontroller. It is a device that obtains the human finger vein image, which Arduino Microcontroller control card are used. This device is using a CCD camera and connected to a PC to acquired finger vein images.

Table V.10: Finger vein devices proposed in research

Referance	Proposed	Limitation
[143]	-DSP based finger-vein capturing device	-Qualified only for authentication on mobile devices
[142]	-System baesd on radio frequency identification	There is not autonomic computing
[144]	-Finger vein capturing device on CCD camera	-Low image quality -Non autonomic computing
[145]	-System baesd on CCD camera and Arduino Microcontroller	-Low image quality
[146]	-Capturing device based on ARM and CMOS array	-Low image quality -Non autonomic computing
[147]	-Capturing device based on CMOS camera and Raspberry pi Zero	-Low image quality -Non autonomic computing

V.6.2 Finger vein designed device

Created design of finger vein biometric system consists of an image acquisition system and computer, so there are three main blocks in the proposed device (see Figure V.11), the blocks described as follows:

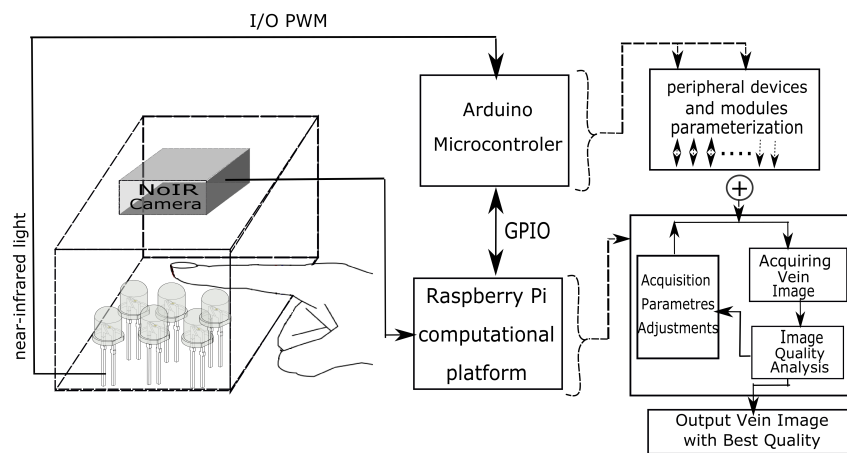


Figure V.11: The general diagram of designed device.

- The first block contains a matrix of six penetrating near-infrared LED with a wavelength of 880 nm [148] as the light source placed in the dorsal side of the finger applies the method of light transmission. With Raspberry Pi NIR camera board [149] which able to deliver clear 5MP image resolution. The module attaches to Raspberry Pi. A 15 pin Ribbon Cable is to the dedicated 15 pins Mobile Industry Processor Interface(MIPI) Camera Serial Interface (CSI), designed principally for interfacing to cameras. This camera board has no infrared

filter making it perfect for taking Infrared photographs or photographing objects in low light conditions.

- The second block is the Arduino microcontroller [150]. It used for controlling diode light intensity and camera parameters. The Arduino UNO is the most used Arduino board, which has: 14 digital input/output pins (of which six can use as PWM outputs), six analogue inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller.
- The third block is the Raspberry Pi platform is a computational decision block that controls all external peripherals of the system. Its central module of the finger vein capturing device and includes: main processing chip, memory, power supply HDMI Out, Ethernet port, USB ports and GPIO ports. The Raspberry Pi 3 model b+ [149, 151] used in our system, it is a Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit. There operating system foundation; based on NOOBS and Arch Linux ARM software package, with Python as the main programming language. His main processing chip connects a NIR camera board and display units.

V.6.3 Near-infrared light controlling

The role of Near-infrared (NIR) light controlling is to increasing infrared vein image information, so we proposed Pulse Width Modulation (PWM) control using Arduino; thus, the brightness of the LED's are under control using a potentiometer. Altering infrared light intensity is applied to collect more vein information and acquire a clear finger vein image. Figure V.12 showing a design simulation of the PWM controller based on Arduino using ISIS Proteus software. The PWM controller will control 6 number NIRLEDs located after the resistor in pins 2,3,4,5,6, and 9. The auto adjustment is the switch located in pin A0. Image quality assessment should be executing to adjusted NIR LEDs brightness and select the best-captured image or the reference image according to the assessment result. Therefore we proposed a two-dimensional entropy method to evaluate the finger vein image quality.

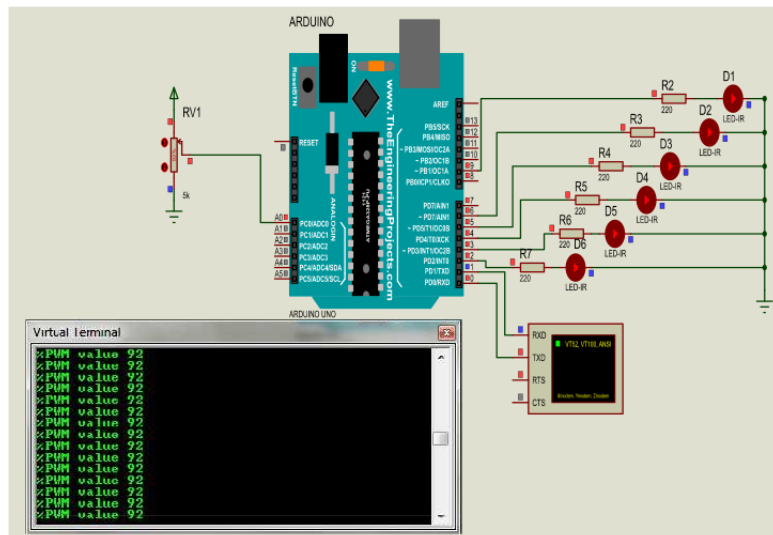


Figure V.12: PWM controller ISIS Circuit Design and Simulation for Arduino Microcontroller

Two-dimensional gray level histogram definition [152]: it is supposed that the size of gray image f is $m \times n$, the gray level is L , the coordinate of one pixel is (i, j) , in image the pixel value is $f(i, j)$, $1 \leq i \leq m, 1 \leq j \leq n$, L_{ij} is the two-dimensional histogram and in Eqs. (V.8) P_{ij} is the

probability normalized which represents the image two-dimensional gray histogram.

$$p_{ij} = \frac{L_{ij}}{(m \times n)} \quad (\text{V.8})$$

Discrete probability distribution is assumed as $p = (p_1, p_2, \dots, p_n)$, Where p_i satisfies the conditions of $\sum_{i=1}^n p_i = 1$ and $0 \leq p_i \leq 1, i = 1, 2, \dots, n$.

The mathematical expression the information entropy or Shanon entropy (Equation (V.9)) was proposed in 1948 ([152]), which described information uncertainty degree as follow:

$$H(p) = \sum_{i=1}^n p_i \log_2(p_i) \quad (\text{V.9})$$

The target information entropy of two-dimensional histogram (Equation (V.10)) or the two-dimensional entropy is shown as follow:

$$H_{2D}(p) = \sum_{i=j}^n p_{ij} \log(p_{ij}) \quad (\text{V.10})$$

V.6.4 Finger vein acquisition and control system

In the proposed system Figure V.11, the raspberry pi platform is used to control the finger vein acquisition process. After the PWM value is determined and the reference image is known, the information acquiring from a finger vein image is treated and analysed to search for the best finger vein image quality. The effectiveness of the proposed design has evaluated using objective Image Quality Assessment (IQA) metrics, i.e. MSE, PSNR, IQI, AD, NK, SC, MD, LMSE and NAE. Table V.11 demonstrates objective assessment metrics used for image quality evaluation ; the metrics with their mathematical expressions, accepted values, and significance [153, 154].

The proposed finger vein system was implemented using the mentioned methods and blocks described in Figure .V.11 after verification and simulation Figure V.13 shows the real image of implement of finger vein system.

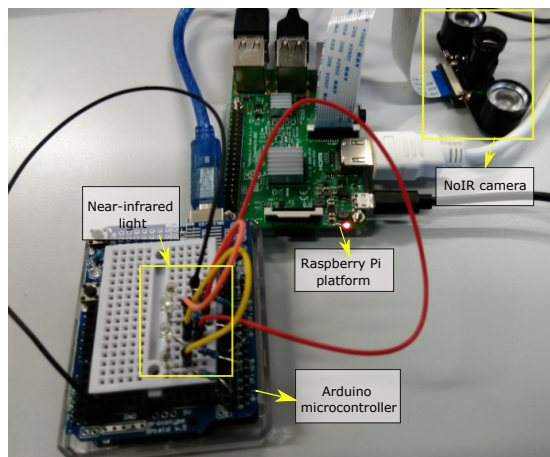


Figure V.13: Implement of finger vein acquisition control system.

Table V.11: Image quality metrics overview

Parameter	Mathematical definition	Signification
Mean Squared Error	$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I'(i, j)]^2$	- Image quality is excellent when the MSE is very low or close to zero.
Peak Signal to Noise Ratio	$PSNR = 10 \times \log_{10} \left(\frac{Max(I)}{\sqrt{MSE}} \right)$	- A higher PSNR indicates that MSE the image quality is excellent.
Image Quality Index	$IQI = \frac{\sigma_{0e}}{\rho_0 \rho_e} \cdot \frac{2\bar{\sigma}_e}{(\bar{\sigma})^2 + (\bar{\rho})^2} \cdot \frac{2\sigma_0 \rho_e}{(\sigma_0)^2 + (\rho_e)^2}$	- The IQI score ranges from -1 to +1. The best image quality when the value close to one.
Average Difference	$AD = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N I(i, j) - I'(i, j) $	- The AD is very low or near to zero, indicating that the image quality is excellent.
Normalized CrossCorrelation	$NK = \frac{\sum_{i=1}^M \sum_{j=1}^N I(i, j) \cdot I'(i, j)}{\sum_{i=1}^M \sum_{j=1}^N I(i, j)^2}$	- The normalized quantity ranges from -1 to 1. The negative picture is represented by a negative value.
Structural Content	$SC = \frac{\sum_{i=1}^M \sum_{j=1}^N \alpha(i, j)^2}{\sum_{i=1}^M \sum_{j=1}^N \alpha'(i, j)^2}$	- A SC value near to 1 indicates that the image quality is excellent.
Maximum Difference	$MD = \max I(i, j) - I'(i, j) $	- The MD very low or equal to zero to indicate excellent image quality.
Laplacian Mean Squared Error	$LMSE = \frac{\sum_{i=1}^M \sum_{j=1}^N O(I(i, j)) - O(I'(i, j)) ^2}{\sum_{i=1}^M \sum_{j=1}^N O(I(i, j)) ^2}$	- The LMSE is very low or near to zero, indicating that the image quality is excellent.
Normalized Absolute Error	$NAE = \frac{\sum_{i=1}^M \sum_{j=1}^N (I(i, j) - I'(i, j))}{\sum_{i=1}^M \sum_{j=1}^N I(i, j)^2}$	- The NAE very low or near to zero, indicating that the image quality is excellent.

Note: - I and I' are the reference and sampled image respectively of size $M \times N$. - σ_{0e} is covariance between reference & sampled image, ρ_0 & ρ_e represents standard deviation of reference and sampled image respectively, \bar{e} , $\bar{\sigma}$ mean value of reference and sampled image respectively. - O is Laplacian operator where, $O(I(i, j)) = I(i + 1, j) + I(i - 1, j) + I(i, j + 1) + I(i, j - 1) - 4 \times I(i, j)$.

V.7 Results and discussion

First of all, ten persons dorsal finger veins were acquired using the proposed NIR light controlling by PWM and Arduino, collected a total of 20 finger vein image. Table V.12 shows the relationship between the PWM duty cycle (%) and two-dimensional entropy, the data indicate that the acquisition system can find the best reference image quickly and work stably. Figure V.14 shows the real photo of the realised finger vein scanner (For more photo see APPENDIX B).



Figure V.14: Realised finger vein scanner.

The two-dimensional entropy curve Figure V.15 shown that the proposed control brightens LEDs find the best image quality was the PWM ratio is between 80% to 95%. In this state, the Potentiometer fixed at the 90% level, and the reference images stored to use in the proposed system evaluation. The finger vein captured images under different light intensities after a lot of experience confirmed that in 90% PWM, we obtain the excellent image quality; as shown in Figure V.15 in the 20% of PWM, the image is dark and image it is not good. Thus, with 100%, the image is so bright the veins form don't a pier clearly. Image number 18 was chosen as a reference image.

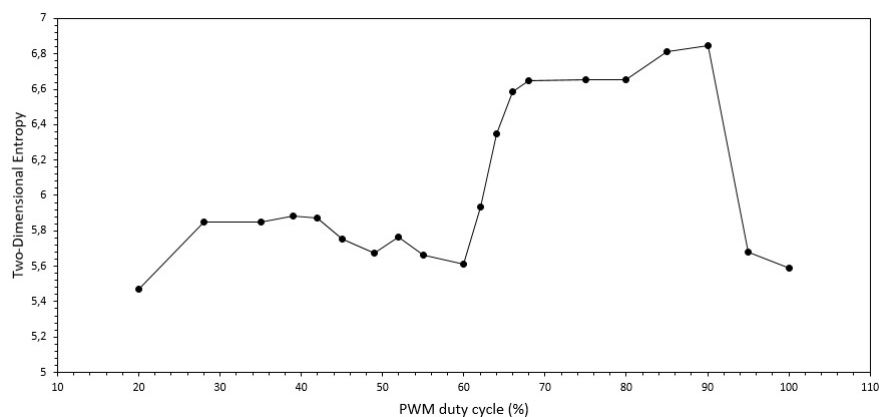


Figure V.15: Two-dimensional entropy curve in different light intensity.

The two-dimensional entropy curve Figure V.15 shown that the proposed control brightens LEDs find the best image quality was the PWM ratio is between 80% to 95%. In this state, the Potentiometer fixed at the 90% level, and the reference images stored to use in the proposed system evaluation. The finger vein captured images under different light intensities after a lot of experience confirmed that in 90% PWM, we obtain the excellent image quality; as shown in Fig.V.16 in the

Table V.12: RESULTS OF IMAGE TWO-DIMENSIONAL ENTROPY

Image Number	PWM duty cycle (%)	Two-Dimensional Entropy
1	20	5.4679
2	28	5.8472
3	35	5.8491
4	39	5.8822
5	42	5.8712
6	45	5.7533
7	49	5.6727
8	52	5.7644
9	55	5.6628
10	60	5.6121
11	62	5.9362
12	64	6.3491
13	66	6.5851
14	68	6.6511
15	75	6.6520
16	80	6.6532
17	85	6.8114
18	90	6.8467
19	95	5.6813
20	100	5.5892

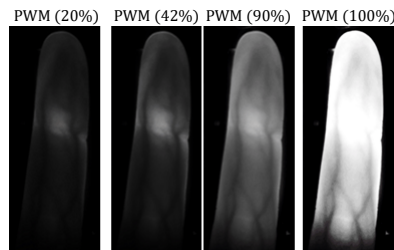


Figure V.16: Finger vein images under different light intensities.

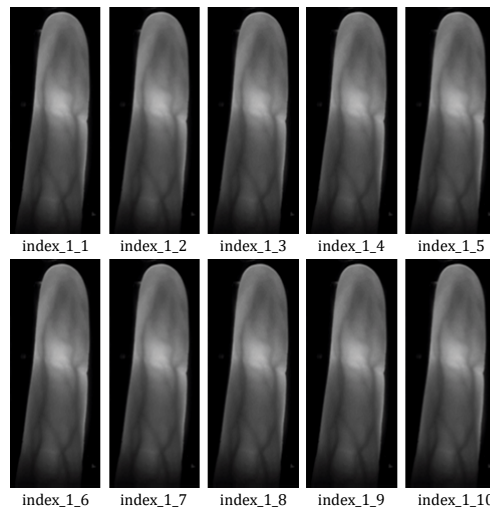


Figure V.17: The ten captured finger vein images in Same brightness level.

Table V.13: Performance evolution parameters for reference image and captured finger vein images.

	Samples	MSE	PSNR	IQI	AD	NK	SC	MD	LMSE	NAE
Different brightness leve	1	0.0024	31.05	0.70	0.4	0.7	0.8	25	1.5	0.1
	2	0.0018	22.45	0.79	0.5	0.7	0.9	29	1.5	0.2
	3	0.0027	33.67	0.98	0.1	0.8	0.8	23	0.02	0.26
	4	0.0004	49.43	0.99	0	0.9	1	16	0.01	0.15
	5	0.0008	51.37	0.99	0	0.9	1	12	0.01	0.025
	6	0.0047	29.43	0.98	0	0.8	1	16	1	0.07
	7	0.0026	43.73	0.93	0.1	0.8	0.9	15	0.07	0.16
	8	0.0037	31.43	0.85	0.3	0.7	0.8	27	1.5	0.2
	9	0.0061	34.43	0.75	0.4	0.7	0.8	25	1.4	0.23
	10	0.0087	33.32	0.73	0.4	0.7	0.8	29	2.4	0.22
Same brightness level	1	0.0029	33.19	0.99	0	0.9	1	12	0.01	0.03
	2	0.0017	35.19	0.99	0	0.9	1	11	0.01	0.01
	3	0.0084	31.40	0.98	0	0.9	1	12	0.02	0.09
	4	0.0144	28.05	0.95	0.1	0.9	0.9	14	0.01	0.09
	5	0.0048	32.12	0.97	0.1	0.8	0.9	11	0.02	0.01
	6	0.0046	32.33	0.96	0.1	0.9	0.9	13	0.02	0.04
	7	0.0087	29.99	0.99	0	0.8	1	12	0.02	0.04
	8	0.0061	31.32	0.98	0	0.8	1	14	0.01	0.02
	9	0.0041	32.72	0.98	0	0.9	1	11	0.01	0.02
	10	0.0067	30.98	0.99	0	0.9	1	12	0.01	0.01

20% of PWM, the image is dark and image it is not good. Thus, with 100%, the image is so bright the veins form don't a pier clearly. Image number 18 was chosen as a reference image.

Following the general diagram presented in Fig.V.11, after capturing the finger vein images and the analysis, control is necessary to select the best image quality. Table V.13 represents the calculated performance evaluation parameters for capturing the finger vein images in different brightness levels and the same brightness level using objective Image Quality Assessment (IQA) metrics. From the results, in the different brightness level case, the quality of the poor images are samples 2 and 10, where the IQI and SC scores are not close to one, and the AD, NK, MD, LMSE and NAE scores are not near to zeros. Also, MSE scores are the highest, and the PSNR scores are the lowest ones. Bayside that, the sample number 5is chosen as the best image quality with the lowest MSE of (0.008), highest PSNR (51.37), IQI (0.99), AD (0), NK (0.9), SC (1), MD (12), LMSE (0.01) and NAE (0.025). On the other hand, in the same brightness level case (see Table V.13), the values of image assessment quality metrics are approximately the same for each sample. But, sample number 2has the best image quality with the lowest MSE of (0.0017), highest PSNR (35.19), IQI (0.99), AD (0), NK (0.9), SC (1), MD (11), LMSE (0.01) and NAE (0.025). The Figure V.17 shown the ten captured finger vein images in Same brightness level.

Table V.14: Comparison of the lowest MSE and highest PSNR of different brightness level.

Device	Lowest MSE	Highest PSNR
[144]	0.0002080	36.8194
[145]	0.0001088	46.3728
Proposed device	0.0000888	51.3720

The experimental results are compared into the work of [144] and [145] because they have done experiments in the same protocols and condition, knowing that ten people are used, and 20 finger dorsal veins are acquired. We evaluated the performance of the designed device by comparing

Table V.15: Comparison of the lowest MSE and highest PSNR of Same brightness level.

Device	Lowest MSE	Highest PSNR
[144]	0.0046468	23.3284
[145]	0.0030257	25.1917
Proposed device	0.0017937	35.1917

the lowest MSE value and the highest PSNR value acquired, as shown in Table V.14 and Table V.15. The comparison of the lowest MSE and the highest value of a finger vein image of different brightness level and the same brightness level with [144] and [145] work; proves that the proposed device produced the best quality finger vein images. Thus, in different brightness level, we have obtained MSE attenuation of 57.31% and 18.39% compared to Kwan and al. And Syafeeza and Faiz, respectively. Besides, in terms of PSNR, we have obtained a gain of 28.35% and 9.74%. In the same brightness level, the MSE decreases by 61.39% and 40.71% compared to Kwan and al. And Syafeeza and Faiz, respectively, then the PSNR increases 33.73% and 28.42%.

V.8 Conclusion

Based on the obtained results of the bibliometrics analysis presented in Chapter III. In this chapter we have proposed tow works:

The first part, using CNNs we have proposed a unimodal and multimodal recognition biometric systems based on the finger vein and the finger knuckle print. The pre-training AlexNet, VGG16 and ResNet50 CNN models are used for features extraction from the two used biometrics modalities. SVM and Softmax are used as classifiers to evaluate and improve the recognition performance. Two multimodal recognition systems based on feature level fusion (concatenation or addition) and score level fusion (weighted product, weighted sum or bayesian rule) are presented. The proposed methods are evaluated with available SDUMLA-HMT and PolyU databases and the performance was analyzed by FAR, FRR, Accuracy and matching time metrics. When compared the unimodal and multimodal techniques (proposed and previous ones), the proposed Resnet50-Softmax with weighted sum fusion (score level fusion) exhibits the higher recognition accuracy of 99.89% and lower EER of 0.05%.

The second part, a finger vein biometric device controlled by Arduino microcontroller and Raspberry Pi has been designed and developed. The captured image quality was evaluated using objective Image Quality Assessment (IQA) metrics, i.e. MSE, PSNR, IQI, AD, NK, SC, MD, LMSE and NAE. Compared to existing state-of-the-art designs, our results improve image quality with an MSE increase of 61.39% and an important PSNR reaching 33.73%. This system revealed more convenience than the PC-based recognition system because of its smaller size, lightweight, and lower power consumption and solving non-autonomic computing problem systems.

CONCLUSION AND PERSPECTIVES

“All progress is precarious, and the solution of one problem brings us face to face with another problem.”

Martin Luther King, Jr.

Conclusion

Biometrics are an alternative based on identifying persons relying on their physical characteristics (iris, fingerprint, hand shape, etc.) and/or behavioural (voice, dynamic signature, walking, etc). Biometrics achieves an important goal in our life. The first goal is to achieve security by eliminating doubt on the identity of a person. The second purpose is to facilitate the identification of individuals. Nowadays, this identification method is preferred over traditional methods involving passwords and badges for different reasons: (i) the person identified must be physically present at the time of identification; (ii) the biometric techniques eliminate the need to remember a password or carry a badge.

Biometric systems which are based on a single modality are called unimodal biometric systems. Although some of these systems have achieved significant improvements in terms of reliability and accuracy, they suffer from some limitations that prevent them from being used in recent applications. These limitations may shape several problems because of noisy data, intra-class variation, inter-class similarities, fraud attacks, non-universality and other factors. To overcome some of these limitations and increase the security level, the fusion of data presented by different modalities may increase the identification accuracy of the identity. These are called multimodal biometric systems.

To invest in the multi-biometric field and to achieve a robust recognition solution, we have focused, throughout this thesis, on new multimodal biometric methods in the finger-based biometric field based on fingerprint, finger vein and finger knuckle print biometric modalities.

In this thesis, we have presented the properties of different biometric modalities, the structure of a general biometric system, application and the concept of biometric recognition by summarizing the different architectures and describe the evaluation metrics of biometrics systems. In addition, we have explored the topic of multimodal biometrics by describing the concept of data fusion, source of multi-biometrics, the concept of multimodality and their fusion levels and a comparison between different fusion approaches is outlined. On the other hand, an overview of finger-based modalities is put forward, and bibliometrics analysis is discussed. Where, multimodal fingerprint, finger vein, finger knuckle print biometrics are described. Moreover, another part concerns an overview of deep learning and the convolution neural network definition and the existing trend architectures.

In The final, A multimodal recognition biometric systems based on the finger vein and the finger knuckle print have been proposed. We propose two multimodal architectures using the finger knuckle print (FKP) and the finger vein (FV) biometrics with different levels of fusion: a features level fusion and scores level fusion. The features extraction for FKP and FV are performed using transfer learning CNN architectures: AlexNet, VGG16 and ResNet50. The key step aims to select separate features descriptors from each unimodal biometrics modality. After that, we combine them using the proposed fusion approaches were support vector machine (SVM) or Softmax applies as classifiers to increase the proposed system security. The efficiency of the proposed algorithms is tested using publicly available biometrics databases. The experimental results show that the proposed fusion architectures achieve an accuracy of 99.89% and an equal error rate of 0.05%. These results demonstrate that using both FV and FKP is efficient and promising for multimodal biometric techniques.

Also, we focuses on designing and developing a finger vein biometric system based on an Arduino and Raspberry Pi board. The proposed finger vein device was based on near-infrared light (NIR). The Arduino Microcontroller is used to automatically control the brightness and determine the impact of NIR lighting on the captured images Raspberry Pi board commanded all external peripherals of the system. The effectiveness of the proposed design has evaluated using objective Image Quality Assessment (IQA) metrics, i.e. MSE, PSNR, IQI, AD, NK, SC, MD, LMSE and NAE. Experimental results improve high performance with an MSE increase of 61.39% and an

important PSNR reaching 33.73% compared with the existing state-of-the-art designs.

Perspectives and future work

Based on the promising obtained results, we plan to:

- Extend the acquired finger vein dataset and improve the designed.
- Add three cameras to the design that it is possible to make 3D reconstructions of the finger veins.
- Include a camera for the finger knuckle print and combined the finger vein reader with a fingerprint reader to develop the multimodal biometric scanner.
- Evaluate the acquired dataset using biometrics recognition algorithms.
- Implementation of the proposed finger-based multimodal system in parallel computing units such as FPGA card benefiting from both parallelism and pipelining processing and testing the feasibility of the multimodal recognition system.

APPENDIX A

MEASURING QUALITY OF SCIENTIFIC PRODUCTION

Bibliometrics analyses are one of a multitude of factors responsible for the overall quality of scientific papers. The bibliometrics analyses are a quantitative analysis method that uses mathematical and statistical tools to measure the interrelationships and impacts of publications within a given area of research.

A.1 Publish or Perish Tool

is a software designed to help individual academics do bibliometric research and explore research, development or evaluate state-of-art journal articles' current state. **Publish or Perish** runs on Windows, Macintosh and Linux Platforms. For detail instructions on how to install and use see the main webpage (<https://harzing.com/resources/publish-or-perish>). This software uses Google Scholar, Crossref, PubMed, Microsoft Academic, Scopus, Web of Science or external data to obtain the references. The sources which cite them and then it analyses those were presenting varied modal of statistics such as; the H-index, the total number of citations; the average citations per paper, citations per author, citations per year...etc. The results are available on-screen (See Figure A.1) and can also be copied to the Windows clipboard (for pasting into other applications) or saved to comma-separated values (CSV), the format accepted by most databases and spreadsheets such as EXCEL [72, 73].

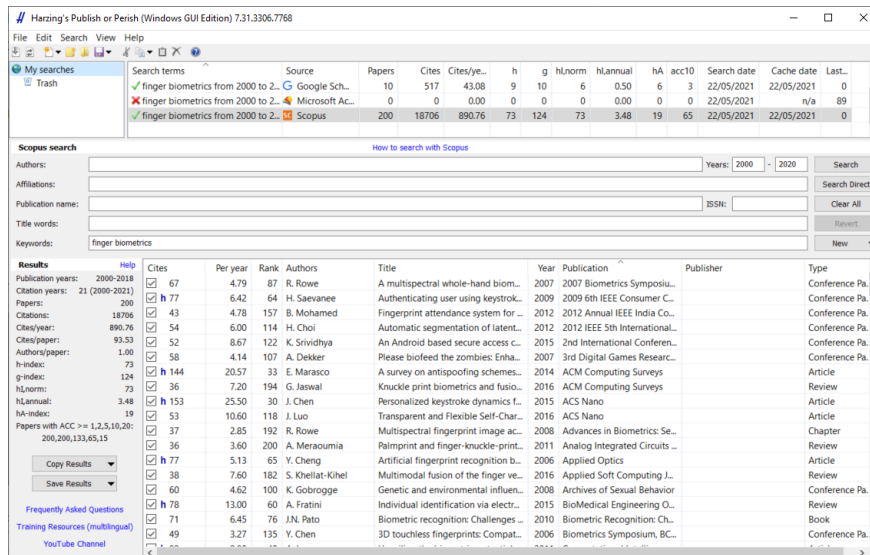


Figure A.1: Publish or Perish software Main Window

A.2 VOSviewer Tool

VOSviewer is a free tool that can be downloaded from the VOSviewer main website

(<https://www.vosviewer.com>). VOSviewer can analyze the computable parameters using a Bibliometric network. The input needs to be a comma-separated value file, also known as .csv file, to the VOSviewer. There are three kinds of visualization analysis using VOSviewer, such as Network visualization, Overlay Visualization and Density visualization. Visualization between the keywords as is shown in exmple See Figure A.2, extracted from the database. The circles in the figure represent the keywords that are extracted from the title of the source. The size of the circle indicates the keyword occurrence. The links between the circle, shows the association among the keywords, less distance means the strong association, and more distance means the weak association. The closely related keywords are represented with the same colors. There are different colors to represent the different clusters. The labels represent the actual keyword, size of the circle, and the label depends on the weight of the keywords. The bigger label size represents the keywords with higher weight. The lines represent the links between the words.

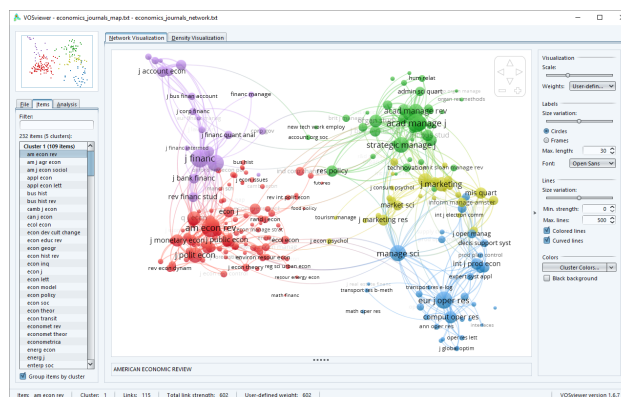


Figure A.2: VOSviewer software Main Window

A.3 Finger multimodal biometrics trend Analysis

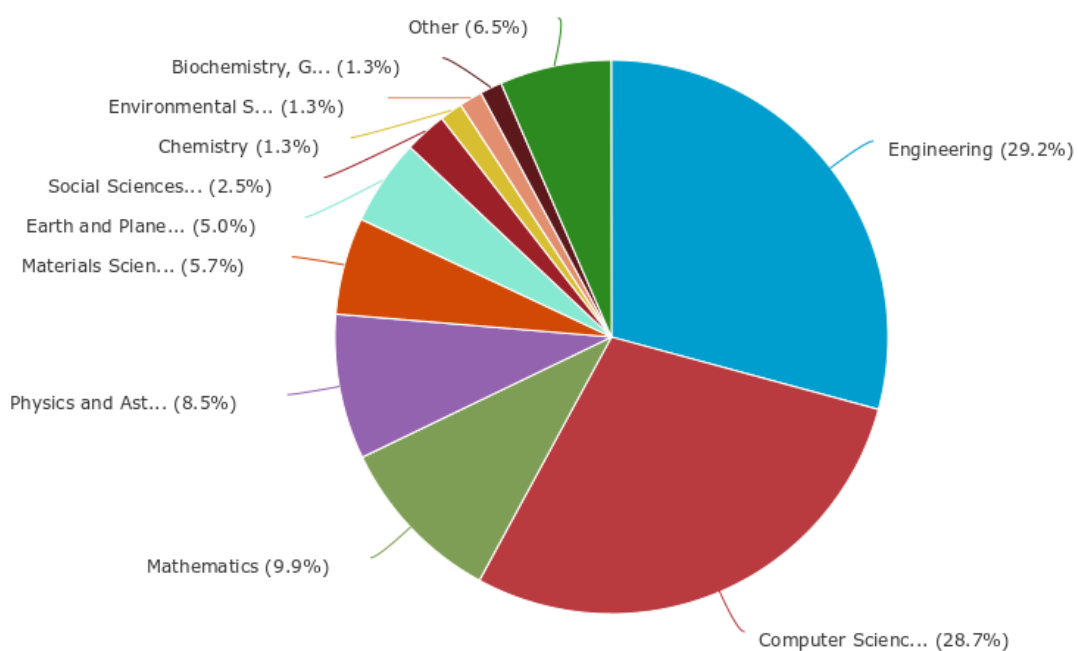


Figure A.3: Documents by subject area
 Source: <https://www.scopus.com/> (Accessed on February 5, 2020)

These documents h-index27

Scopus

Of the documents considered for the h-index, have been cited at least times

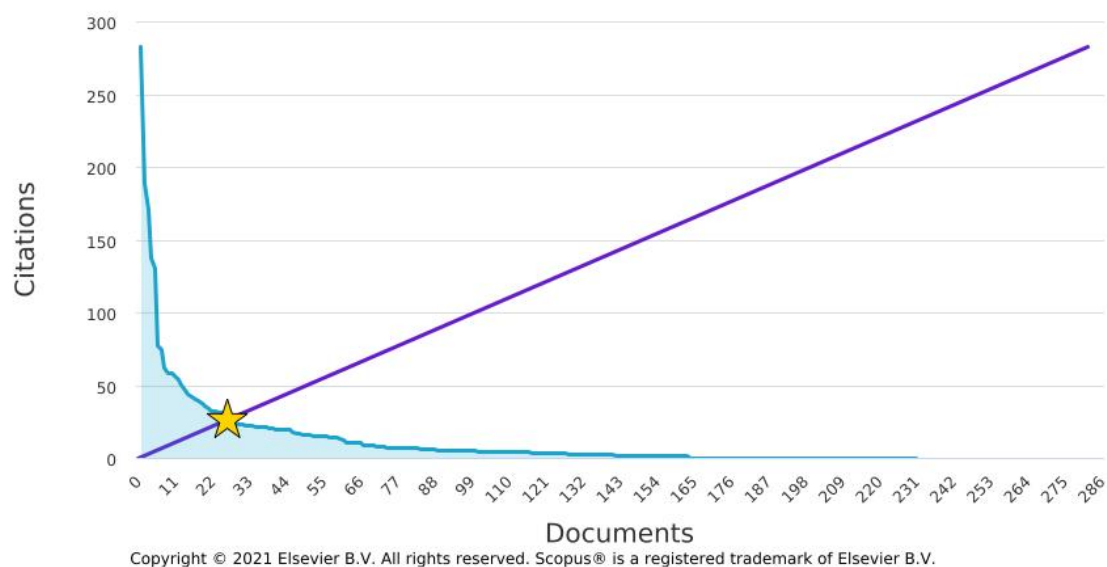


Figure A.4: h- index for documents
 Source: <https://www.scopus.com/> (Accessed on February 5, 2020)

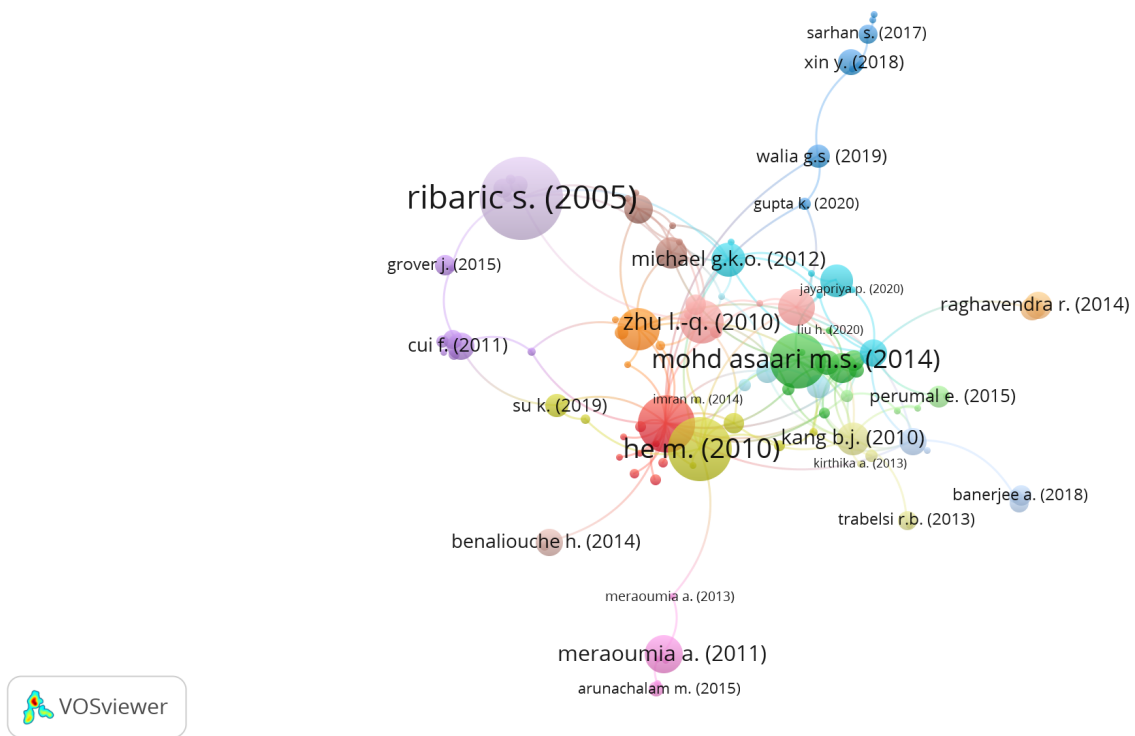
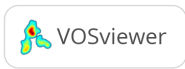
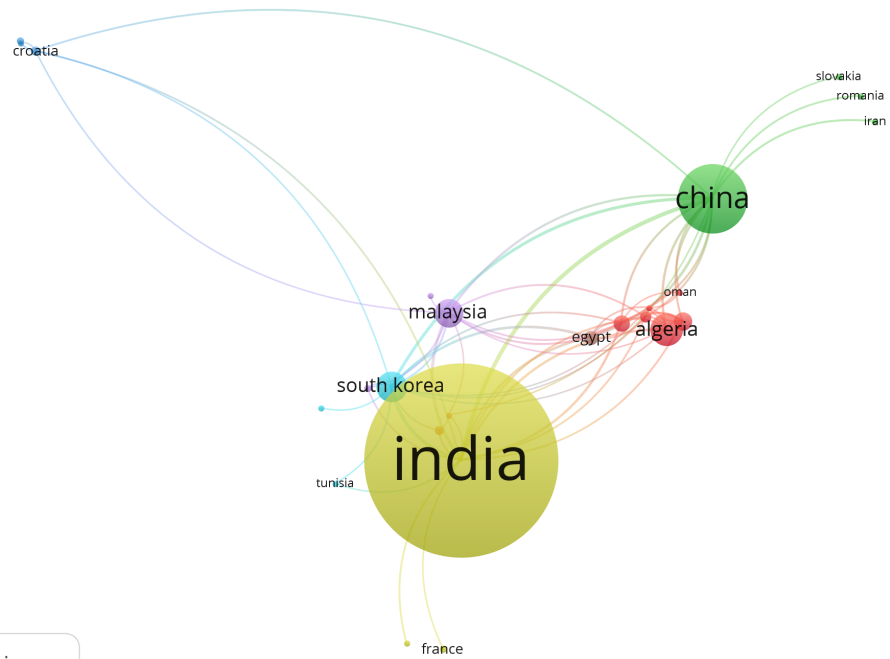


Figure A.5: Network visualization map of citation document.

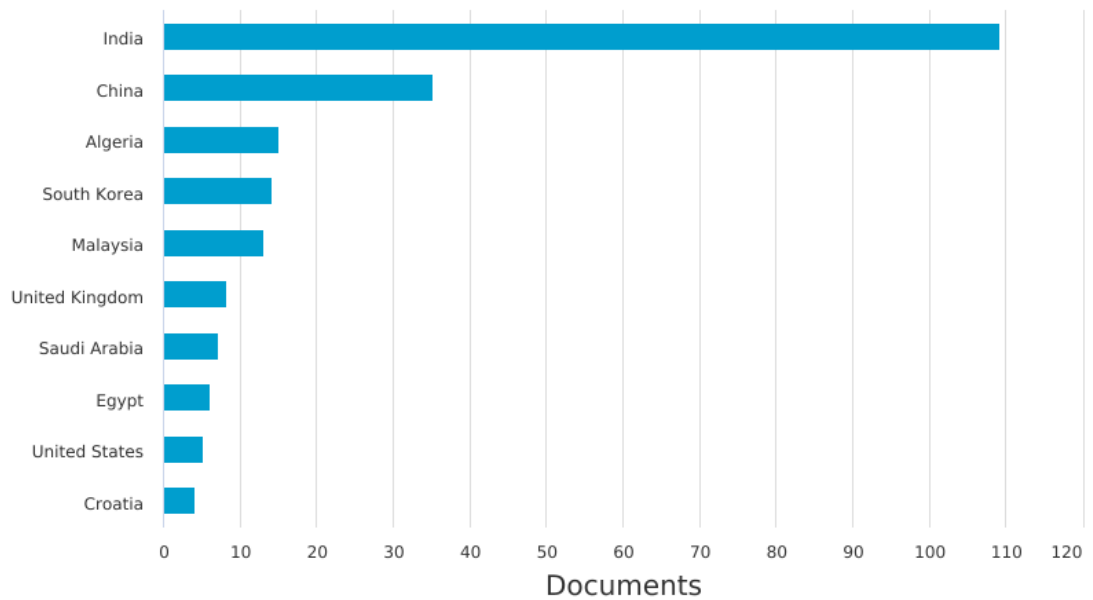
The thickness of the connecting line (link strength) is proportional to the extent of research collaboration between the connected countries. The node size of each author represents the percentage of documents with the number of citations. A similar colour indicates close research interest. The map was created by VOSviewer.



Documents by country or territory

Scopus

Compare the document counts for up to 15 countries/territories.



Copyright © 2021 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

APPENDIX B

DATA COLLECTION FOR FINGER VEIN BIOMETRIC

The collection of finger vein datasets using the designed finger vein system shows in Figure ?? and Figure B.1. Ten volunteers (25 to 60 years old on the average) was invited to present themselves for the imaging of their index finger both hands. At the end of the data collection, we have a total of 20 images, 75% women and 25% men, Blood groups (50 % A, 15% B, 5 %AB and 30 %O, for the RhD 90% + and 10% -)

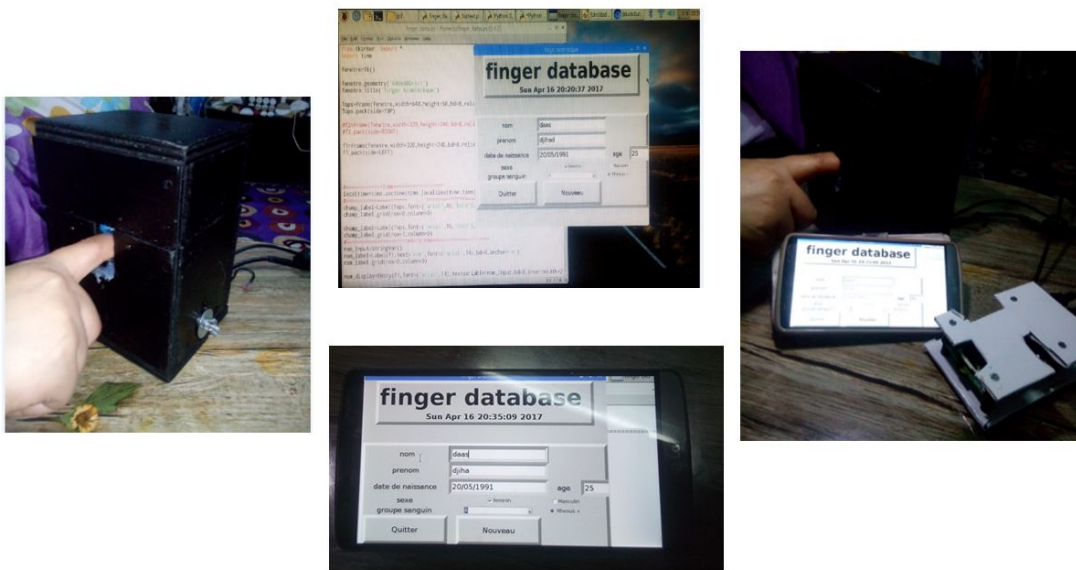


Figure B.1: Finger vein biomtrics data collection

BIBLIOGRAPHY

- [1] Amine Naït-Ali. *Hidden Biometrics: When Biometric Security Meets Biomedical Engineering*. Springer Nature (Book), 2019.
- [2] Carmelo Velardo. *Estimation visuelle d'indices anthropométriques*. PhD thesis, Paris, ENST, 2012.
- [3] P.R. Avuthu. *Multimodal Biometrics: Representation, Optimization and Kernelization*. Master's thesis collection, Department of Electrical Engineering. California State University, Long Beach (Book), 2016. ISBN 9781339802121.
- [4] Adams Kong, David Zhang, and Mohamed Kamel. *A survey of palmprint recognition*. *pattern recognition*, 42(7):1408–1418, 2009.
- [5] Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing. *Advances in biometrics for secure human authentication and recognition*. CRC Press Taylor and Francis Group (Book), 2013.
- [6] Hao Luo, Fa-Xin Yu, Jeng-Shyang Pan, Shu-Chuan Chu, and Pei-Wei Tsai. *A Survey of Vein Recognition Techniques*. *Information Technology Journal*, 9(6):1142–1149, aug 2010. doi: 10.3923/itj.2010.1142.1149. URL <https://doi.org/10.3923%2Fitj.2010.1142.1149>.
- [7] Junying Zeng, Yao Chen, Chuanbo Qin, Fan Wang, Junying Gan, Yikui Zhai, and Boyuan Zhu. *A Novel Method for Finger Vein Recognition*. In *Chinese Conference on Biometric Recognition (CCBR 2019)*, pages 46–54. Springer International Publishing, 2019. doi: 10.1007/978-3-030-31456-9_6. URL https://doi.org/10.1007%2F978-3-030-31456-9_6.
- [8] Hyung Hong aMin Lee and Kang Park. *Convolutional Neural Network-Based Finger-Vein Recognition Using NIR Image Sensors*. *Sensors*, 17(6):1297, jun 2017. doi: 10.3390/s17061297. URL <https://doi.org/10.3390%2Fs17061297>.
- [9] Yuxun Fang, Qiuxia Wu, and Wenxiong Kang. *A novel finger vein verification system based on two-stream convolutional network learning*. *Neurocomputing*, 290:100–107, may 2018. doi: 10.1016/j.neucom.2018.02.042. URL <https://doi.org/10.1016%2Fj.neucom.2018.02.042>.

- [10] Yikui Zhai, He Cao, Lu Cao, Hui Ma, Junyin Gan, Junying Zeng, Vincenzo Piruri, Fabio Scotti, Wenbo Deng, Yihang Zhi, and Jinxin Wang. **A Novel Finger-Knuckle-Print Recognition Based on Batch-Normalized CNN**. In *Chinese conference on biometric recognition (CCBR 2018)*, pages 11–21. Springer International Publishing, 2018. doi: 10.1007/978-3-319-97909-0_2. URL https://doi.org/10.1007%2F978-3-319-97909-0_2.
- [11] Rachid Chlaoua, Abdallah Meraoumia, Kamal Eddine Aiadi, and Maarouf Korichi. **Deep learning for finger-knuckle-print identification system based on PCANet and SVM classifier**. *Evolving Systems*, 10(2):261–272, apr 2018. doi: 10.1007/s12530-018-9227-y. URL <https://doi.org/10.1007%2Fs12530-018-9227-y>.
- [12] Lunke Fei, Bob Zhang, Shaohua Teng, An Zeng, Chunwei Tian, and Wei Zhang. **Learning Discriminative Finger-knuckle-print Descriptor**. In *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP, Brighton, United Kingdom)*. IEEE, may 2019. doi: 10.1109/icassp.2019.8683156. URL <https://doi.org/10.1109%2Ficassp.2019.8683156>.
- [13] Sara Daas, Mohamed Boughazi, Mouna Sedhane, and Badreddine Bouledjane. **A review of finger vein biometrics authentication System**. In *2018 International Conference on Applied Smart Systems (ICASS)*, pages 1–6. IEEE, 2018.
- [14] Sara Daas, Amira Yahi, Toufik Bakir, Mouna Sedhane, Mohamed Boughazi, and El-Bay Bourennane. **Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion**. *IET Image Processing*, DOI: <https://doi.org/10.1049/iet-ipr.2020.0491>, 14(15):3859–3868, 2020.
- [15] Sara Daas, Amira Yahi, , Mohamed Boughazi, and El-Bay Bourennane. **Finger Vein Biometric Scanner Design Using Raspberry Pi**. *International Journal of Computational Systems Engineering, Special Issue on: ISPR 2020 Recent Advances in Intelligent Systems and Pattern Recognition*, 2021.
- [16] Maarouf KORICHI and AAIADI MERAOUZIA. **Biometrics and Information Security for a Secure Person Identificatio**. PhD thesis, PhD thesis, UNIVERSITY OF KASDI MERBAH OUARGLA, Algérie, 2019.
- [17] Karm Veer Arya and Robin Singh Bhadoria. **The Biometric Computing: Recognition and Registration**. CRC Press Taylor and Francis Group (Book), 2019.
- [18] Babich Aleksandra. **Biometric Authentication. Types of biometric identifiers**. PhD thesis, HAAGA-HELIA University of Applied Sciences,Finland, 2012.
- [19] KIHELSouad KHELLAT. **Identification biométrique par fusion multimodale de l’empreinte d’articulation, l’empreinte digitale et l’empreinte veineuse du doigt**. PhD thesis, PhD thesis, Université des Sciences et de la Technologie d’Oran Mohamed Boudiaf, Algérie, 2016.
- [20] Pierre Bonazza. **Système de sécurité biométrique multimodal par imagerie, dédié au contrôle d’accès**. PhD thesis, PhD thesis, Bourgogne Franche-Comté France, 2019. URL <https://www.theses.fr/2019UBFCK017>.
- [21] Hafs Toufik. **Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques: l’empreinte digitale et la signature manuscrite cursive en ligne**. PhD thesis, PhD thesis, université badji mokhtar annaba, Algérie, 2016.

- [22] Ibtissam BENCHENNANE. *Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus*. PhD thesis, University of sciences and technology in Oran, Algérie, 2015.
- [23] Azeddine Benlamoudi. *Multi-Modal and Anti-Spoofing Person Identification*. PhD thesis, PhD thesis, UNIVERSITY OF KASDI MERBAH OUARGLA, Algérie, 2018.
- [24] Samir AKROUF. *Une approche multimodale pour l'identification du locuteur*. PhD thesis, PhD thesis, UNIVERSITE FERHAT ABBAS-SETIF, Algérie, 2014.
- [25] Nefissa Khiari Hili. *Biométrie multimodale basée sur l'iris et le visage*. PhD thesis, PhD thesis, l'Université d'Evry Val d'Essonne, France, 2016.
- [26] Chuck Wilson. *Vein pattern recognition: a privacy-enhancing biometric*. CRC Press Taylor and Francis Group (Book), 2010.
- [27] Syazana-Itqan Syafeeza Saad Hamid Norihan Abdul Saadand Wira Hidayat Bin Mohd. *A review of finger-vein biometrics identification approaches*. *Indian Journal of Science and Technology*, 9(32), 2016.
- [28] Andreas Uhl, Christoph Busch, Sébastien Marcel, and Raymond Veldhuis. *Handbook of vascular biometrics*. Springer Nature (Book), 2020. doi: 10.1007/978-3-030-27731-4.
- [29] Shaveta Dargan and Munish Kumar. *A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities*. *Expert Systems with Applications*, 143:113114, 2020. doi: <https://doi.org/10.1016/j.eswa.2019.113114>.
- [30] sylvain hocquet le. *Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite*. PhD thesis, PHD thesis, Université François Rabelais Tours, France, 2006.
- [31] L.German Rachel and Barber K. Suzanne. *Current Biometric Adoption and Trends*. University of Texas at Austin Centre of identity, 2017.
- [32] Sinjini Mitra and Mikhail Gofman. *Biometrics in a data driven world trends technologies and challenges*. CRC Press Taylor and Francis Group (Book), 2016.
- [33] Guodong Guo and Harry Wechsler. *Mobile Biometrics*. Security. Institution of Engineering and Technology (Book), 2017.
- [34] Shaun Whitehead, Jen Mailley, Ian Storer, John McCardle, George Torrens, and Graham Farrell. *IN SAFE HANDS: A Review of Mobile Phone Anti-theft Designs*. *European Journal on Criminal Policy and Research*, 14(1):39–60, jun 2008.
- [35] IDX and Biometrics. *IDEX Annual report 2019*. Technical report, Accessed April 2019., 2019.
- [36] Justin Lee. *Netatmo's home security camera with facial recognition now available in the UK*. Technical report, Accessed Sptember 2020., Jun 18, 2015.
- [37] heleh. *An general overview of the fingerprint door lock protecting your house*. Technical report, Accessed Sptember 2019., 2018.
- [38] Solution Intelligentes Informatique (S2I). *solution sur mesure simplifier la gestion de temps du travail de votre efectif*. Technical report, 2016.

- [39] Steve Gold. **Military biometrics on the frontline**. *Biometric Technology Today*, 2010(10): 7–9, nov 2010. doi: 10.1016/s0969-4765(10)70207-1.
- [40] Hichem chaya. **The Algerian biometric and electronic national identity card (CNBE)**. Technical report, Algerian Ministry of Interior, 2016.
- [41] forecasts revenue growth at global. **Biometrics Technology Market Size, Share & Trends Analysis Report Report By End-use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), And Segment Forecasts, 2018 - 2025**. Technical report, Accessed Sptember 2020., Sep, 2018.
- [42] Nesrine Charfi. **Biometric recognition based on hand schape and palmprint modalities**. PhD thesis, PHD thesis, Universite bretagne Lorie , IMT Atlantique Nantes, France, 2017.
- [43] Yang Liu and Elizabeth Shriberg. **Comparing Evaluation Metrics for Sentence Boundary Detection**. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*. IEEE, apr 2007. doi: 10.1109/icassp.2007.367194.
- [44] HADJAR Ahmed. **Identification des individus par la biométrie multimodale**Soutenu. PhD thesis, PhD thesis, UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D’ORAN MOHAMED BOUDIAF,Algérie, 2015.
- [45] the NIST report to the United States Congress. **SUMMARY OF NIST STANDARDS FOR BIOMETRIC ACCURACY, TAMPER RESISTANCE, AND INTEROPERABILITY**. Technical report, the National Institute of Standards and Technologies (NIST), November 2002.
- [46] Jung SohFarzin DeraviAlessandro TrigliaAlex Bazin. **Multibiometrics and Data Fusion, Standardization**. In: *Li S.Z., Jain A. (eds) Encyclopedia of Biometrics*. Springer, Boston, MA., 2009.
- [47] Regis Fournier Amine Nait-Ali. **Signal and image processing for biometrics**. WILEY (Book).
- [48] Pramod K Varshney. **Multisensor data fusion**. *Electronics & Communication Engineering Journal*, 9(6):245–253, 1997.
- [49] Suneet Narula Garg, Renu Vig, and Savita Gupta. **A survey on different levels of fusion in multimodal biometrics**. *Indian Journal of Science and Technology*, 10(44), 2017.
- [50] Larbi NOUAR et al. **Identification Biométrique par Fusion Multimodale**. PhD thesis, PhD thesis, l’université Djillali Liabes de Sidi Bel Abbes, Algérie, 2018.
- [51] Arun Ross. **Fusion, Feature-Level**. n: *Li S.Z., Jain A. (eds) Encyclopedia of Biometrics*. Springer, Boston, MA., 2009.
- [52] Marina Cocchi, Age K Smilde, Iven Van Mechelen, Agnieszka Smolinska, Jasper Engel, Ewa Szymanska, Lutgarde Buydens, Lionel Blanchet, N Vervliet, L De Lathauwer, et al. **Data Fusion Methodology and Applications**. 31:396, 2019. ISSN 9780444639844.
- [53] Harpreet Kaur, Deepika Koundal, and Virender Kadyan. **Image fusion techniques: a survey**. *Archives of Computational Methods in Engineering*, pages 1–23, 2021.
- [54] MJ Sudhamani, MK Venkatesha, and KR Radhika. **Revisiting feature level and score level fusion techniques in multimodal biometrics system**. In *2012 International Conference on Multimedia Computing and Systems*, pages 881–885. IEEE, 2012.

- [55] SK Bhardwaj. **An algorithm for feature level fusion in multimodal biometric system**. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume*, 3, 2014.
- [56] Arun A Ross, Anil K Jain, and Karthik Nandakumar. **Levels of fusion in biometrics**. *Handbook of multibiometrics*, pages 59–90, 2006.
- [57] Yunhong Wang, Tieniu Tan, and Anil K Jain. **Combining face and iris biometrics for identity verification**. In *International conference on Audio-and video-based biometric person authentication*, pages 805–813. Springer, 2003.
- [58] John Daugman. **New methods in iris recognition**. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5):1167–1175, 2007.
- [59] Li Cao, Yong Cai, Yinggao Yue, Shaotang Cai, and Bo Hang. **A novel data fusion strategy based on extreme learning machine optimized by bat algorithm for mobile heterogeneous wireless sensor networks**. *IEEE access*, 8:16057–16072, 2020.
- [60] Kamer Vishi and Vasileios Mavroeidis. **An evaluation of score level fusion approaches for fingerprint and finger-vein biometrics**. *arXiv preprint arXiv:1805.10666*, 2018.
- [61] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas. **On combining classifiers**. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3):226–239, 1998.
- [62] Bouchemha Amel. *Etude et Application des transformées géométriques à la Compression des images haute résolution et à la Biométrie (Authentification/Vérification de l’empreinte palmaire)*. PhD thesis, PhD thesis, Université de Annaba , Algérie, 2016.
- [63] Karthik Nandakumar. **Multibiometric systems: Fusion strategies and template security**. Technical report, MICHIGAN STATE UNIV EAST LANSING DEPT OF COMPUTER SCIENCE/ENGINEERING, 2008.
- [64] Tin Kam Ho, Jonathan J. Hull, and Sargur N. Srihari. **Decision combination in multiple classifier systems**. *IEEE transactions on pattern analysis and machine intelligence*, 16(1): 66–75, 1994.
- [65] Pradeep K Atrey, M Anwar Hossain, Abdulmotaleb El Saddik, and Mohan S Kankanhalli. **Multimodal fusion for multimedia analysis: a survey**. *Multimedia systems*, 16(6):345–379, 2010.
- [66] Jennifer Tetzlaff Douglas G., Altman David Moher, Alessandro Liberati. **Preferred Reporting Items for Systematic Reviews and MetaAnalyses: The PRISMA Statement**. *The PRISMA Group, PLoS Med.*, 2009.
- [67] Yves Gingras. *Bibliometrics and Research Evaluation*. The MIT Press (Book), 2016.
- [68] scopus preview. **Availablen Online: <https://www.scopus.com>**. (Accessed on February 5, 2020).
- [69] crossref. **Availablen Online: <https://www.crossref.org/>**. (Accessed on February 5, 2020).
- [70] Google Scholar. **Availablen Online: <https://scholar.google.com/>**. (Accessed on February 5, 2020).
- [71] Microsoft Academic. **Availablen Online: <https://academic.microsoft.com/>**. (Accessed on February 5, 2020).

- [72] Angela Repanovici. **Measuring the visibility of the university’s scientific production using google scholar, Publish or Perish software and Scientometrics**. In *World Library and Information Congress: 76th IFLA General Conference and Assembly*. Retrieved December, volume 19, page 2010, 2010.
- [73] Anne-Wil Harzing. *The Publish or Perish Book*. Tarma Software Research Pty Ltd, Melbourne, Australia,, 2011.
- [74] Bernard J Jansen and Udo Pooch. **A review of web searching studies and a framework for future research**. *Journal of the American Society for Information science and Technology*, 52(3):235–246, 2001.
- [75] Wenming Yang, Xiaola Huang, Fei Zhou, and Qingmin Liao. **Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion**. *Information sciences*, 268:20–32, 2014.
- [76] SDUMLA-HM. Finger vein database available in: <http://mla.sdu.edu.cn/info/1006/1195.htm>, 2016. URL <http://mla.sdu.edu.cn/info/1006/1195.htm>.
- [77] PolyU FKP. Finger-knuckle-print database available in: <https://www4.comp.polyu.edu.hk/biometrics/FKP.htm>, 2017. URL <https://www4.comp.polyu.edu.hk/~biometrics/FKP.htm>.
- [78] Pavol Marák—Alexander Hambalik. **Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation**. *Tatra Mt. Math. Publ*, 67: 117–134, 2016.
- [79] Lunji Qiu. **Fingerprint sensor technology**. In *2014 9th IEEE Conference on Industrial Electronics and Applications*, pages 1433–1436. IEEE, 2014.
- [80] Pooja A Parmar and Sheshang D Degadwala. **Fingerprint indexing approaches for biometric database: a review**. *International Journal of Computer Applications*, 130(13), 2015.
- [81] Jianjiang Feng, Soweon Yoon, and Anil K Jain. **Latent fingerprint matching: Fusion of rolled and plain fingerprints**. In *International Conference on Biometrics*, pages 695–704. Springer, 2009.
- [82] FVC 2004 fingerprint database. Fingerprint database available in: <http://bias.csr.unibo.it/fvc2004/databases.asp>, 2004. URL <http://bias.csr.unibo.it/fvc2004/databases.asp>.
- [83] K Syazana-Itqan, AR Syafeeza, NM Saad, Norihan Abdul Hamid, and Wira Hidayat Bin Mohd Saad. **A review of finger-vein biometrics identification approaches**. *Indian Journal of Science and Technology*, 9(32), 2016.
- [84] Ajay Kumar and Yingbo Zhou. Human identification using finger images. *IEEE Transactions on image processing*, 21(4):2228–2244, 2012.
- [85] Bram T Ton and Raymond NJ Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. In *Biometrics (ICB), 2013 International Conference on*, pages 1–5. IEEE, 2013.
- [86] Yu Lu, Shan Juan Xie, Sook Yoon, Zhihui Wang, and Dong Sun Park. An available database for the research of finger vein recognition. In *Image and Signal Processing (CISP), 2013 6th International Congress on*, volume 1, pages 410–415. IEEE, 2013.

- [87] Wenming Yang, Xiaola Huang, Fei Zhou, and Qingmin Liao. **Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion**. *Information sciences*, 268:20–32, 2014.
- [88] Ajay Kumar. **Importance of being unique from finger dorsal patterns: Exploring minor finger knuckle patterns in verifying human identities**. *IEEE transactions on information forensics and security*, 9(8):1288–1298, 2014.
- [89] Lin Zhang, Lei Zhang, David Zhang, and Hailong Zhu. **Online finger-knuckle-print verification for personal authentication**. *Pattern recognition*, 43(7):2560–2571, 2010.
- [90] IIT Delhi Finger Knuckle Database. Finger-knuckle-print database available in: <https://www4.comp.polyu.edu.hk/biometrics/FKP.htm>, 2009. URL https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm.
- [91] The Hong Kong Polytechnic University Contactless Finger Knuckle Images Database (HKPU FKP). **finger-knuckle-print database Available in: <https://www4.comp.polyu.edu.hk/csajaykr/fn1.htm>**, 2014. URL https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm.
- [92] The Hong Kong Polytechnic University Contactless Hand Dorsal Images Database (HKPU HDI). **finger-knuckle-print database Available in: <https://www4.comp.polyu.edu.hk/csajaykr/knuckleV2.htm>**, 2016. URL <https://www4.comp.polyu.edu.hk/~csajaykr/knuckleV2.htm>.
- [93] Andreas François Vermeulen. **Classic Machine Learning**. In *Industrial Machine Learning*, pages 13–62. Springer, 2020.
- [94] Jay H Lee, Joohyun Shin, and Matthew J Realf. **Machine learning: Overview of the recent progresses and implications for the process systems engineering field**. *Computers & Chemical Engineering*, 114:111–121, 2018.
- [95] Mayank and Richa Singh Angshul Majumdar Vatsa. *Deep Learning in Biometrics*. CRC Press Taylor and Francis Group (Book), 2018.
- [96] Bir Bhanu and Ajay Kumar. *Deep learning for biometrics*. Springer (Book), 2017.
- [97] Ryszard S Choras. **Image feature extraction techniques and their applications for CBIR and biometrics systems**. *International journal of biology and biomedical engineering*, 1(1): 6–16, 2007.
- [98] Paul Geladi, Hans Isaksson, Lennart Lindqvist, Svante Wold, and Kim Esbensen. **Principal component analysis of multivariate images**. *Chemometrics and Intelligent Laboratory Systems*, 5(3):209–220, 1989.
- [99] Svante Wold, Kim Esbensen, and Paul Geladi. **Principal component analysis**. *Chemometrics and intelligent laboratory systems*, 2(1-3):37–52, 1987.
- [100] Pierre Comon. **Independent component analysis, a new concept?** *Signal processing*, 36(3): 287–314, 1994.
- [101] Robert Harry Riffenburgh. *Linear discriminant analysis*. PhD thesis, Virginia Polytechnic Institute, 1957.
- [102] John Shawe-Taylor, Nello Cristianini, et al. *Kernel methods for pattern analysis*. Cambridge university press, 2004.

- [103] Heiko Hoffmann. **Kernel PCA for novelty detection**. *Pattern recognition*, 40(3):863–874, 2007.
- [104] Jong-Min Lee, S Joe Qin, and In-Beum Lee. **Fault detection of non-linear processes using kernel independent component analysis**. *The Canadian Journal of Chemical Engineering*, 85(4):526–536, 2007.
- [105] Taiping Zhang, Bin Fang, Yuan Yan Tang, Zhaowei Shang, and Bin Xu. **Generalized discriminant analysis: A matrix exponential approach**. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 40(1):186–197, 2009.
- [106] Ning Wang, Qiong Li, Ahmed A Abd El-Latif, Jialiang Peng, and Xiamu Niu. **An enhanced thermal face recognition method based on multiscale complex fusion for Gabor coefficients**. *Multimedia tools and applications*, 72(3):2339–2358, 2014.
- [107] Chun-Hui Hsiao. **State analysis of linear time delayed systems via Haar wavelets**. *Mathematics and Computers in Simulation*, 44(5):457–470, 1997.
- [108] David G Lowe. **Distinctive image features from scale-invariant keypoints**. *International journal of computer vision*, 60(2):91–110, 2004.
- [109] Matti Pietikäinen, Abdenour Hadid, Guoying Zhao, and Timo Ahonen. **Local binary patterns for still images**. In *Computer vision using local binary patterns*, pages 13–47. Springer, 2011.
- [110] Marko Heikkilä, Matti Pietikäinen, and Cordelia Schmid. **Description of interest regions with local binary patterns**. *Pattern recognition*, 42(3):425–436, 2009.
- [111] Martin Lades, Jan C Vorbruggen, Joachim Buhmann, Jörg Lange, Christoph Von Der Malsburg, Rolf P Wurtz, and Wolfgang Konen. **Distortion invariant object recognition in the dynamic link architecture**. *IEEE Transactions on computers*, 42(3):300–311, 1993.
- [112] Tai Sing Lee. **Image representation using 2D Gabor wavelets**. *IEEE Transactions on pattern analysis and machine intelligence*, 18(10):959–971, 1996.
- [113] Sotiris B Kotsiantis, I Zaharakis, P Pintelas, et al. **Supervised machine learning: A review of classification techniques**. *Emerging artificial intelligence applications in computer engineering*, 160(1):3–24, 2007.
- [114] Pratap Chandra Sen, Mahimarnab Hajra, and Mitadru Ghosh. **Supervised classification algorithms in machine learning: A survey and review**. In *Emerging technology in modelling and graphics*, pages 99–111. Springer, 2020.
- [115] Xingqun Qi, Tianhui Wang, and Jiaming Liu. **Comparison of Support Vector Machine and Softmax Classifiers in Computer Vision**. In *2017 Second International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China*. IEEE, dec 2017. doi: 10.1109/icmce.2017.49. URL <https://doi.org/10.1109%2Ficmce.2017.49>.
- [116] Yichuan Tang. **Deep learning using support vector machines**. *arXiv preprint arXiv:1306.0239*, 2013.
- [117] Dongmei Han, Qigang Liu, and Weiguo Fan. **A new image classification method using CNN transfer learning and web data augmentation**. *Expert Systems with Applications*, 95: 43–56, 2018.

- [118] Yoon Chung Han. *Biometric Data Art: Personalized Narratives and Multimodal Interaction*. University of California, Santa Barbara (Book), 2016.
- [119] xuran ZHAO. *Réduction de la Dimensionnalité Multivue pour la Biométrie Multimodal*. PhD thesis, 2013.
- [120] Yann LeCun et al. **LeNet-5, convolutional neural networks**. URL: <http://yann.lecun.com/exdb/lenet>, 20(5):14, 2015.
- [121] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. **Imagenet classification with deep convolutional neural networks**. *Advances in neural information processing systems*, 25: 1097–1105, 2012.
- [122] Karen Simonyan and Andrew Zisserman. **Very deep convolutional networks for large-scale image recognition**. *arXiv preprint arXiv:1409.1556*, 2014.
- [123] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. **Going deeper with convolutions**. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1–9, 2015.
- [124] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. **Imagenet: A large-scale hierarchical image database**. In *2009 IEEE conference on computer vision and pattern recognition*, pages 248–255. Ieee, 2009.
- [125] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, et al. **Imagenet large scale visual recognition challenge**. *International journal of computer vision*, 115(3):211–252, 2015.
- [126] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. **Deep Residual Learning for Image Recognition**. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR, Las Vegas, NV, USA)*. IEEE, jun 2016. doi: 10.1109/cvpr.2016.90. URL <https://doi.org/10.1109%2Fcvpr.2016.90>.
- [127] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. **Densely connected convolutional networks**. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 4700–4708, 2017.
- [128] Saptarshi Sengupta, Sanchita Basak, Pallabi Saikia, Sayak Paul, Vasilios Tsalavoutis, Frederick Atiah, Vadlamani Ravi, and Alan Peters. **A review of deep learning with special emphasis on architectures, applications and recent trends**. *Knowledge-Based Systems*, 194: 105596, 2020.
- [129] DH Kim and T MacKinnon. **Artificial intelligence in fracture detection: transfer learning from deep convolutional neural networks**. *Clinical radiology*, 73(5):439–445, 2018.
- [130] Richard Jiang, Chang-Tsun Li, Danny Crookes, Weizhi Meng, and Christophe Rosenberger. *Deep biometrics*. Springer (Book), 2020.
- [131] Yu-Dong Zhang, Vishnu Varthanan Govindaraj, Chaosheng Tang, Weiguo Zhu, and Junding Sun. **High performance multiple sclerosis classification by data augmentation and AlexNet transfer learning model**. *Journal of Medical Imaging and Health Informatics*, 9(9):2012–2021, 2019.

- [132] Asifullah Khan, Anabia Sohail, Umme Zahoora, and Aqsa Saeed Qureshi. **A survey of the recent architectures of deep convolutional neural networks**. *Artificial Intelligence Review*, 53(8):5455–5516, apr 2020. doi: 10.1007/s10462-020-09825-6. URL <https://doi.org/10.1007%2Fs10462-020-09825-6>.
- [133] S. Veluchamy and L.R. Karlmarx. **System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier**. *IET Biometrics*, 6(3):232–242, jan 2017. doi: 10.1049/iet-bmt.2016.0112. URL <https://doi.org/10.1049%2Fiet-bmt.2016.0112>.
- [134] Wenming Yang, Xiaola Huang, Fei Zhou, and Qingmin Liao. **Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion**. *Information Sciences*, 268:20–32, jun 2014. doi: 10.1016/j.ins.2013.10.010. URL <https://doi.org/10.1016%2Fj.ins.2013.10.010>.
- [135] Wenming Yang, Chuan Qin, Xingjun Wang, and Qingmin Liao. **Cross section binary coding for fusion of finger vein and finger dorsal texture**. In *2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan*. IEEE, mar 2016. doi: 10.1109/icit.2016.7474843. URL <https://doi.org/10.1109%2Ficit.2016.7474843>.
- [136] Weibo Liu, Zidong Wang, Xiaohui Liu, Nianyin Zeng, Yurong Liu, and Fuad E. Alsaadi. **A survey of deep neural network architectures and their applications**. *Neurocomputing*, 234: 11–26, apr 2017. doi: 10.1016/j.neucom.2016.12.038. URL <https://doi.org/10.1016%2Fj.neucom.2016.12.038>.
- [137] Purnawarman Musa, Farid Al Rafi, and Missa Lamsani. **A Review: Contrast-Limited Adaptive Histogram Equalization (CLAHE) methods to help the application of face recognition**. In *2018 Third International Conference on Informatics and Computing (ICIC), Palembang, Indonesia*. IEEE, oct 2018. doi: 10.1109/iac.2018.8780492. URL <https://doi.org/10.1109%2Fiac.2018.8780492>.
- [138] Kamer Vishi and Vasileios Mavroeidis. An evaluation of score level fusion approaches for fingerprint and finger-vein biometrics. *arXiv preprint arXiv:1805.10666*, 2018.
- [139] ISO/IECTR 24722:2015. Multimodal and other multibiometric fusion. *Information Technology*, 2018.
- [140] Julien Mahier, Baptiste Hemery, Mohamad El-Abed, Mohamed El-Allam, Mohamed Bouhaddaoui, and Christophe Rosenberger. **Computation EvaBio: A Tool for Performance Evaluation in Biometrics**. *International Journal of Automated Identification Technology (IJAIT)*, page 24, 2011. URL <https://hal.archives-ouvertes.fr/hal-00984026>.
- [141] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. **A fingerprint and finger-vein based cancelable multi-biometric system**. *Pattern Recognition*, 78:242–251, jun 2018. doi: 10.1016/j.patcog.2018.01.026. URL <https://doi.org/10.1016%2Fj.patcog.2018.01.026>.
- [142] Zhi Liu and Shangling Song. **An embedded real-time finger-vein recognition system for mobile devices**. *IEEE Transactions on Consumer Electronics*, 58(2):522–527, 2012.
- [143] V Ty and G Harish. **An embedded real-time finger-vein recognition system for security levels**. *International journal of Ensrineerinsr Research and General Science*, 1(1), 2013.

- [144] AR Syafeeza, LH Kwan, K Syazana-Itqan, Hamid NA, WHM Saad, and Zahariah Manap. **A low cost finger-vein capturing device**. 2006.
- [145] AR Syafeeza, K Faiz, K Syazana-Itqan, YC Wong, Zarina Mohd Noh, MM Ibrahim, and NM Mahmod. **Design of Finger-vein Capture Device with Quality Assessment using Arduino Microcontroller**. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 9(1):55–60, 2017.
- [146] Qiuyuan Huang, Kangzhe Hu, Peng Zhou, Yuxiang Luo, and Lina Wu. **Design of Finger Vein Capturing Device Based on ARM and CMOS Array**. In *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pages 193–196. IEEE, 2018.
- [147] SP Rozendal. **Redesign of a finger vein scanner**. B.S. thesis, University of Twente, 2018.
- [148] Michał Waluś, Krzysztof Bernacki, and Jacek Konopacki. **Impact of NIR wavelength lighting in image acquisition on finger vein biometric system effectiveness**. *Opto-Electronics Review*, 25(4):263–268, 2017.
- [149] G Senthilkumar, K Gopalakrishnan, and V Sathish Kumar. Embedded image capturing system using raspberry pi system. *International Journal of Emerging Trends & Technology in Computer Science*, 3(2):213–215, 2014.
- [150] M Abdul Kader Riyaz, S ArunJeyakumar, M Abdul Hameed Sharik, and A Tamilarasi. **Graphene coated LED based automatic street lighting system using Arduino microcontroller**. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pages 1555–1560. IEEE, 2017.
- [151] KH Shakthi Murugan, V Jacintha, and S Agnes Shifani. **Security system using raspberry Pi**. In *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, pages 863–864. IEEE, 2017.
- [152] Jia Xu, Cui Jianjiang, Xue Dingyu, and Pan Feng. **Near infrared vein image acquisition system based on image quality assessment**. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 922–925. IEEE, 2011.
- [153] Rajeshwar Dass and Niranjan Yadav. **Image quality assessment parameters for despeckling filters**. *Procedia Computer Science*, 167:2382–2392, 2020.
- [154] WA Mustafa, H Yazid, M Jaafar, M Zainal, and AS Abdul. and n. mazlan,“a review of image quality assessment (iqa): Snr, gcf, ad, nae, psnr, me,”. *J. Adv. Res. Comput. Appl*, 7 (1):1–7, 2017.