REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Aboubakr Belkaïd Tlemcen

Faculté des Sciences

Département d'informatique

Mémoire

Présenté pour l'obtention du diplôme de
Magister en Informatique

Option: Intelligence Artificielle et Aide à la Décision

Par:

Mohammed DEMRI

Intitulé:

Multimodal Biometric Fusion Using Evolutionary Techniques

Soutenu devant le Jury :

Président: Mr. Fethi BEREKSI REGUIG	Professeur	Université Abou Bkr Belkaid, Tlemcen
Examinateur: Mr. Med El-Amine CHIKH	Professeur	Université Abou Bkr Belkaid, Tlemcen
Examinateur: Mr. Abdekarim BENAMMAR	MCB	Université Abou Bkr Belkaid, Tlemcen
Encadreur: Mr. Abdellatif RAHMOUN	Professeur	Université Djillali Liabes, Sidi Bel abbes

June 2012

Abstract

Multimodal Biometric Fusion Using Evolutionary Techniques

Biometrics refers to the automatic recognition of the person based on his physiological or behavioral characteristics, such as fingerprint, face, voice, gait …etc. However, Unimodal biometric system suffers from several limitations, such as non-universality and susceptibility to spoof attacks. To alleviate this problems, information from different biometric sources are combined and such systems are known as **multimodal biometric** systems. In this thesis, we propose Particle Swarm Optimization **(PSO)** and Genetic Algorithm (**GA**) as two evolutionary techniques to combine face and voice modalities at the matching scores level. The effectiveness of these two techniques is compared to those obtained by using a simple **BFS**, a hybrid intelligent (**ANFIS**) and a statistical learning (**SVM**) fusion techniques. The well-known **Min-Max** normalization technique is used to transform the individual matching scores into a common range before the fusion can take place. The proposed schemes are experimentally evaluated on publicly available datasets of scores (**XM2VTS**, **TIMIT**, **NIST** and **BANCA**) and under three different data quality conditions namely, clean varied and degraded. In order to reduce the effects of scores variations on the accuracy of biometric systems, we use Unconstraint Cohort Normalization (**UCN**) mechanism to normalize the matching scores before combining them. It is revealed in this study that by deploying such fusion techniques, the verification error rates (**EERs)** can be reduced considerably, and subjecting the scores to UCN process before combining them has resulted in reducing the verification EERs for the single modalities as well as for multimodal biometric fusion.

Keywords: Multimodal Biometrics; face; voice; Matching Scores; Evolutionary Techniques; optimization; hybrid intelligent; statistical learning; PSO; GA; BFS; ANFIS; SVM; Min-Max; UCN; performance evaluation.

Résumé

L'utilisation des Techniques évolutionnaires pour la fusion biométrique Multimodal

La biométrie est l'identification automatique de la personne basée sur ses caractéristiques physiologiques ou comportementales, telles que les empreintes digitales, le visage, la voix,... etc. Cependant, Un système biométrique Unimodal souffre de certaines limitations, telles que la non-universalité et la susceptibilité aux falsifications. Pour remédier aux ces problèmes, des informations provenant de différentes sources biométriques sont combinés, et de tels systèmes sont appelés les system biométrique multimodal. Dans ce mémoire, nous proposons l'utilisation de l'algorithme d'optimisation par les essaims de particules (**OEP**) et les algorithmes génétiques (**AG**) comme deux techniques évolutionnaires pour combiner la modalité du visage et de la voix au niveau des scores. L'efficacité de ces deux techniques est comparée à ceux obtenus en utilisant une simple **BFS**, une méthode intelligente hybride (**ANFIS)** et une technique d'apprentissage statistique (**SVM)**. La technique de normalisation Min-Max est utilisée pour transformer les scores individuels en même intervalle avant de les combiner. Les deux techniques proposées sont évaluées expérimentalement sur des scores publiquement disponibles (**XM2VTS**, **TIMIT**, le **NIST** et **BANCA**) et sous trois conditions de qualité de données à savoir, propres, variées et dégradées. Afin de réduire l'effet de variation de scores sur l'efficacité du système biométrique, nous utilisons un mécanisme de normalisation de cohorte sans contrainte (UCN). Cette étude révèle que par le déploiement de telles techniques de fusion, les taux d'erreur de vérification (EER) peuvent être réduits considérablement, et la normalisation des scores par l'UCN avant de les combiner, a permis de réduire les EER pour les modalités individuels ainsi que pour fusion biométrique multimodal

Mots-clés: Biométrie multimodale ; Le visage ; La voix ; scores de correspondance; Techniques évolutionnaires ; optimisation ; intelligent hybride; apprentissage statistique ; PSO ; GA ; BFS ; ANFIS ; SVM ; Min-Max ; UCN ; évaluation des performances.

ملخص

استخدام تقنيات التطورفي دمج القياسات البيومترية

التحقق من الهوية (البيومترية) هي التعرف الآلي على الأشخاص اعتمادا على صفاتهم الفيزيولوجية أو السلوكية، مثل بصمة الإصبع، الصوت، ... الخ. إلا أن نظام التحقق من الهوية الأحادي الواسطة يعاني من بعض القيود مثل: لا شمولية وإمكانية التعرض للمحاكاة و التقليد. و للتخفيف من حدة هذه المشاكل وتعزيز أداء النظام البيومتري، يتم دمج المعلومات من مصادر مختلفة، وهذا ما يعرف بالنظام **البيومتري المتعدد الوسائط**. في هذه المذكرة، نقترح استخدام سرب الجسيمات الأمثل (**PSO**) و الخوارزميات الجينية (**GA**) كتقنيتين تطوريتين لدمج وساطتي الصوت و الوجه علي مستوى درجات التطابق. تتم مقارنة مدى فعالية هذه التقنيتين مع تلك التي حصلنا عليها باستخدام كل من تقنية دمج بسيطة (**BFS**)، تقنية ذكية هجينة (**ANFIS**) وتقنية التعلم الإحصائي (**SVM**). تستخدم تقنية التطبيع **Min-Max** المشهورة من اجل تحويل درجات التطابق إلى نفس المجال قبل عملية الدمج. يتم تجريبياً تقييم فعالية التقنيات المقترحة على بعض قواعد البيانات المتاحة (**NIST،TIMIT, XM2VTS, BANCA**) وتحت ثلاثة ظروف مختلف لجودة البيانات وهي: نقية، متنوعة ومتدهورة. و من أجل الحد من آثار التغير(الاختلاف) في درجات التطابق علي دقة النظام البيومتري المتعدد الوسائط، قمنا بتطبيع الدرجات قبل دمجها باستخدام تقنية التطبيع الغير مقيد (**UCN**). وقد كشفت هذه الدراسة أن اعتماد مثل هذه التقنيات في عملية دمج الوسائط البيومترية على مستوى الدرجة، يقلل من نسبة خطأ التحقق (**EER**) بنسبة كبيرة ، و أن إخضاع درجات التوافق إلى تقنية **UCN** قبل دمجها أدى كذالك إلى تخفيف خطأ التحقق سواءً بالنسبة للوسائط الأحادية أو بالنسبة للنظام المتعدد الوسائط البيومترية.

الكلمات المفتاحية: متعددة الوسائط البيومترية ؛ دمج على مستوى الدرجة ؛ الوجه ؛ الصوت ؛ تقنيات التطور ؛ التحسين ؛ ذكي هجين ؛ تعلم إحصائي ؛ التطبيع الغير مقيد ؛ تقييم الفعالية، **PSO, GA, ANFIS, SVM, BFS, Min-Max, UCN**

To my parents;
To all my teachers;
To all my friends.

Acknowledgments

First and foremost, I am extremely thankful to almighty Allah for giving me the chance, strength and courage to complete this work, and without his willing, this thesis would not have been possible.

I would like to express my sincere gratitude to my advisor ***Mr. Abdelatif RAHMOUN*** *for providing me the opportunity to work in the exciting and challenging area of biometrics. His motivation and support have guided me towards the successful completion of my thesis.*

I address my sincere thanks to ***Prof. Fethi BEREKSI REGUIG*** *who makes me the honor of chairing my thesis jury.*

I am grateful to other jury members: ***Prof. Med Amine CHEIKH*** *and* ***Dr. Abdekarim BENAMMAR*** *for taking some of their golden time to review this dissertation, for their guidance and for their critical but valuable and constructive comments.*

My special gratitude also goes to ***Prof. CHIKH Med Amine****, the chief of our Magister project, for his kindness and simplicity.*

I am sincerely and heartily grateful to ***Mme. Fewzia BETOUAF****, for her hospitality and encouragement.*

I also extend my thanks to all those, near or far, who contributed to this work whether by participation or encouragement, thank you to: Ammar, Walid, Seddik, Mamoun, Touhami, Mohammed, Fateh, M'hammed, Hichem and Abedelhafid.

Finally I express my affection and my gratitude to my family (my parents, my brothers and sisters) for their patience and unwavering support. Without their help and support, this thesis would not have been possible.

Last but absolutely not least, my heartfelt thanks to all those who I forgot but who nevertheless deserve to be thanked.

Table of Contents

Abstract……………………………………………………………………………….. I
Dedication…………………………………………………………………………... IV
Acknowledgments…………………………………………………………………..V
Table of Contents………………………………………………………………….. VI
Glossary of Important Terms……………………………………………………... X
List of Tables………………………………………………………...……….. XIII
List of Figures……………………………………………………..……………. XIV

General Introduction

1. Background……………………………………………………..……………. 01
2. Motivations………………………………………………………………………. 02
3. Aims and Objectives ………………………………………………………………. 04
4. Thesis Organization……………………………………………………..……. 04

Chapter 01: Biometrics and Multimodal Biometric Systems

1.1 Introduction ……………………………………………..………….…..………..…07
1.2 Identity verification using a biometric system……………………………….…………..07
1.2.1 The identity verification ……………………………………………….…..………07
1.2.2 Biometrics…………………………………………………………………….………….08
1.2.3 Biometric characteristics……………………………..……………………….…..……….09
1.2.4 Biometric Modalities……………………………………………………...……….…..10
1.2.4.1 Facial recognition…………………………………………………..………….…..10
1.2.4.2 Voice verification……………………………………………………………….……11
1.2.4.3 Fingerprint recognition………………………………………..……….……..12
1.2.4.4 Hand geometry………………………………………………...………………..12
1.2.4.5 Iris recognition …………………………………………………….……………..13
1.2.4.6 Keystroke dynamics………………………………………………….…………..13
1.2.4.7 Signature…………………………..………………………..………………………13
1.2.4.8 Gait recognition……………………………………………………..…………….14
1.2.4.9 Retina scanning……………………………………………………………..………14
1.2.5 The structure of a biometric system………………………………………..……15
1.2.6 Verification versus identification……………………………………………….……16
1.2.6.1 Verification…………………………………………………...…………..16
1.2.6.2 Identification……………………………………………………………….…….……17
1.2.7 Limitations of unimodal biometric systems…………………………….…………….……17
1.3 Multimodal biometric systems………………………………………..………..…18
1.3.1 Advantages of multimodal biometric systems……………………………..……….......19
1.3.2 Fusion scenarios……………………………………………………………….………..19
1.3.2.1 Multiple Sensors…………………………………………………………….…………20
1.3.2.2 Multiple algorithms………………………………………………..…………..20

1.3.2.3 Multiple instances ……………………………………………………………..…....20
1.3.2.4 Multi-sample systems………………………………………..……………...20
1.3.2.5 Multiple modalities…………………………………………….……….....20
1.3.3 Different levels of fusion……………………………..…………..…………21
1.3.3.1 Pre-Classification fusion……………………………………..…………22
1.3.3.1.1 Sensor Level……………………………………………….……….……..22
1.3.3.1.2 Feature Extraction Level…………………………………………….……22
1.3.3.2 Post-Classification fusion…………………………..………………..……..22
1.3.3.2.1 Matching Score Level……………………………………………..……22
1.3.3.2.2 Decision Level…………………………………………………………23
1.4 Conclusion and Summary………………………..……………………….………..24

Chapter 02: Performance evaluation of a biometric system

2.1 Introduction………………………………………………………………...26
2.2 The performance evaluation ……………………………………………….…....26
2.2.1 Error Rates …………………………………………….…………….……… 26
2.2.2 Threshold criterion…………………………………………..………….……28
2.2.3 Performance curves …………………………...……………….…...……………29
2.2.3.1 FAR vs FRR curve……………………………………….…..…..………………..29
2.2.3.2 Receiver Operating Characteristic (ROC) curve……………………………….……..30
2.2.3.3 Detection Error Trade-off (DET) curve………………………………….....……….31
2.2.4 Operating Points……………………….……...……………..……….…….31
2.2.4.1 Equal Error Rate (EER) ……………………………………………..…………….31
2.2.4.2 Weighted Error Rate (WER)……………………………...……….....….32
2.2.4.3 Fixed FAR……………………………………..………………………….……32
2.2.4.4 Fixed FRR……………………………………..…………………….....…….33
2.2.5 Operating points on the DET curves………………………………….…...…….33
2.2.6 The choice of an operating point ……………………………...……………...34
2.3 Comparing biometric systems……………………..……………………......….35
2.4 Summary and Conclusion………………………..…………...…………......…….35

Chapter 03: Multimodal Biometrics Fusion Techniques

3.1 Introduction…………………………………………………….……………………37
3.2 Score Normalization ………………………………………………….………………..37
3.2.1 Scores Normalization Techniques………………………………………………38
3.2.1.1 Min-Max Normalization (MM)……………….…………………………………38
3.2.1.2 Z-score Normalization (ZS)……………………...……………………………..38
3.2.1.3 Tanh (TH)……………………………………………………………………….39
3.2.1.4 Double sigmoid………………………………………………....……………39
3.2.1.5 Decimal Scaling Normalization…………..……………………………………..40
3.2.1.6 Median and median absolute deviation (MAD)normalization………………………..40
3.2.1.7 Unconstrained Cohort Normalization (UCN)………………………...……………41

3.3 Multimodal biometric score level fusion techniques……………………………….42
3.3.1 Simple Approach…………………………………………………………...43
3.3.1.1 Product Rule…………………………………………………………….43
3.3.1.2 Sum Rule………………………………………………………………….43
3.3.1.3 Maximum Rule………………………………………………………….43
3.3.1.4 Minimum Rule………………………………………………………….44
3.3.1.5 Brute Force Search BFS………………………………………………….44
3.3.1.5.1Advantage and disadvantage of BFS ……………………………………44
3.3.1.5.2 Brute Force Search for Multimodal biometric scores fusion…………..…………44
3.3.2 Evolutionary approach…………………………………………………..45
3.3.2.1 Genetic Algorithms……………………………………………………….45
3.3.2.1.1 GA Operators ……………………………………………...……………45
3.3.2.1.2 Advantages and disadvantages of Gas………………………………….46
3.3.2.1.3 Genetic Algorithms for Multimodal biometric scores fusion …………….…46
3.3.2.2 Particle Swarm Optimization (PSO)…………………………………..……47
3.3.2.2.1 Principle of Particle Swarm Optimization Algorithm……………………..48
3.3.2.2.2 Advantages and Disadvantages of the Basic PSO Algorithm …..………………..50
3.3.2.2.3 Multimodal biometric scores fusion using PSO……………………..………51
3.3.3 Hybrid Intelligent Approach………………………………………………51
3.3.3.1 Adaptive Neuro-Fuzzy Systems………………………………………………52
3.3.3.1.1 ANFIS Architecture……………………………………………...…………52
3.3.3.1.2 Learning algorithm of ANFIS……………………………………………..55
3.3.3.1.3 Advantages and disadvantages of ANFIS algorithm……………………………56
3.3.3.1.4 ANFIS for Multimodal biometric scores fusion……………………...………56
3.3.4 Statistical approach……………………………………………………...…………56
3.3.4.1 Support Vector Machine (SVM)………………………………………………56
3.3.4.1.1 Linear Support Vector Machines for Linearly Separable Case……………..……..57
3.3.4.1.2 Linear SVM for non-linearly separable data……………………..…………….59
3.3.4.1.3 Non-linear SVM……………………………………………………………...59
3.3.4.1.4 Advantages and disadvantages of SVM…………………...……………………60
3.3.4.1.5 Matching score level fusion using SVM……………………...………………61
3.4 Recent works on Multimodal biometrics fusion …………………………………….61
3.5 Conclusion and summary………………………………………………………64

Chapter 04: Experimental Setup and Results Discussion

4.1 Introduction………………………………………...……………………66
4.2 Experimental Setup………………………………………………………..66
4.2.1 Multimodal biometric Databases……………………...…………………………66
4.2.1.1 BANCA Database………………………………………………………67
4.2.1.2 XM2VTS Database……………………………………………..…………67
4.2.1.3 TIMIT Database………………………………………………...……67
4.2.1.4 NIST Database…………………………………………………………..67
4.2.2 Design and implementation………………………………………………….. 68
4.2.2.1 Development Tools……………………………………………………..68

4.2.2.2 The main interface of our prototype…………………………………..……………68
4.2.2.3 The fusion process……………………………………………………………………69
4.2.3 Results and Discussions……………………………………………….....……….74
4.2.3.1 Fusion under clean data condition……………………………………….…………..74
4.2.3.2 Fusion under Varied Data condition……………………………………...………78
4.2.3.3 Fusion under Degraded Data condition……………………………..……………..80
4.3 Summary and Conclusion…………………………………………………...……….88

Conclusions and Future Works

1. Conclusion ………………………………………………………………………… 85
2. Recommendations for future work …………………………………………………… 86

References

References………………………………………………………………………………… 87

Glossary of Important Terms

ID	IDentity
PDA	Personal Digital Assistance
PC	Personal Computer
FA	False Acceptance
FR	False Rejection
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
ROC	Receiver Operating Characteristic
DET	Detection Error Trade-off
WER	Weighted Error Rate
HTER	Half Total Error Rate
WER	Weighted Error Rate
WTER	Weighted Total Error Rate
MM	Min-Max
UCN	Unconstrained Cohort Normalization
ZS	Z-score
std	standard deviation
BFS	Brute Force Search
AUC	Area Under the Curve
TH	Tanh
MAD	Median and median absolute

GA	Genetic algorithm
PSO	Particle Swarm Optimization
pbest	Particle’s best
gbest	global best
ANFIS	Adaptive Neuro-Fuzzy Inference System
ANN	Artificial Neural Network
FL	Fuzzy Logic
LSE	Least Squares Estimate
SVM	Support Vector Machine
ERM	Risk Minimization
SRM	Structural Risk Minimization
VC	Vapnik-Chervonenkis
PCA	Principle Component Analysis
MFCC	Mel Frequency Cepstral Coefficients
HMM	Hidden Markov Model
GMM	Gaussian Mixture Models
DS	Dempster-Shafer
AUC	Area Under Curve
LLR	Likelihood Ratio
M2VTS	Multi-Modal Verification for Teleservices and Security applications
XM2VTS	eXtended M2VTS
TIMIT	Texas Instruments Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
MATLAB	MATrix LABoratory

RAD	Rapid Application Development
GUI	Graphical User Interface
IDE	Integrated Development Environment
QP	Quadratic Programming

List of Tables

Chapter 03

Table 3.1: Tow passes in the hybrid learning procedure for ANFIS ……………………..……..…55
Table 3.2: Commonly Used Kernel Functions……………………………………………..…….60

Chapter 04

Table 4.1: Results on the clean data at the Equal Error Rate (EER)………………………..…74
Table 4.2: Results on the varied data at the Equal Error Rate (EER)...................................….... 78
Table 4.3: Results on the degraded data at the Equal Error Rate (EER)……………………. 81

List of Figures

Chapter 01

Figure 1.1: Authentication schemes……………………………………..…………………08
Figure 1.2: Some biometrics applications………………………………………….……..09
Figure 1.3: Face Modality……………………………..………………………………11
Figure 1.4: Voice Modality……………………………...……………………………..11
Figure 1.5: Fingerprint Modality……………………………………………………….12
Figure 1.6: Hand geometry Modality……………………………..……………………12
Figure 1.7: Iris Modality………………………………………………………………..13
Figure 1.8: Signature Modality…………………………………………………...……….14
Figure 1.9: Gait Modality……………………………………………………...……..14
Figure 1.10: Retina Modality………………………………………………………..……15
Figure 1.11: Biometric Enrollment………………………………………………..………16
Figure 1.12: Biometric Verification…………………………………………………….. 17
Figure 1.13: Biometric Identification…………………………………………….……17
Figure 1.14: Fusion scenarios in multimodal biometric………………………………………..21
Figure 1.15: Fusion levels in multimodal biometrics…………………………………….……….23

Chapter 02

Figure 2.1: Illustration of the FRR and the FAR…………………………………………….28
Figure 2.2: Illustration of The EER point and the optimal Threshold…………………………29
Figure 2.3: FAR vs FRR Curve………………………………………………….………30
Figure 2.4: ROC curves……………………………………………………...………30
Figure 2.5: DET curves……………………………………………………..……….31
Figure 2.6: FAR vs FRR curve………………………………………………….……..32
Figure 2.7: The operating points represented on a DET curve…………………………..……..33

Chapter 03

Figure 3.1: Double sigmoid normalization………………………………………………..40
Figure 3.2: Unconstrained cohort normalization (UCN) ……………………………………42
Figure 3.3: Genetic Algorithm Flowchart……………………………………………...……46
Figure 3.4: **(a)** Type-3 fuzzy reasoning. **(b)** Equivalent ANFIS (type-3 ANFIS)………...……49
Figure 3.5: Illustrating the velocity updating scheme of basic PSO……………………...……49
Figure 3.6: Particle swarm optimization flowchart…………………………………..………51
Figure 3.7: The Separating hyperplane…………………………………………………...……53
Figure 3.8: Mapping from input space to Feature space via a nonlinear map Φ………………59

Chapter 04

Figure 4.1: The main interface of our Biometrics Fusion prototype…………………………...69
Figure 4.2: The fusion flowchart……………………………………………………….………73
Figure 4.3: **(a)** DET curves for different fusion techniques under clean data quality condition without UCN……………………………………………………………………………...………76
Figure 4.3: **(b)** DET curves for different fusion techniques under clean data quality condition with UCN……………………………………………………………………………...……….76
Figure 4.4: **(a)** ROC curves for different fusion techniques under clean data quality condition without UCN………………….......…………………………………………………………………77
Figure 4.4: **(b)** ROC curves for different fusion techniques under clean data quality condition with UCN……………………....……………………………………………………………….77
Figure 4.5: **(a)** DET curves for different fusion techniques under varied data quality condition without UCN…………………………………………………………………..…………….79
Figure 4.5: **(b)** DET curves for different fusion techniques under varied data quality condition with UCN……………………………………………………………………………….....79
Figure 4.6: **(a)** ROC curves for different fusion techniques under varied data quality condition without UCN…………………………………………………………………………………….. 80
Figure 4.6: **(b)** ROC curves for different fusion techniques under varied data quality condition with UCN……………………………………………………………………………...…..80
Figure 4.7: **(a)** DET curves for different fusion techniques under degraded data quality condition without UCN…………………………………………………………………...……………82
Figure 4.7: **(b)** DET curves for different fusion techniques under degraded data quality condition with UCN…………………………………………………………………..…..82
Figure 4.8: **(a)** ROC curves for different fusion techniques under degraded data quality condition without UCN……………………………………………………………………………..83
Figure 4.8: **(b)** ROC curves for different fusion techniques under degraded data quality condition with UCN…………………………………....…………………………………………………….83

General Introduction

1. Background

Nowadays, due to the expansion of the networked society, there is increasingly need for secured and reliable personal identity verification/identification using the Automatic means. The need for reliable, simple, flexible and secure system is a great concern and a challenging issue for several applications that render services to only legitimately enrolled users. Examples of such applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions (teleshopping) and physical access control.

The traditional methods of establishing a person's identity are already widely used in the context of identity verification. These methods are based on something *that you know* (knowledge-based security) such as passwords, which can be shared or forgotten; or something *that you have* or possess (token-based security) such as keys, magnetic cards, ID cards and PIN numbers, which can be shared, stolen, copied or lost **[04]**.

Biometric authentication (also known as Biometrics) is the efficient means of remedying the various problems arising from the traditional authentication means and enhancing the security level and offering greater convenience and several advantages. Biometric authentication **[25, 74, 75]** is the automatic recognition of the person based on *who you are* refers to his/her physiological or *what you produce* refers to his/her behavioral characteristics or features. These distinctive physiological features include face, fingerprints, hand geometry, iris, retina, DNA etc. Behavioral characteristics are actions carried out by a person in a unique way; they include signature, keystroke, voice etc. These characteristics are called biometric modalities or traits.

A biometric system is basically a *pattern recognition* system that acquires biometrics data from the person, extracts the most significant feature set from these data, compares this feature set against the feature sets stored in the database, and take the final decision based on the result of the comparison (Accept/ Reject). Thus, a typical biometric system has four main modules, namely, sensor module, feature extraction module, a matching module, and a database module **[10]**.

Generally, a biometric system has two stages of operation: enrollment and recognition. Enrollment refers to the stage in which the system stores some biometric reference information about the person in a database. In the recognition stage, the system scans the user's biometric trait, extracts features, and matches them against the reference biometric information stored in the database. A high similarity score between the query and the reference data results in the user being authenticated or identified **[69]**.

It is very important to have commonly used criteria to measure the performance of biometric systems, so that these systems could be compared, real-world performance can be estimated, and progress could be motivated. In biometrics, performance is based on the probability of accepting impostor users, referred to False Acceptance Rate (FAR); and the probability of rejecting genuine users, referred to False Rejection Rate (FRR). Receiver Operating Curve (ROC) and Detection Error Trade-off (DET) could be used for a graphical comparison of performances between different systems. For a simple empirical measure, the *Equal Error Rate* (EER) is usually used in biometrics, which refers to the point at which FRR and FAR are identical at a given decision threshold **[77]**.

2. Motivations

Biometric systems that use only one single biometric modality (unimodal biometric system) often suffer from several limitations **[13]** such as noise in sensed data, non universality of the biometric modality which refers to the possibility that a subset of users do not possess the biometric trait being acquired., intra-class variations, unacceptable error rate and the vulnerability to spoof attacks which means that it is possible for unimodal systems to be fooled. Various researchers have recommended that no single biometric modality can provide the protection required for high security applications **[61, 62]**.

To overcome these problems and enhance the performance of biometric systems, information from different biometric modalities are combined, such systems are known as **multimodal biometric** systems **[13**]. Multimodal biometric systems integrate the evidence presented by multiple sources.

Multimodal biometric systems can address the problem of non universality, since multiple traits ensure sufficient population coverage. Further, multibiometric systems could provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user **[75]**.

In a multimodal biometric system, fusion can be done at three different levels, the feature extraction level, fusion at the matching score level and the decision level **[07]**. Fusion at the feature extraction level combines different biometric features in the recognition process. Score fusion matches the individual scores of different recognition systems to obtain a multimodal score. Decision level systems perform logical operations upon the monomodal system decisions to reach a final resolution **[78]**. It has been however, reported that the most appropriate and effective approach to multimodal biometrics is through the fusion of data at the score level **[76]**. Because fusing scores at this stage allows a parallel development of each unibiometric system and offers a good trade-off between richness of information and ease of implementation.

Since the matching scores output by the different modalities are heterogeneous, score normalization **[07, 16]** is needed to transform these scores into a common domain, prior combining them. Fusing the scores without such normalization would de-emphasize the contribution of the matcher having a lower range of scores **[77].**

In this thesis, score normalization is used to convert the matching scores obtained from different traits into the same range by using Min-Max normalization process. Furthermore, the term score normalization is used in this thesis to enhance the scores obtained from the degraded modalities and reduce the effects of scores variations by introducing unconstraint cohort normalization (**UCN**) mechanisms into the normalized matching scores. It has been shown in **[01, 02, 18, 19]** that the accuracy of multimodal biometrics can be further enhanced if the scores from the individual modalities involved are first subjected to UCN process.

In recent years, a noticeable amount of research has been focused on biometric fusion. Many fusion techniques have been proposed in this field area of research. These techniques include, Logistic regression [72], K-nearest Neighbor **[72]**, Fuzzy Logic **[50, 73]**, Dempster-Shafer Theory **[40]**, neural network **[01, 71]**, Classification Tree **[13]**, Linear Discriminant Function **[13]**, Sum Rule **[13, 22, 61, 70]**, Support Vector Machine **[11, 17, 22]** Genetic Algorithms **[02]** and some simple combination techniques such as: Min Rule, Max Rule and Product Rule **[61, 70]**.

3. Aims and objectives

The primary goal of this thesis is to determine if multimodal biometrics provide any significant improvement in accuracy over its unimodal counterpart:

- This thesis presents investigations for enhancing the accuracy of multimodal biometric verification system, through the introduction of *Genetic Algorithm* (GA) and *Particle Swarm Optimization* (PSO) as two evolutionary techniques into the Score-Level fusion of face and voice modalities.
- In order to evaluate their performances, these two evolutionary techniques are conducted on publicly available datasets of scores (**XM2VTS**, **TIMIT**, **NIST** and **BANCA**) and under three different data quality conditions namely, clean varied and degraded.
- To highlight their strengths and weakness, these two evolutionary techniques are compared to three other fusion schemes, namely, a classical method such as *Brute Force Search* (BFS), a hybrid intelligent technique such as *Adaptive Neuro-Fuzzy Inference System* (ANFIS) and a statistical technique such as *Support Vector Machine* (SVM).
- While normalization setup is often necessary to map the individual matching scores into common range before combining them, for this purpose, the well-known *min-max* normalization technique is chosen in this study since they appear frequently in the literature and usually attained good performance.
- This thesis also addresses the problem of variations in biometric data by subjecting the scores into *Unconstrained Cohort Normalization* (UCN) process before combining them.

4. Thesis organization

The rest of the thesis is organized as follows:

- **Chapter 1** presents an overview on biometrics, describes the basic concepts of biometrics and motivation of multimodal biometrics. By the end of this chapter the principle of multimodal biometric fusion is illustrated, which is the field of the study of this thesis.
- **Chapter 2** considers the issue of performance evaluation in biometric systems, by presenting some state-of-the-art criteria and metrics used to evaluate the performance of a biometric verification system.

- **Chapter 3** explores some state-of-the-art fusion schemes and describes their principle in detail along with examples highlighting their application into the field of multimodal biometric score-level fusion. The chapter concludes by reviewing some recent researches carried out to date in the field area of multimodal biometric fusion.

- **Chapter 4** experimentally investigates the performance of the proposed techniques, interprets, and explains the main results obtained.

- The thesis concludes by summarizing the main findings obtained and suggesting some guidelines and recommendations for the future work.

Chapter

01

Biometrics and Multimodal Biometrics Systems

Abstract: *This Chapter presents an introduction to biometrics as an efficient tool for person recognition instead of traditional means such as password, ID cards …etc. this chapter then presents the limitations and constraints related to the use of unimodal biometrics systems that use only one single modality. To alleviate these limitations, this chapter proposes Multimodal Biometric systems that integrate the evidence offered by multiple biometrics sources. Finally, this chapter presents the advantages of multimodal biometric system over its unimodal counterpart, the fusion scenario and different level of fusion.*

Résumé : *Ce chapitre propose une introduction à la biométrie comme un outil efficace pour la reconnaissance de la personne au lieu des moyens traditionnel tels que les mots de passe, les cartes d'identité,…etc. Ce chapitre présente ensuite les problématiques et contraintes liées à l'utilisation de systèmes biométriques monomodales qui utilisent une seul modalité biométrique. Pour remédier à ces limitations, ce chapitre propose l'utilisation les systèmes biométriques multimodales qui intègrent l'évidence offerte par des sources biométriques multiples. Finalement, ce chapitre les avantages du système biométrique multimodale, les scénarios de fusion et les différents niveaux de la fusion.*

1.1 Introduction

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person. Biometrics is used more and more in applications of the everyday life. So with its beginnings at the end of the 19th century the biometric data were treated manually, today, with the data processing, the biometric systems are automated **[08]**.

In this Chapter, we will introduce biometrics and its use for the identity verification. We will present then the general structure of a biometric system and we will indicate the limitations of the biometric systems which use only one modality. Finally, as a solution to these limitations, we will present the use of multimodal biometric systems which is the field of the study of this thesis.

1.2 Identity verification using a biometric system

The identity is a philosophical concept related to the spirit and the personality of each individual. The identity is defined with its birth by a name and personal data (date and birthplace, family, residence, social security number…) and it is verified more and more during the life of an individual. In order to make safe the transactions and trips, each person needs to declare his identity and let it to be verified on many occasions (borders, bank account, and access to reserved places…) **[08]**. Biometrics is the most complete means of identification, because it joins an identity to a natural person by means of his physiological or behavioral characteristics.

1.2.1 The identity verification

Security applications require a user authentication. This identity verification was done until now with the identification means related to something which one knows (what you know), such as a passwords and other codes, or which one has (what you possess), such as an ID card and other identity documents as it is shown in Figure 1.1. Most of the applications combine these two means of identification as it is the case for the purchasing cards, where we must at the same time have the card but also know the code to be able to use it.

But these authentication means create some problems, because they can be lost, stolen or reproduced an also you need to remember multiple passwords and maintain multiple authentication tokens.

On the other hand, with the biometric data it would be possible to make sure if this person does not have already another identity by comparing her biometric data with the whole of the data stored in the database. Hence biometrics is the efficient means of remedying the various problems arising from the traditional authentication means and enhancing the security level **[08]**.

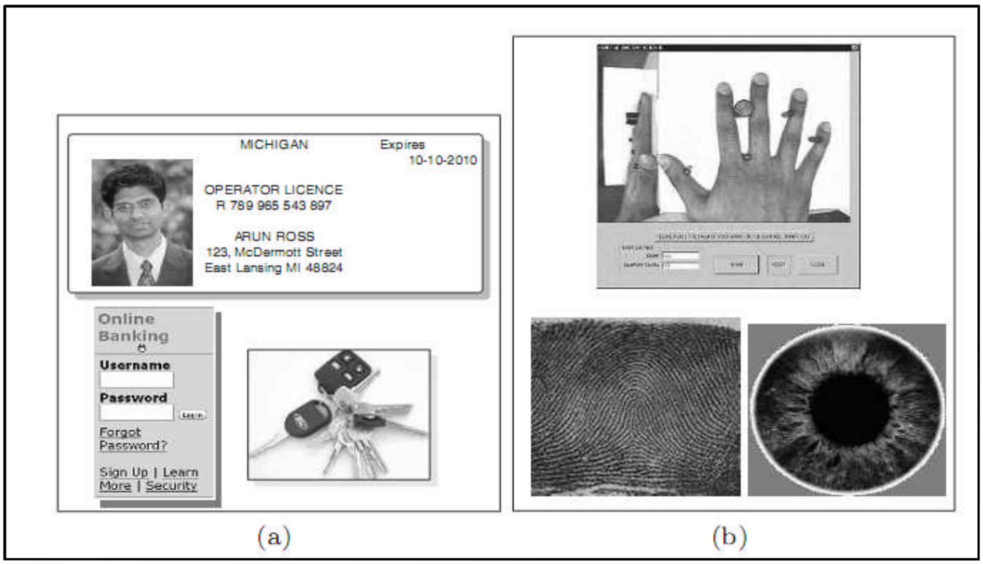


Figure 1.1: Authentication schemes,

(a) Traditional schemes use ID cards, passwords and keys.

(b) Establish an identity based on "who you are" rather than by "what you possess" or "what you remember" **[10]**.

1.2.2 Biometrics

Biometrics is the science of establishing the identity of a person based on '**Who you are**' refers to his physiological characteristics such as fingerprints, iris, or face. And '**What you produce**' refers to his behavioral patterns that characterize your identity such as the voice or the signature **[05]**. These physiological or behavioral characteristics are called biometric modalities. Biometrics such as we wants to use it today in the security systems aims to make an automatic recognition **[08]**.

The importance of biometrics in our society has been reinforced by the need for large-scale identity management systems whose functionality relies on the reliable determination of an individual's identity in the context of several different applications. Examples of these applications include **[04]**:

- Sharing networked computer resources.
- Granting access to nuclear facilities.
- Performing remote financial transactions.
- Boarding a commercial flight.
- Web-based services (e.g., online banking).
- Customer service centers (e.g., credit cards).
- …etc.

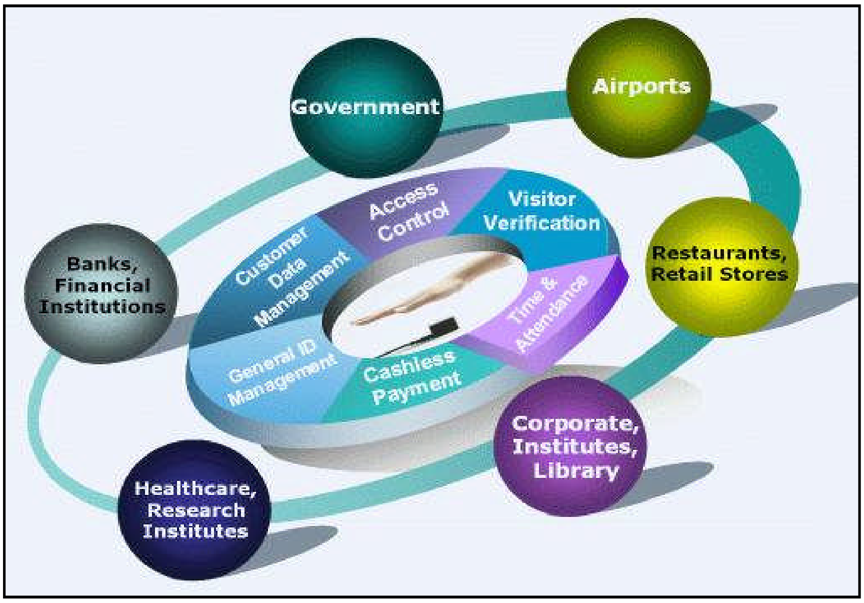


Figure 1.2: Some biometrics applications.

1.2.3 Biometric characteristics

The choice of a biometric trait for a particular application depends on a variety of issues besides its matching performance and accuracy. In theory, any human characteristic (physiological or behavioral) can be used as a biometric identifier as long as it satisfies these requirements **[25]**:

- **Universality**: Every person in the population should posses the biometric modality.
- **Distinctiveness**: The given modality should be sufficiently different across individuals comprising the population, it's also known as uniqueness **[04]**.
- **Permanence**: The biometric trait should be sufficiently invariant over a period of time with respect to the matching algorithm.
- **Collectability:** The ability to measure the biometric quantitatively, in other words, it should be possible to acquire and digitize the biometric traits using suitable devices that do not cause undue troubles to the individual.

Other criteria required for practical applications include:

- **Performance**: The efficiency, accuracy, speed, robustness and resource requirements of particular applications based on the biometric.
- **Acceptability**: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
- **Circumvention**: The ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers, in the case of physical traits, and mimicry, in the case of behavioral traits).

The biometric modalities do not have all these properties, or at least have them with different degrees. No biometrics is thus perfect or ideal, but is more or less adapted to applications. The compromise between presence or absence of some of these properties is done according to each application requirements, in the choice of the biometric method.

1.2.4 Biometric Modalities

Different biometric modalities have been proposed and used in various applications. Physiological biometrics includes the ear, face, hand geometry, iris, retina, palmprint and fingerprint. Behavioral biometrics includes voice, signature, gait or keystroking [**05]**. Examples of these traits are shown in the following sections:

1.2.4.1 Facial recognition

Facial recognition is usually thought of as the primary way in which people recognize one another. The most popular approaches to face recognition are based on either **[04]**:

- The location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships.
- The overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces.

In practice, a reliable facial recognition system should automatically:

- Detect whether a face is present in the acquired image.
- Locate the face if there is one.
- Recognize the face from a general any pose and under different ambient conditions.

Figure 1.3: Face Modality.

1.2.4.2 Voice verification

Voice is a combination of physical and behavioral biometric characteristics. The voice authentication process is based on the extraction and modeling of specific features from speech **[12]**. These physical features of an individual's voice are based on the shape and size of the vocal tracts, mouth, nasal cavities, and lips that are used in the synthesis of the sound**.**

The physical characteristics of human voice are invariant for an individual, but the behavioral aspect of the speech changes over time due to age, medical conditions (such as common cold), emotional state, etc. The major disadvantage of voice-based recognition system is that speech features are sensitive to many factors such as background noise **[04]**.

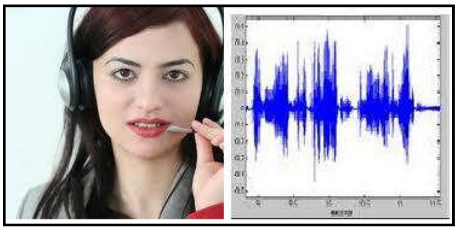


Figure 1.4: Voice Modality.

1.2.4.3 Fingerprint recognition

Humans have used fingerprints for personal identification for many decades. Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations **[25]**.

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of fetal development. It has been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person **[04]**. One main shortcoming for fingerprint identification systems is that small injuries and burns highly affect the fingerprint **[12]**.

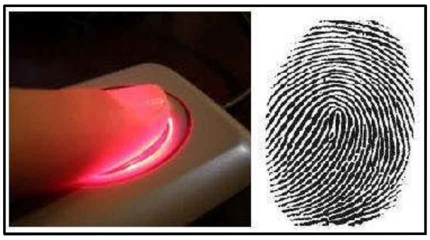


Figure 1.5: Fingerprint Modality.

1.2.4.4 Hand geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and the lengths and widths of the fingers **[10]**. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not affect the authentication accuracy of hand geometry-based systems.

However, the geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population **[04]**.

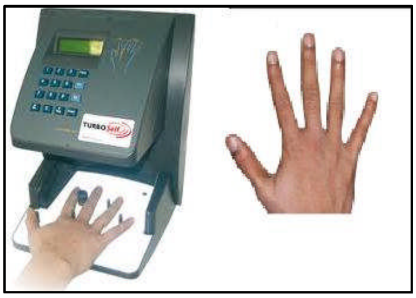


Figure 1.6: Hand geometry Modality.

1.2.4.5 Iris recognition

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The complex iris texture carries very distinctive information useful for personal recognition. Each iris is distinctive and even the irises of identical twins are different **[10]**.

Iris-based systems have the lowest false match rates among all currently available biometric methods, and are the least intrusive technique of the eye-based biometrics. It is one of the few biometric systems, besides fingerprinting, that works well in “identification” (one-to-many comparison) mode **[48]**.

Figure 1.7: Iris Modality.

1.2.4.6 Keystroke dynamics

Keystroke dynamics is another early technique in which a great deal of time and effort was invested, including by some major information technology companies **[49]**.

Keystroke dynamics, or analysis, is also referred to as typing rhythms. It is an automated method of analyzing the way a user types at a terminal or keyboard, examining dynamics such as speed, pressure, total time taken to type particular words, and the time elapsed between hitting certain keys. Specifically, keystroke analysis measures two distinct variables: “dwell time,” which is the amount of time a person holds down a particular key, and “flight time,” which is the amount of time it takes between keys.

This technique works by monitoring the keyboard inputs at thousands of times per second in an attempt to identify the user by his/her habitual typing rhythm patterns **[48]**.

1.2.4.7 Signature

The personal signature is has been accepted in government, legal, and commercial transactions as a method of authentication. Due to the PDAs and Tablet PCs, on-line signature may emerge as the biometric of choice in these devices. Signature is a behavioral biometric that changes over a period of time and is influenced by the physical and emotional conditions of the signatories **[04]**.

Figure 1.8: Signature Modality.

1.2.4.8 Gait recognition

Gait is the manner in which a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Most gait recognition algorithms attempt to extract the human silhouette in order to derive the spatio-temporal attributes of a moving individual. Some algorithms use the optic flow associated with a set of dynamically extracted moving points on the human body to describe the gait of an individual **[25]**.

However, the gait of an individual is affected by several factors including the choice of footwear, nature of clothing, affliction of the legs, walking surface, etc.

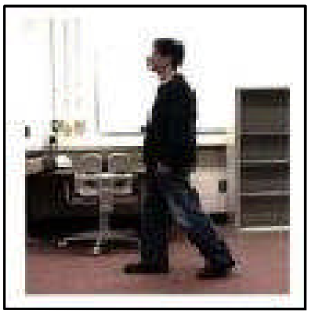


Figure 1.9: Gait Modality.

1.2.4.9 Retina scanning

Research conducted in the 1930s suggested that the patterns of blood vessels in the back of the human eye were unique to each individual, making retinal scan one of the oldest known biometrics **[48]**.

The retina is a thin layer of cells at the back of the eyeball of vertebrates. It is the part of the eye which converts light into nervous signals.

The principle of retina biometrics captures and analyzes the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil. These blood vessels have a unique pattern, from eye to eye and person to person.

Retinal patterns are highly distinctive traits. Every eye has its own totally unique pattern of blood vessels; even the eyes of identical twins are distinct **[48]**. Although each pattern normally remains stable over a person's lifetime, it can be affected by disease such as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome.

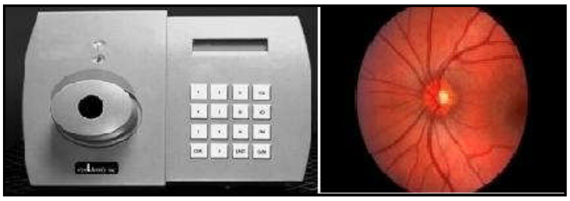


Figure 1.10: Retina Modality.

1.2.5 The structure of a biometric system

A biometric system is a pattern recognition system, which acquires the 'individual biometric data , extracts some features from this data , compares it against one or the whole stored in the database, and it take a decision based on the comparison results, so, a biometric system function according to the following stages **[31]**:

- **Enrollment:** In order to access to the biometric system, the user has to be registered. In this stage, we assign an ID, and capture an image of the specific biometric trait. This image is then converted to a template (after the feature extraction process).
- **Storage:** In this stage, the biometric template is stored on a database, an individual workstation or portables devices for the future comparison (authentication).
- **Matching:** When the user (already enrolled in the database) tries to access the system for the verification or identification task, he will introduce another biometric sample, which is converted into a template and is then compared to the

stored template. Then, according to the final decision taken by the biometric system, the user is then accepted as client, or rejected as an impostor.

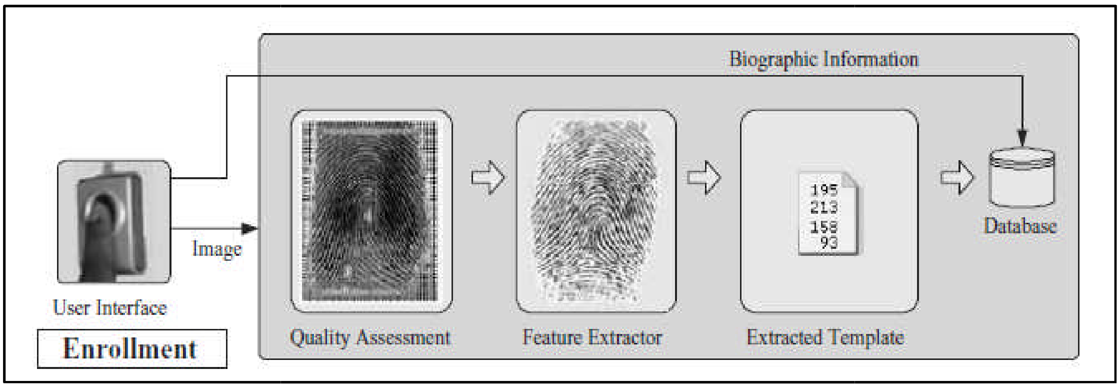


Figure 1.11: Biometric Enrollment.

1.2.6 Verification versus identification

There are several types of application which require the user's authentication. Depending on the application context, these applications can be separated into two categories which are the identity verification or identification.

1.2.6.1 Verification

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. Generally, it is usually associated with the means of traditional identification such as a smart card, a badge or a key, and is used as an additional security to ensure that the card or the badge was not stolen or is not used by a not authorized person. The verification is a YES or NO decision type with the question: “the individual is he well that which he claims to be? “**[08].** the system conducts a **one-to-one** comparison to determine whether the claim is true or not. Verification is typically used for positive recognition, to prevent multiple people from using the same identity **[04]**.

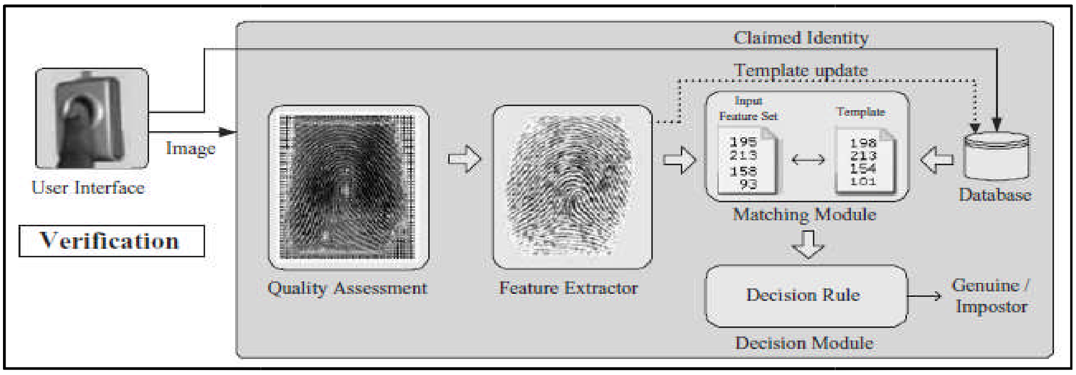


Figure 1.12: Biometric Verification.

1.2.6.2 Identification

In the identification mode, to recognize an individual the biometric system search in the templates of all the users in the database for a match. Therefore, the system conducts a **one-to-many** comparison to establish an individual's identity ("Whose biometric data is this?"). Identification can be used for the negative recognition to prevent a single person from using multiple identities **[04]**. The identification can be used to authorize the use of the services, such as controlling the access to a protected zone for which only a restricted number of people (saved in a database) have the access authorization **[08]**.

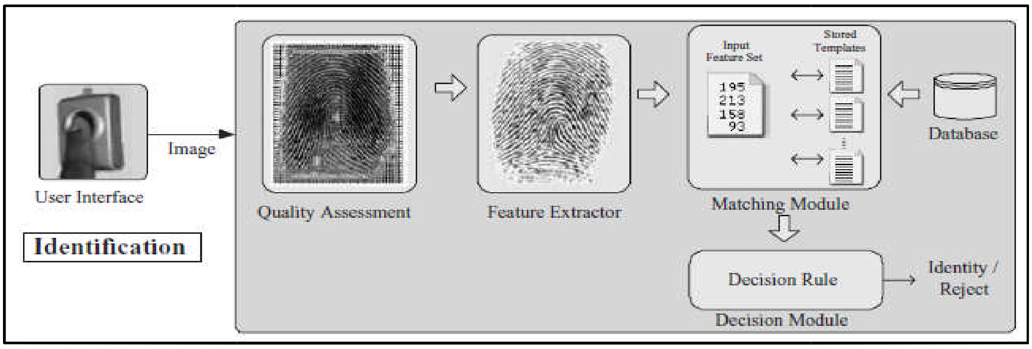


Figure 1.13: Biometric Identification.

1.2.7 Limitations of unimodal biometric systems

Unimodal biometric system establishes a physical link between a person and her identity, and it offers a reliable solution for a secured verification. However, the biometric systems suffer from certain limitations, and the performance of a biometric system employing a single trait is constrained by these intrinsic factors **[03]**:

- **Noise in sensed data:** Noise in the sensed data may result from defective or improperly maintained sensor. Ex. fingerprint image with scar, voice sample altered by cold etc.
- **Intra-class variation:** Caused by an individual who is incorrectly interacting with sensor and this will increase False Reject Rate (FRR).
- **Intra-class similarities:** Refers to overlapping of feature spaces corresponding to multiple classes or individuals. This may increase the False Acceptance Rate (FAR).
- **Non-universality:** Biometric system may not able to acquire meaningful biometric data from a subset of users.
- **Spoof attacks:** Involves the deliberate manipulation of one’s biometric traits in order to avoid recognition. This type of attack is relevant when behavior traits are use.

1.3 Multimodal biometric systems

Biometric authentication systems that used only one biometric trait may not accomplish the requirements of demanding applications in terms of the characteristics described before (section 1.2.3), and the limitations of a unimodal biometric system can be addressed by designing a system that integrates (fuse) biometric information from multiple sources, for example, multiple traits of the same individual, such systems, known as multimodal biometric systems **[28]**.

Multimodal biometric system is expected to be more robust to noise, address the problem of non-universality, improve the matching accuracy, and provide reasonable protection against spoof attacks **[07]**.

1.3.1 Advantages of multimodal biometric systems

Besides enhancing matching accuracy, the other advantages of multibiometric systems over unimodal biometric systems are enumerated below **[10]**.

(a) Non-universality: Multimodal biometric systems address the problem of non-universality encountered by unimodal biometric systems. One example, if a subject’s dry or cut finger prevents her from successfully enrolling into a fingerprint system, then the availability of another biometric trait, say iris, can be used in the inclusion of the individual in the biometric system.

(b) **Indexing large-scale biometric databases:** Multimodal biometric systems can facilitate the filtering or indexing of large-scale biometric databases. For example, in a bimodal system consisting of face and fingerprint, the face feature set may be used to compute an index value for extracting a candidate list of potential identities from a large database of subjects. The fingerprint modality can then determine the final identity from this limited candidate list.

(c) **Spoof attacks:** It becomes increasingly difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual.

(d) **Noise in sensed data:** Multibiometric systems also effectively address the problem of noisy data. When the biometric signal acquired from a single trait is corrupted with noise, the availability of other (less noisy) traits may aid in the reliable determination of identity. Some systems take into account the quality of the individual biometric signals during the fusion process. This is especially important when recognition has to take place in adverse conditions where certain biometric traits cannot be reliably extracted. For example, in the presence of ambient acoustic noise, when an individual's voice characteristics cannot be accurately measured, the facial characteristics may be used by the multibiometric system to perform authentication.

(e) **Fault tolerance:** A multimodal biometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems involving a large number of subjects (such as a border control application).

1.3.2 Fusion scenarios

What are the sources of information that can be considered in a multimodal biometric system? We address this question by introducing some terminology to describe the various scenarios that are possible to obtain multiple sources of evidence (Figure 1.14). In the first four scenarios described below, information fusion is accomplished using a single trait, while in the fifth scenario multiple traits are used.

1.3.2.1 Multiple Sensors

A single biometric trait is captured using two or more sensors. For example an infrared sensor may be used in conjunction with a visible-light sensor to acquire the subsurface information of a person’s face.

1.3.2.2 Multiple algorithms

A single biometric input is processed with different feature extraction algorithms in order to create templates with different information content. One example is processing fingerprint images according to minutiae- and texture-based representations.

1.3.2.3 Multiple instances

A single biometric modality but multiple parts of the human body are used, and are also referred to as multi-unit systems in the literature. One example is the use of multiple fingers in fingerprint verification.

1.3.2.4 Multi-sample systems

A single sensor may be used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait. One example is the sequential use of multiple impressions of the same finger in fingerprint verification. Similarly, a face system, for example, may capture (and store) the frontal profile of a person's face along with the left and right profiles in order to account for variations in the facial pose.

1.3.2.5 Multiple modalities

Multiple biometric modalities are combined. This is also known as multimodal biometrics. These systems combine the evidence presented by different body traits for establishing identity. For example, some of the earliest multimodal biometric systems utilized face and voice scores to improve the identity verification of an individual **[10]**.

Besides the above mentioned scenarios, it is also possible to use biometric traits in conjunction with non-biometric identity tokens in order to enhance the authentication performance.

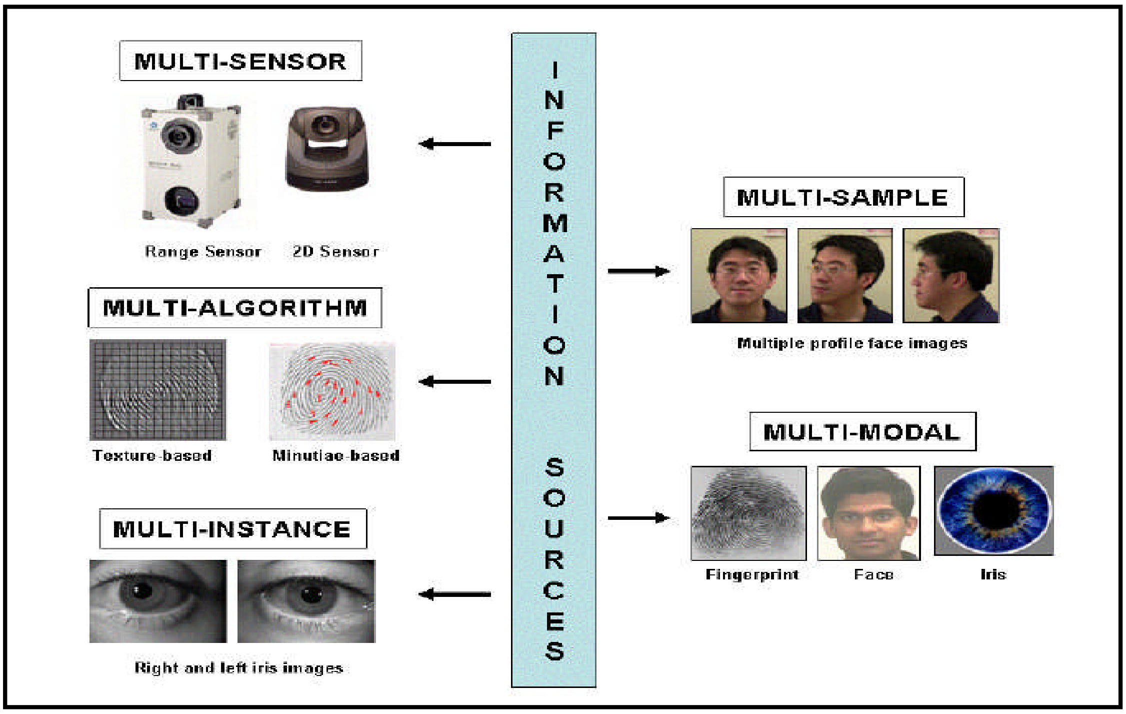


Figure 1.14: Fusion scenarios in multimodal biometric.

1.3.3 Different levels of fusion

Biometric system has four important modules. The sensor module acquires the biometric data from a user via sensors; the feature extraction module processes the acquired biometric data and extracts a feature set to represent it; the matching module compares the extracted feature set with the stored templates using a classifier or matching algorithm in order to generate matching scores; in the decision module the matching scores are used either to identify an enrolled user or verify a user's identity **[07]**.

In a multibiometric system, fusion can be accomplished by utilizing the information available in any of these modules. Thus, four different levels of fusion are possible: the sensor level, the features extraction level, the matching score level, and the decision level (Figure 1.14). Sanderson et al. **[29]** have classified information fusion in biometric systems into two broad categories: pre-classification fusion and post-classification fusion. The sensor level and the features extraction level are referred to as pre-classification fusion while the matching score level and the decision level are referred to as post-classification fusion.

1.3.3.1 Pre-Classification fusion

Pre-classification fusion refers to combining information prior to the application of any classifier or matching algorithm. This integration can take place either at the sensor level or at the feature level.

1.3.3.1.1 Sensor Level

The raw data, acquired from sensing the same biometric characteristic with two or more sensors, is combined. Sensor level fusion is applicable only if the multiple sources represent samples of the same biometric trait obtained either using a single sensor or different compatible sensors **[10]**.

1.3.3.1.2 Feature Extraction Level

This level refers to combining different feature sets extracted from multiple biometric sources. When the feature sets are homogeneous (e.g., multiple measurements of a person's hand geometry), a single resultant feature vector can be calculated as a weighted average of the individual feature vectors. When the feature sets are non-homogeneous (e.g., features of different biometric modalities like face and hand geometry), we can concatenate them to form a single feature vector. Concatenation is not possible when the feature sets are incompatible (e.g., fingerprint minutiae and eigen-face coefficients) **[10]**.

1.3.3.2 Post-Classification fusion

In the post-classification fusion the information is combined after the decisions of the classifiers have been obtained. This integration can take place either at the matching score level or at the decision level.

1.3.3.2.1 Matching Score Level

When each biometric system outputs a match score indicating the proximity of the input data to a template, integration can be done at the match score level. This is also known as fusion at the measurement level or confidence level.

The match scores output by biometric matchers contain the richest information about the input pattern. Also, it is relatively easy to access and combine the scores generated by the different matchers. Consequently, integration of information at the match score level is the most common approach in multimodal biometric systems **[04]**.

1.3.3.2.2 Decision Level

Integration of information at the abstract or decision level can take place when each biometric system independently makes a decision about the identity of the user (in an identification system) or determines if the claimed identity is true or not (in a verification system).

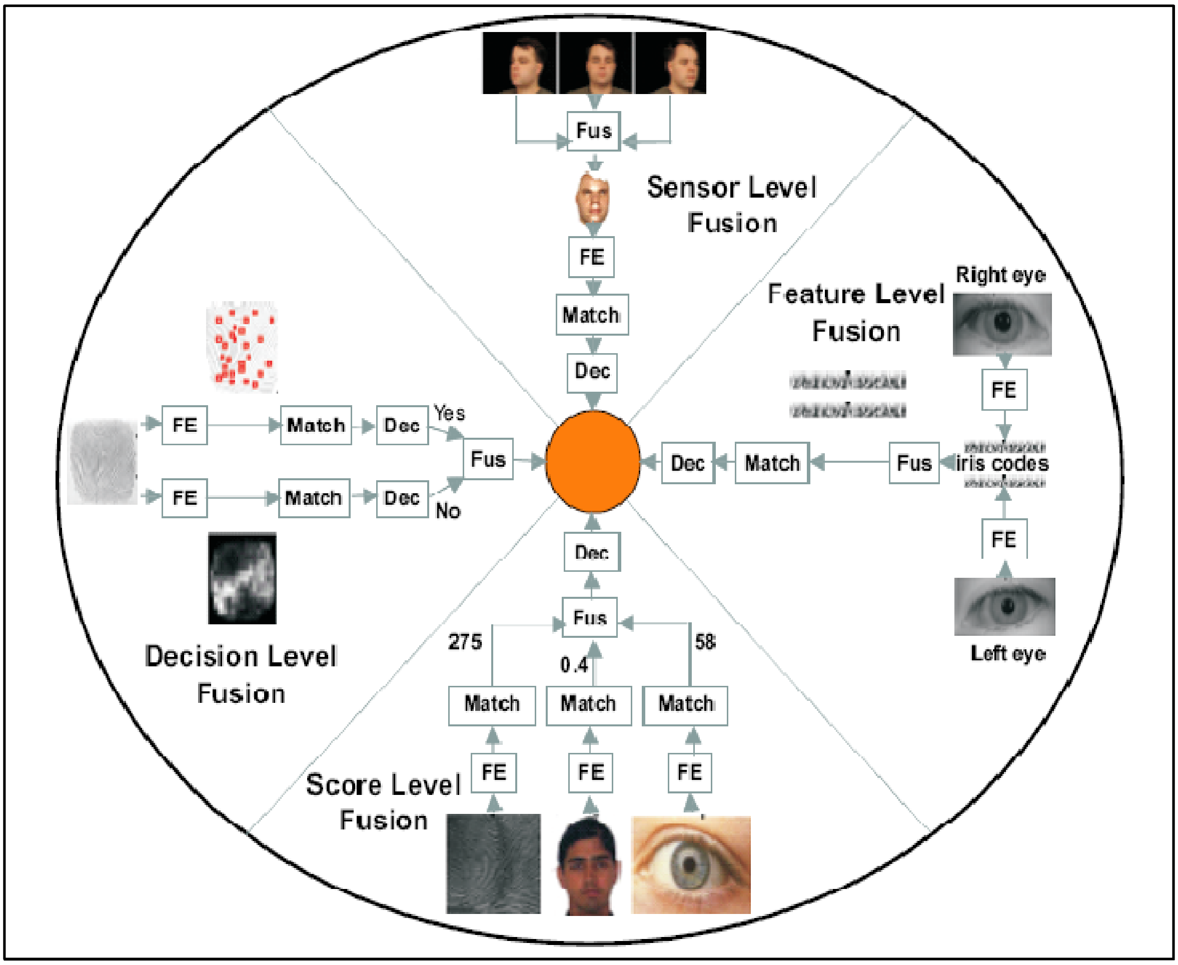


Figure 1.15: Fusion levels in multimodal biometrics.

It is difficult to combine information at the feature level because the feature sets used by different biometric modalities may either be inaccessible or incompatible. Fusion at the decision level is too rigid since limited amount of information is presented at this level. Therefore, integration at the matching score level is generally preferred due to the ease in accessing and combining the scores generated by different matchers, also fusing information at this level is interesting because it reduces the complexity by allowing different classifiers to be used independently of each other .

1.4 Conclusion and Summary

In this first Chapter, we have presented the field of the study of this thesis: biometrics and multimodal biometrics. We have briefly introduced some aspects of biometrics, including, its definition, characteristics and some biometric modalities that can be used for the identity verification. We have defined the structure of the biometric systems and presented some limitations of these systems when they use only one biometric modality. Then we have presented a way to reduce the limitations of the unimodal biometric systems while combining several biometric traits, thus leading to multimodal biometrics. The various sources of biometric information that can be fused as well as the different levels of fusion that are possible have been already discussed. Since the main goal of this study is evaluating and comparing the effectiveness of multimodal biometric fusion technique involved, the next chapter will present some state-of-the-art performance evaluation criteria and metrics used in this dissertation.

Chapter

02

Performance evaluation of a biometric system

Abstract: *This Chapter presents some state-of-the-art tools and metrics used to evaluate the performance of biometric systems. This chapter presents three different types of performance evaluation namely, technological evaluation, the evaluation of the scenario and operational evaluation. In this chapter, only the last one will be discussed and illustrated. For the operational evaluation, this chapter gives an overview on six metrics used in the literature to evaluate and compare the performances of biometric systems. These metrics include three error rates (FAR, FRR and EER) and three curves (ROC, DET and FAR vs FRR). The error rates are considered as operating points necessary to define a decision threshold, this latter will be then used by the system to decide if the claimed person should be rejected or accepted. The curves are used to visualize and directly compare the performance of unimodal or multimodal biometric systems. Finally, this chapter presents how typically two or more biometric systems could be compared in terms of performances.*

Résumé : *Ce chapitre présente quelques outils utilisés dans la littérature pour l'évaluation des performances d'un system biométrique. Ce chapitre présente trois différents type d'évaluation des performances, notamment l'évaluation technologique, l'évaluation du scénario et l'évaluation opérationnelle. Dans ce chapitre, seule le dernière type sera discuté et illustrée. Pour l'évaluation opérationnelle, ce chapitre donne un aperçu sur les six critères utilisés dans la littérature pour évaluer et comparer les performances des systèmes biométriques. Ces critères comprennent trois taux d'erreur (FAR, FRR and EER) et trois courbes (ROC, DET and FAR vs FRR). Les taux d'erreur sont considérés comme des points de fonctionnement nécessaires pour définir un seuil de décision qui sera par suite utilisé par le système pour décider si la personne réclamée doit être rejetée ou acceptée. Les courbes sont utilisées pour visualiser et directement comparer la performance des systèmes biométriques monomodales ou multimodales. Enfin, ce chapitre présente la façon dont deux ou plusieurs systèmes biométriques pourraient être comparés en termes de performances.*

2.1 Introduction

As we saw in the previous chapter, biometric systems, either monomodal (single biometric modality) or multimodal (A combination of biometric modalities) are intended to be used in many applications. To consider the deployment of these systems in everyday life, these systems need to be evaluated to estimate their performance in real use. According to the application specificity, three types of evaluation were differentiated in **[42]** to estimate the performance of a biometric system: technological evaluation, the evaluation of scenario and operational evaluation. The first one test the performance of algorithmic parts of the system (features extraction, comparison and decision) using a publicly available database (benchmark). The evaluation of scenario tests a more complete system also including the sensors, the environment and the population specific to the application (scenario) tested. The operational evaluation tests the biometric system in the real conditions of use.

In this chapter, we will present some state-of-the-art criteria and methods used to evaluate the performance of a biometric verification system, in terms of values and performance curves.

2.2 The performance evaluation

As mentioned before, there are three different types of performance evaluation, but in our study we will concentrate on the most common one which is known as “technological” evaluation of the biometric and multimodal biometric systems, i.e., an evaluation of their error rates for the identity verification. There are some of the biometric systems errors that cannot be treated because they depend on the acquisition module. These errors are impossibilities of acquisition “failure to enroll” or “failure to acquire” by the sensor of the biometric data **[08]**.

2.2.1 Error Rates

For the evaluation of the “algorithmic” part of the multimodal biometric system two types of error can be detected **[08]**:

- **Impossibility of comparison** (depends on the extraction module or comparison Module): This type of error is due to the module of treatment (extraction and comparison) which contains in general a quality control part. If the system is unable to provide a comparison score, then we talk about impossibility of comparison “failure to match”.

- **Classification errors** (depends on the decision module and thus on the decision threshold): There is two types of classification errors corresponding to the decisions for the two classes (Client and Impostor) measured in different manner. They result from the none exact correspondence between two biometric samples of a person and thus make it possible to evaluate the level of the decision accuracy of the system. These errors of classification are the only ones which will be really measured in the performances estimation (in terms of error rate) of a biometric system on a multimodal database.

A fully operational biometric system makes a decision using the following decision function **[06]**:

$$\boldsymbol{Decision}(\boldsymbol{x}) = \begin{cases} \boldsymbol{accept} & \boldsymbol{if}\ \boldsymbol{y}(\boldsymbol{x}) > \boldsymbol{\eta} \\ \boldsymbol{reject} & \boldsymbol{otherwise} \end{cases} \qquad (\mathbf{2.1})$$

where $\boldsymbol{\eta}$ is the decision threshold and **y(*x*)** is the output of the underlying expert system supporting the hypothesis that the biometric sample $\boldsymbol{x}$ belongs to a client. Because of the accept-reject outcomes, the system may make two types of errors, false acceptance (**FA**) and false rejection (**FR**). So, biometric authentication can be considered as a detection task, involving a trade-off between these two types of errors **[05]**.

- **False acceptance (FA):** Taking place when an unauthorized or impostor user is accepted as being a true user.
- **False rejection (FR):** Occurring when a client, target, genuine, or authorized user is rejected by the system.

The normalized versions of FA and FR are often used and called False Acceptance Rate (**FAR**) and False Rejection Rate (**FRR**) respectively.

- **False Acceptance Rate (FAR**): The number of False Acceptance accesses divided by the total number of Imposters ***(NI)*** in the test database.
- **False Rejection Rate (FRR**): The number of False Rejection accesses divided by the total number of Clients ***(NC)*** in the test database.

The decision error rates of the multimodal biometric verification systems (FAR and FRR) are dependent on the decision threshold **(** $\boldsymbol{\eta}$ **)** and are given according to the threshold by**:**

$$FAR(\eta) = \frac{FA(\eta)}{NI} \tag{2.2}$$

$$FRR(\eta) = \frac{FR(\eta)}{NC} \tag{2.3}$$

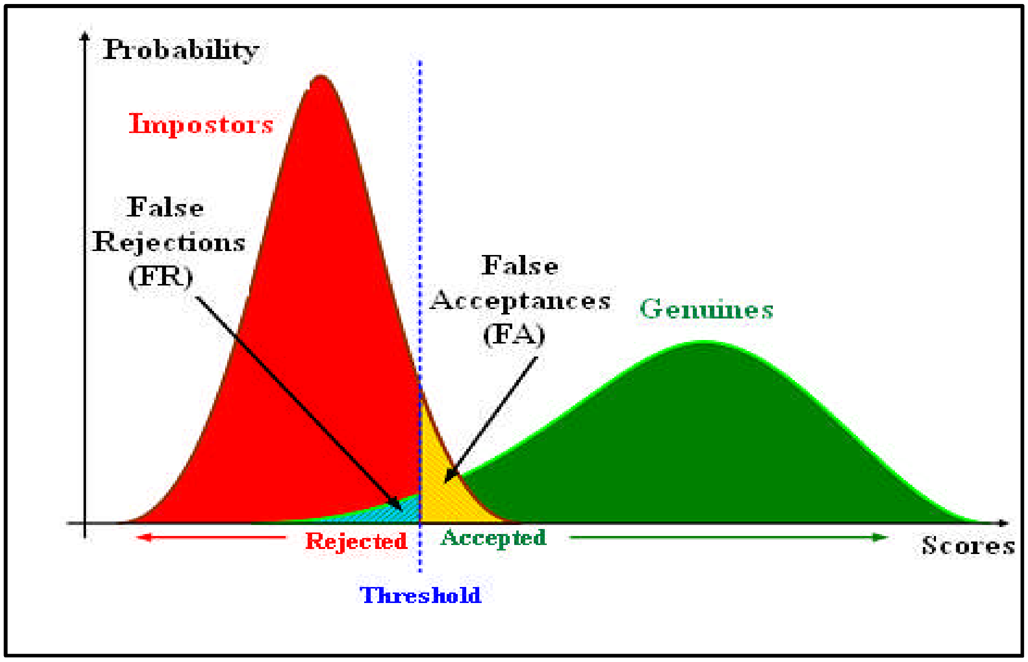


Figure 2.1: Illustration of the FRR and the FAR.

Some applications require a very low FAR (Identity verification), while some others do not tolerate in a high FRR (identification on a personal computer). For these reasons, we often calculate the performance of the biometric authentication system at several operating points (see Section 2.3). Therefore we often calculate the performances of the systems at several operating points, in order to be able to know the performances of the system for each type of application.

2.2.2 Threshold criterion

In the applications using the biometric identity verification system, one of the important parameters to regulate is the decision threshold. This threshold will depend on the type of application and the desired performances.

To choose an optimal threshold, a threshold criterion is needed. A threshold criterion refers to a strategy to choose a threshold to be applied on an evaluation (test) set. It is necessarily tuned on a development (training) set **[47]**.

It was argued **[48]** that the threshold should be chosen a priori as well, based on a given criterion. This is because when a biometric system is operational, the threshold parameter has to be fixed a priori **[06]**.

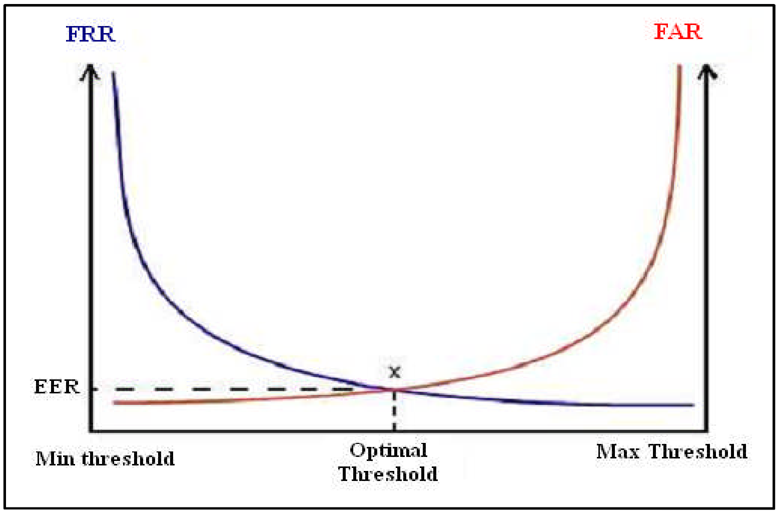


Figure 2.2: Illustration of The EER point and the optimal Threshold.

2.2.3 Performance curves

The performance curves are used to represent and visualize the performances of the biometric or multimodal biometric verification systems with respect to the whole range of possible threshold values **[45].**

2.2.3.1 FAR vs FRR curve

This curve, sometimes called the Equal Error Graph, is the most often used by researchers trying to understand the performance of their Verification system. It shows the evolution of both error rates (FAR and FRR) at all thresholds (Figure 2.3). Minimizing the area under the Crossover of the two plots is generally the goal of the researcher.

The user of a Verification System uses this curve to calculate where to set their operating threshold. The graph will show the expected FAR and FRR at any chosen threshold **[46]**.

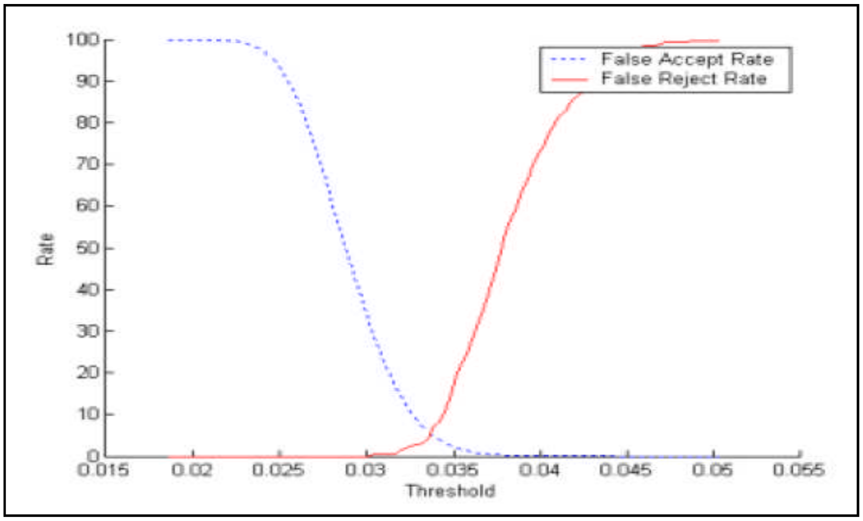


Figure 2.3: FAR vs FRR Curve.

2.2.3.2 Receiver Operating Characteristic (ROC) curve

ROC curves are a method for summarizing the performance of imperfect diagnostic, detection, and pattern matching systems. An ROC curve plots (parametrically as a function of the decision threshold) the rate of "false positives" (i.e. impostor attempts accepted) on the x-axis, against the corresponding rate of "true positives" (i.e. genuine attempts accepted) on the y-axis. ROC curves are threshold independent, allowing performance comparison of different systems under similar conditions, or of a single system under differing conditions **[33]**.

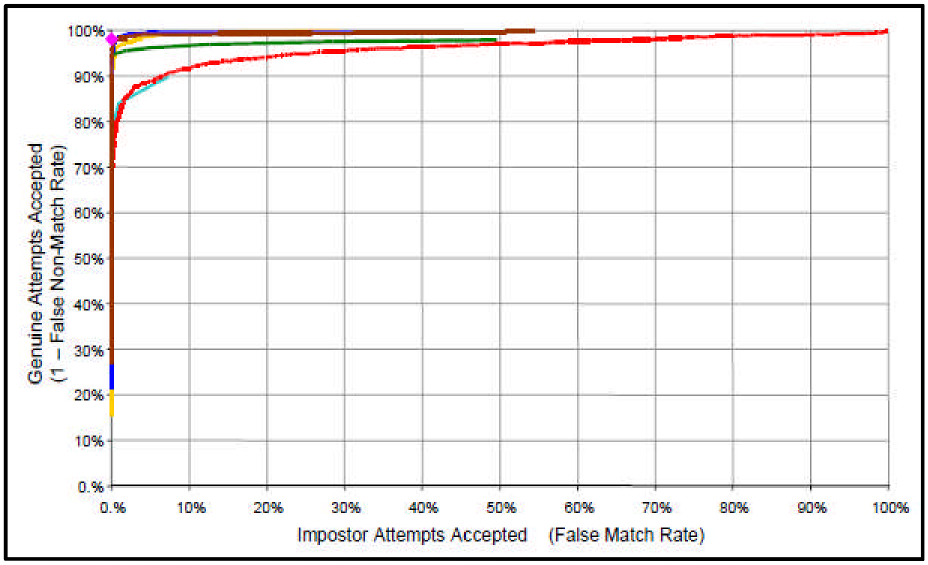


Figure 2.4: ROC curves.

2.2.3.3 Detection Error Trade-off (DET) curve

In the case, a modified ROC curve known as a “detection error trade-off” curve **[46]** is preferred. A DET curve plots error rates on both axes, giving uniform treatment to both types of error. The graph can then be plotted using logarithmic axes. This spreads out the plot and distinguishes different well-performing systems more clearly. For example the DET curve in Figure2.5 uses the same data as the ROC curve in Figure 2.4. DET curves can be used to plot matching error rates, false non-match rate (FRR) against false match rate (FAR) **[33]**.

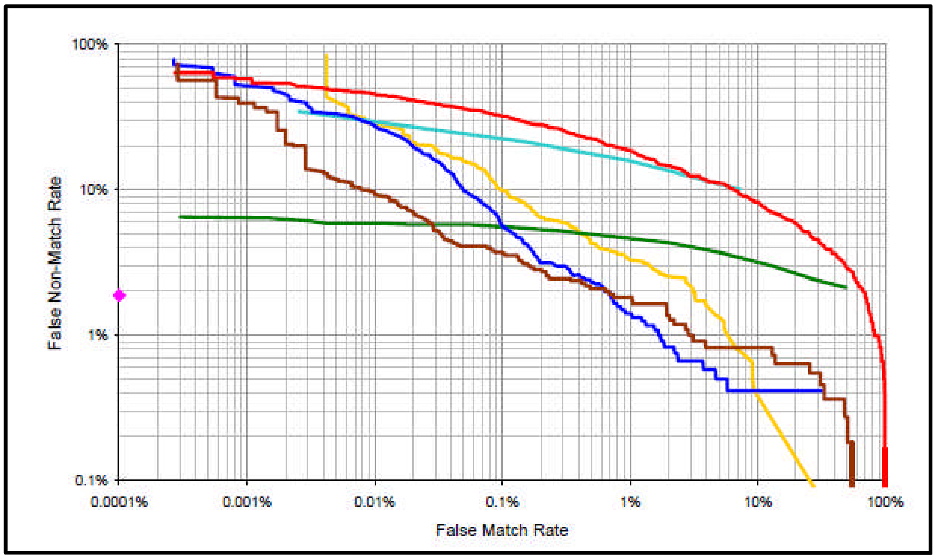


Figure 2.5: DET curves.

2.2.4 Operating Points

For the applications, we must fix a threshold at which we take the decisions of accepting or rejecting the identity claimed. This corresponds to choosing an operating point of the system. The mostly used operating point is Equal Error Rate (EER).

2.2.4.1 Equal Error Rate (EER)

This operating point corresponds to the threshold **η** where **FAR(η) = FRR(η)**. In practice, the scores distributions are not continuous and a crossover point might not exist. In this case (Figure. 2(b),(c)), the EER value is computed as follows **[43]** :

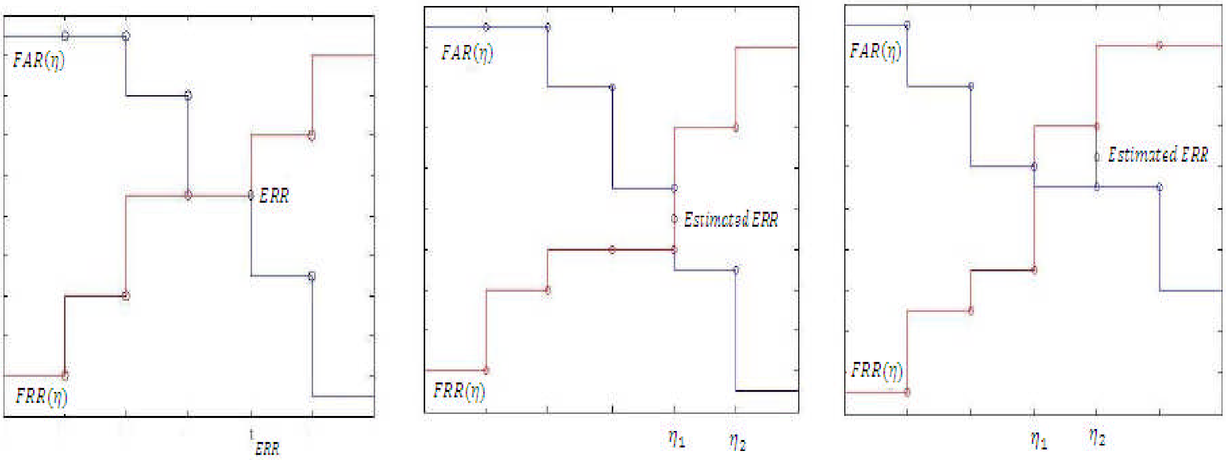
$$\boldsymbol{EER = \begin{cases} \frac{FAR(\eta_1)+FRR(\eta_1)}{2} & \text{if } FAR(\eta_1) - FRR(\eta_1) \leq \ FAR(\eta_2) - FRR(\eta_2) \\ \frac{FAR(\eta_2)+FRR(\eta_2)}{2} & otherwise \end{cases}} \quad \textbf{(2.4)}$$

where

$$\boldsymbol{\eta_1} = \mathbf{max}_{\eta\in S}\{\boldsymbol{\eta}/\boldsymbol{FRR}(\boldsymbol{\eta}) \le \boldsymbol{FAR}(\boldsymbol{\eta})\} \qquad (\mathbf{2.5})$$

$$\boldsymbol{\eta_2} = \min_{\boldsymbol{\eta}\in \boldsymbol{S}}\{\boldsymbol{\eta}/\boldsymbol{FRR}(\boldsymbol{\eta}) \ge \boldsymbol{FAR}(\boldsymbol{\eta})\} \qquad (\mathbf{2.6})$$

and **S** is the set of thresholds used to calculate the score distributions.



(a) EER point exists (b) EER is estimated at η_1 (c) EER is estimated at η_2

Figure 2.6: FAR vs FRR curve: (a) example where EER point exists. (b), (c) examples where EER point does not exist (estimated).

2.2.4.2 Weighted Error Rate (WER)

This operating point corresponds to the threshold where the FRR is proportional to the FAR with a coefficient that depends on the application. The threshold of WER is equal to the threshold of the EER when the coefficient is equal to one.

2.2.4.3 Fixed FAR

This operating point corresponds to the threshold where FAR is equal to a rate fixed by the application (e.g. 1% or 0.1%). The performance of the system is given by the FRR value corresponds to this fixed value.

2.2.4.4 Fixed FRR

This operating point corresponds to the threshold where FRR is equal to a rate fixed by the application (e.g. 1% or 0.1%). The performance of the system is given by the FAR value corresponds to this fixed value.

2.2.5 Operating points on the DET curves

Figure 2.7 shows the four above-mentioned operating points represented on the DET curve. The threshold point of EER is the threshold for which the two error rates FAR and FRR are equal; it corresponds to the intersection of the curve with the diagonal for the DET curve.

On the DET curve represented in figures 2.7, three operating points are represented, WER such as FRR = 2FAR, and the tow points FAR at FRR =0.05, and FRR at FAR= 0.05. In this Figure (ROC), the term of the operating point is perfect sense because this is a point located on the curve for which we can estimate the values of the error rates, FAR and FRR.

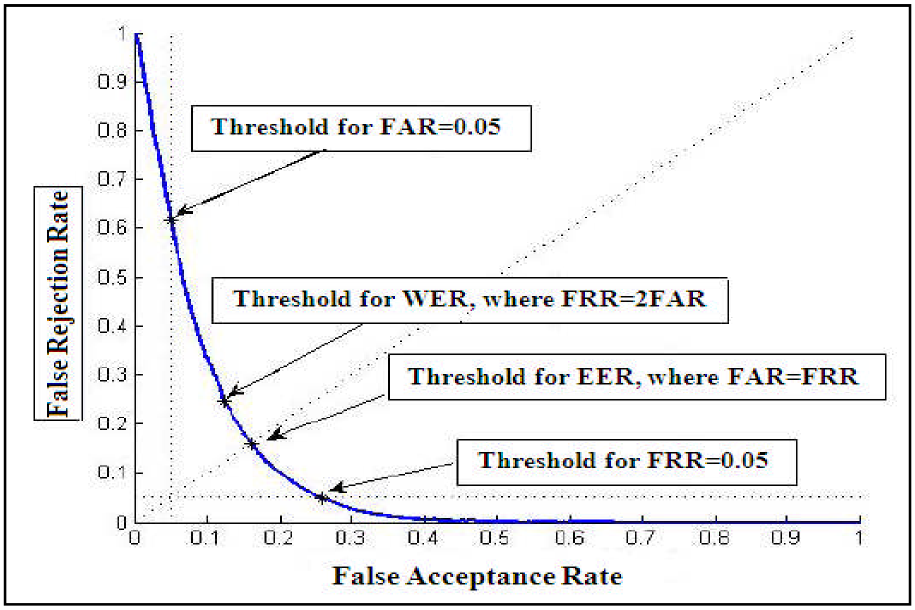


Figure 2.7: The operating points represented on a DET curve **[08]**.

For each of these points, several values can then be estimated using FAR and FRR. The most standard error is also called average HTER (Half Total Error Rate) which represent the average between FAR and FRR.

$$\mathbf{HTER} = \frac{\boldsymbol{FAR + FRR}}{\mathbf{2}} \qquad (\mathbf{2.7})$$

For the operating points associated with the WER (Weighted Error Rate) it is logical to use a global (total) error value that takes into account the weighting. The WTER (Weighted Total Error Rate) can be used as follows:

$$\boldsymbol{WTER = \alpha * FAR + (1 - \alpha) * FRR} \qquad (\mathbf{2.8})$$

In our preceding example, where we used the operating point that corresponds to FRR=2FAR, i.e. $\frac{\mathbf{1}}{\mathbf{3}}\mathbf{FRR} = \frac{\mathbf{2}}{\mathbf{3}}\mathbf{FAR}$**,**

For the other two operating points that correspond to the fixed values of FAR or FRR, in both cases, the global value of the error rate was not used, but the value of the error rate is not fixed. For example, on Figure 2.7, for the point corresponding to FAR = 0.05 we read that FRR = 0.61.

2.2.6 The choice of an operating point

The operating point that represents the choice of the threshold in the decision module depends on the application concerned. Generally, if there is any defined application, and it is a system performance test using on a benchmark database, most often we use the EER because it is a fairly neutral operating point that promotes neither of the two errors.

However, when an application is predefined or when the performance goals are known, we can use the other operating points and usually the operating points correspond to fixed values for one of the two errors (FARR, FRR).

To adjust the optimal decision threshold, we must compromise between the comfort and the security. Comfort corresponds to a low false rejection rate (FRR) and security corresponds to a low false acceptance rate (FAR).

It is important to note that the decision threshold associated to a chosen operating point will be estimated on the development database, and we set the parameters necessary for the performance testing. For the real application the choice of this database is primordial for having a reliable biometric system.

2.3 Comparing biometric systems

It is insufficient to compare two or more biometric systems using only their FARs without taking into consideration their FRRs. Because in this case, it is possible that the system with the lower FAR has got an acceptable higher FRR. But even if the FARs and FRRs values are given, there still exists the problem, that those values are threshold depending. Assuming that the threshold of the system is adjustable, there is no reasonable way to decide if a system with a higher FAR and a lower FRR perform better than a system with a lower FAR and a higher FRR values.

The EER of a system can be used to give a threshold independent performance measure. The lower the EER is the better is the system's performance. To get comparable results it is necessary that the compared EERs are calculated on the same test data using the same test protocol. For example for comparing various multimodal fusion techniques, the fusion process must be performed on the same dataset and in the same conditions.

2.4 Summary and Conclusion

In this chapter, we presented some state -of -the-art tools and criteria used to evaluate the reliability of the biometrics or multimodal biometric systems and compare their performances. We have seen that there are three types of performance evaluation, namely technological evaluation, the evaluation of scenario and operational evaluation. But this chapter was accentuated on the technological one, which evaluates the biometric systems according to their error rates for the identity verification. It was shown that, FAR and FRR are the two well-known errors that can be used to calculate the operating points necessary for defining a decision threshold, this threshold is then used to decide if the person claimed is a client or impostor. To visualize the performance of the biometric system, three well-known curves were presented namely ROC, DET and FAR vs FRR curves.

All these tools and criteria will be used in the last chapters, first to investigate the performance of each fusion methods involved, then to make a comparative study between these methods. Since score level fusion is commonly preferred in the literature, the next chapter will focus on this level of fusion by highlighting some fusion techniques involved in this study and some recent works carried out to date in this field area of research.

Chapter

03

Multimodal biometrics fusion techniques

***Abstract**: This Chapter presents a theoretical review of some state-of-the-art biometrics fusion techniques. These techniques are categorized into two main approaches, namely combination approach and classification one. For the first approach, this chapter provides five simple methods for biometrics fusion, such as product rule, sum rule, maximum rule, minimum rule and Brute Force Search (BFS), and two evolutionary techniques such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO). For the second approach, two different techniques are presented in this chapter, namely a hybrid intelligent technique such as Adaptive Neuro-Fuzzy Inference System (ANFIS) and a statistical learning method such as Support Vector Machine (SVM). Through this chapter, an overview of some well-known scores normalization techniques is given. This chapter also presents the principle of Unconstraint Cohort Normalization (UCN) as an effective method to tackle to the problem of data variation. Finally, the chapter provides some recent works and investigations carried out to date in the field of biometric fusion.*

***Résumé :** Ce chapitre présente une étude théorique de quelques techniques de fusion biométrique multimodales. Ces techniques sont classées en deux principales approches, à savoir l'approche de combinaison et l’approche de classification. Pour la première approche, ce chapitre fournit cinq méthodes simples pour la fusion biométrique, à savoir le produit, la somme, le maximum, le minimum et recherche par force brute (BFS), et deux techniques évolutives telles que les algorithmes génétiques (GA) et l’optimisation par les essaims de particule (PSO). Pour la deuxième approche, deux techniques différentes sont présentées dans ce chapitre, à savoir une technique intelligente hybride comme système adaptative d'inférence Neuro-floue (ANFIS) et une méthode d'apprentissage statistique, comme les Machines à Support Vecteur (SVM). Grâce à ce chapitre, un aperçu de certaines techniques de normalisation des scores est donné. Ce chapitre présente également le principe de la normalisation de cohorte sans contrainte (UCN) comme une méthode efficace pour remédier au problème de la variation des données. Enfin, le chapitre fournit quelques travaux récents réalisés dans le domaine de la fusion biométrique.*

3.1 Introduction

In the first chapter, we've already seen that in a multimodal biometric system, information fusion can be done at four different levels, and it was shown that integration at the matching score level is generally preferred and mostly used.

Scores level fusion can be divided into two distinct categories. In the first approach the fusion is viewed as a classification problem, while in the second approach it is viewed as a combination problem **[07]**. In this chapter we will give an overview on some classification and combination approach based techniques used in multimodal biometric score level fusion.

For the combination approach, we will introduce some evolutionary techniques along with simple ones. For the classification approach we will introduce a hybrid intelligent method and a statistical learning one.

Since the matching scores resulted from the various modalities are heterogeneous, score normalization is needed to convert them into the same nature, prior to combining them, so some well-known scores normalization methods will be also introduced in this chapter, and the principle of the UCN normalization process will be also discussed and illustrated.

By the end of this chapter, we will provide a review of the outcomes of some recent works and investigations carried out to date in the field of multimodal biometric fusion.

3.2 Score Normalization

Since the matching scores output by the various modalities are diverse, score normalization is needed to transform these scores into a common domain, prior to combining them. For example, one matcher may produce a distance (dissimilarity) measure while another may produce a proximity (similarity) measure; as a result, the matching scores at the output of the matchers may follow different statistical distributions. Consequently, score normalization is essential to transform the scores of the individual matchers into a common range. Score normalization is a critical part in the design of a combination scheme for score level fusion. Score normalization consists of changing both the location and scale parameters of the scores distribution, so that the scores of different classifiers are mapped into a common domain **[07]**.

3.2.1 Scores Normalization Techniques

According to the literature, there are various well-known range-normalization techniques, namely (but not limited to), Min-Max, Z-score, Tanh, Median-MAD, Double-sigmoid, Decimal Scaling Normalization. Min-Max and Z-score (in most cases) have shown to be amongst the most effective and widely used methods for the scores normalization. For a good normalization scheme, the estimates of the location and scale parameters of the matching score distribution must be robust and efficient. Robustness refers to insensitivity to the presence of outliers. Efficiency refers to the closeness of the obtained estimate to the optimal estimate when the distribution of the data is known.

Unconstrained Cohort Normalization (UCN) is an adapted normalization technique that aims to reduce the effect of data degradation on the matching scores.

3.2.1.1 Min-Max Normalization (MM)

Min-max normalization technique performs linear transformation on the data so does not change the initial distribution type. It is used when the maximum and minimum values of the data produced by the classifiers are known. Each data point is normalized using the following transformation **[41]:**

$$n = \frac{s - min\ (S)}{max(S) - min(S)} \qquad (\mathbf{3.1})$$

where, **n** is the normalized score, **min(S)** and **max(S)** are the minimum and maximum values of the scores dataset.

This method retains the statistical distribution and only scales and transforms the data into a common numerical range between [0, 1]. It performs best for Gaussian distributions.

Min-Max normalization method is not robust (i.e., the method is sensitive to outliers), because the minimum and the maximum scores are estimated using the training dataset, so they are fixed, consequently, there is a risk of overflow of data in the operational phase of the system if one of the testing dataset scores exceeds the maximum, consequently, we may obtain some negatives values **[16]**.

3.2.1.2 Z-score Normalization (ZS)

Z-score normalization technique uses the arithmetic mean and standard deviation of the training data, the z-score normalized method is given by:

$$n = \frac{s - mean(S)}{std(S)} \tag{3.2}$$

where $\boldsymbol{mean}()$ is the arithmetic mean and $\boldsymbol{std}()$is the standard deviation of the given data. However, both mean and standard deviation are sensitive to outliers and hence, this method is not robust. Z-score normalization does not guarantee a common numerical range for the normalized scores of the different matchers **[10]**.

3.2.1.3 Tanh (TH)

The tanh-estimators are robust and highly efficient normalization method, it maps the raw scores to the [0, 1] range, the tanh normalization is given by:

$$n = \frac{1}{2}\left[tanh\left(0.01\frac{(s - mean(S))}{std(S)}\right) + 1\right] \tag{3.3}$$

The Tanh normalization method is not sensitive to outliers,

3.2.1.4 Double sigmoid

The double sigmoid function used in **[38],** to normalize scores in a multimodal biometric system that combines different fingerprint classifiers. The normalized scores are given by the following function:

$$n = \begin{cases} \dfrac{1}{1 + exp(-2\left(\left(\frac{s-m}{s_1}\right)\right)} & \text{if } s < m. \\ \dfrac{1}{1 + exp\left(\left(\frac{s-m}{s_2}\right)\right)} & Otherwise. \end{cases} \tag{3.4}$$

where **m** is the reference operating point and **s₁** and **s₂** denote the left and right edges of the region in which the function is linear, i.e., the double sigmoid function exhibits linear characteristics in the interval $(m - s_1, m - s_2)$.

Figure 3.1 shows an example of the double sigmoid normalization, where the scores in the [0, 300] range are mapped to the [0, 1] range using m = 200, s_1 = 20 and s_2 = 30.

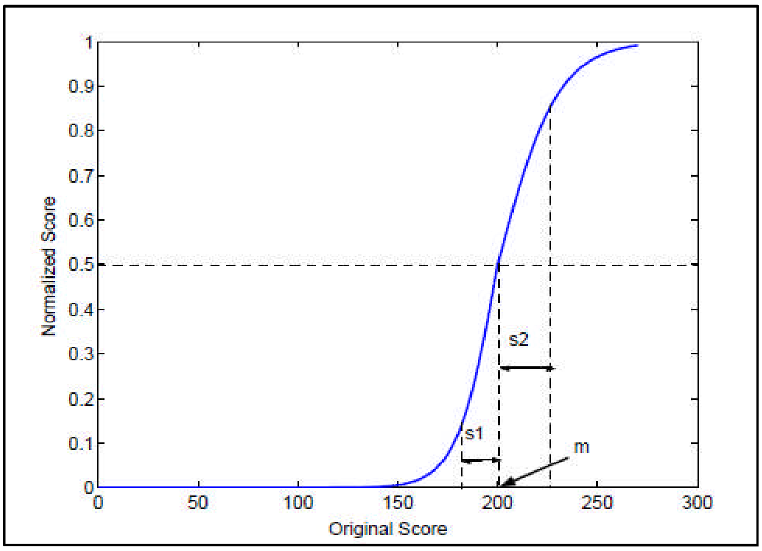


Figure 3.1: Double sigmoid normalization.

This scheme transforms the scores into the [0, 1] interval. But, it requires careful tuning of the parameters m, s_1, s_2 to obtain good efficiency.

3.2.1.5 Decimal Scaling Normalization

Decimal scaling can be applied when the scores of different matchers are on a logarithmic scale. For example, if one matcher has scores in the range [0, 1] and the other has scores in the range [0, 1000], the following normalization could be applied.

$$n = \frac{s}{10^m} \qquad (3.5)$$

where $m = \log_{10}$ max (s). The problems with this approach are lack of robustness and the assumption that the scores of different matchers vary by a logarithmic factor.

3.2.1.6 Median and median absolute deviation (MAD)normalization

The normalized scores using median and MAD is given by the following equation:

$$n = \frac{s - median}{MAD} \qquad (3.6)$$

where MAD = median(|s − median|).

These normalization techniques are insensitive to outliers and the points in the extreme tails of the distribution. It have a low efficiency compared to the mean and the standard deviation estimators, i.e., when the score distribution is not Gaussian, median and MAD are poor estimates of the location and scale parameters**[07]**.

Finally, it can be concluded that the min-max, decimal scaling and z-score normalization schemes are efficient, but are not robust to outliers. On the other hand, the median normalization scheme is robust but inefficient. Only the double sigmoid and tanh-estimators have both the desired characteristics, namely robustness and efficiency.

3.2.1.7 Unconstrained Cohort Normalization (UCN)

Biometric data variations are considered as one of the main problems in multimodal fusion. Such variations are reflected in the corresponding biometric scores, and can badly influence the overall effectiveness and accuracy of biometric recognition. These variations can arise due to non ideal capturing condition such background noise. Another aspect of difficulty in multimodal biometrics is the lack of information about the relative variation in the different types of biometric data **[26]**.

To tackle this problem of data variation, recently, there have been considerable investigations into the enhancement of the accuracy and the robustness of multimodal biometrics, through the introduction of UCN into the field **[18, 19]**. Whilst this score normalization scheme has been widely used in voice biometrics **[39]**, UCN can be very useful to separate the genuine scores from the impostors' scores.

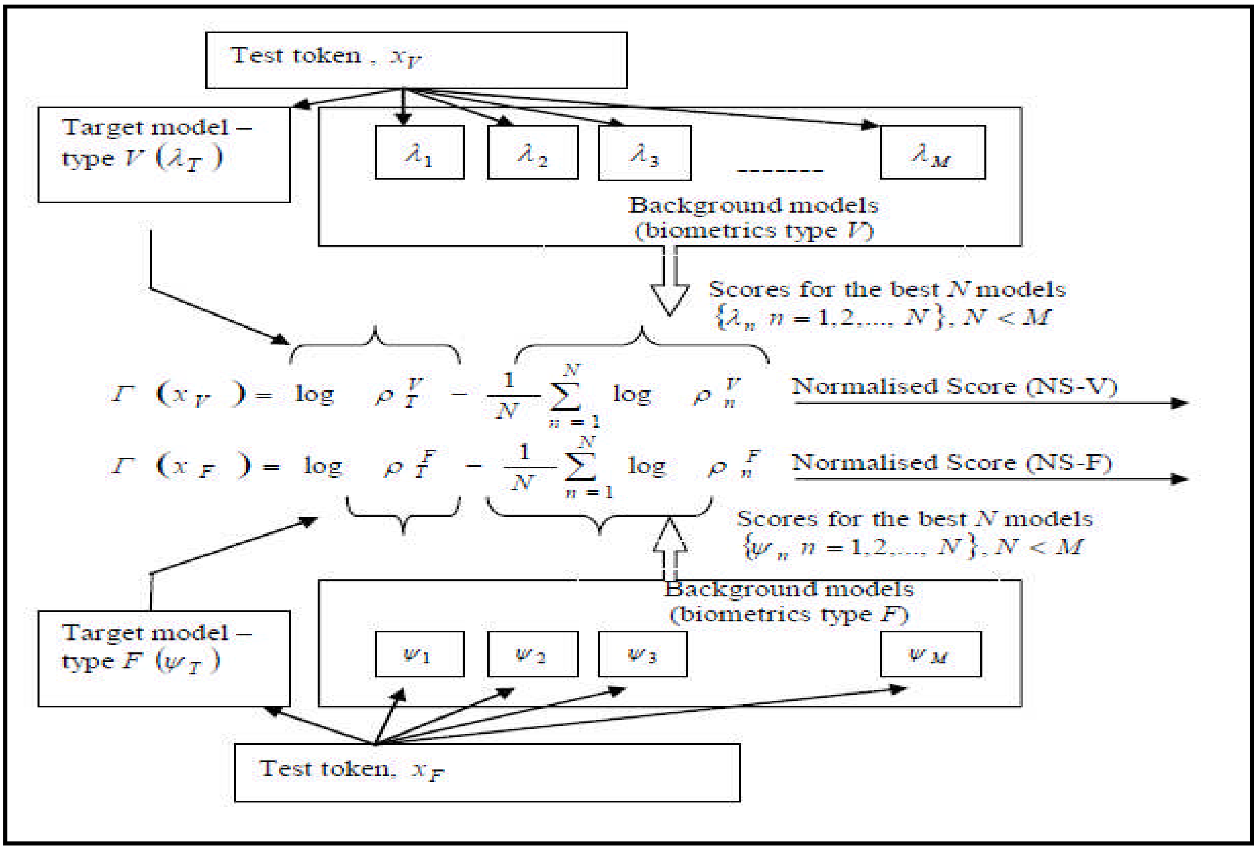
UCN provides a useful means for appropriately adjusting the individual biometric scores for a client, without any prior knowledge of the level of degradation of each biometric data type involved. Another motivation for using UCN in multimodal biometrics is that it facilitates the suppression of the individual biometric scores for impostors in relation to those for the clients **[18]**.

As described in **[19]**, given a test token of certain biometrics type, the normalized matching score provided through UCN can be expressed as:

$$X_{(f/s)} = log\ \rho T^{(f/s)} - \frac{1}{C}\sum_{c=1}^{C} \log \rho c^{(f/s)} \qquad (3.7)$$

where $\boldsymbol{f}$ and $\boldsymbol{s}$ denote the biometrics type (face and speech), $\boldsymbol{X_{(f/s)}}$ is the normalized score for face or speech modality, $\boldsymbol{\rho T^{(f/s)}}$ is the score for the target model, $\boldsymbol{\rho c^{(f/s)}}$are the scores obtained for a set of competing models, and C is the number of competing models considered. These competing models are selected dynamically from a group of background models, based on their closeness to the test token.

Figure 3.2 illustrate the concept of deploying UCN in a multimodal biometric recognition system.


Test token , x_V
Target model – type V (λ_T)
λ_1
λ_2
λ_3

λ_M
Background models (biometrics type V)
Scores for the best N models $\{\lambda_n, n = 1,2,\ldots, N\}, N < M$
$\Gamma(x_V) = \log \rho_T^V - \frac{1}{N}\sum_{n=1}^{N} \log \rho_n^V$
Normalised Score (NS-V)
$\Gamma(x_F) = \log \rho_T^F - \frac{1}{N}\sum_{n=1}^{N} \log \rho_n^F$
Normalised Score (NS-F)
Scores for the best N models $\{\psi_n, n = 1,2,\ldots, N\}, N < M$
Background models (biometrics type F)
Target model – type F (ψ_T)
ψ_1
ψ_2
ψ_3
ψ_M
Test token, x_F

Figure 3.2: Unconstrained cohort normalization (UCN) of scores from the individual biometric modalities **[26]**.

3.3 Multimodal biometric score level fusion techniques

Score level fusion, also denoted as measurement or confidence level fusion **[05]**, refers to the use of fusion techniques to combine the matching scores provided by the different classifiers.

In the context of the identity verification or identification, score level fusion can be categorized into two approaches. In the first approach the fusion is viewed as a classification problem, where the individual matching scores are normalized into the same range and then combined to generate a single scalar score (fused score) which is then used to make the final decision **[07]**. While in the second approach the fusion is viewed as a combination problem, where a feature vector is constructed using the matching scores output by the individual matchers; this feature vector is then classified into one of two classes: “Accept” (genuine user) or “Reject” (impostor user) **[05]**.

In our study, the comparative study between two state-of-the-art evolutionary techniques tools along with some classical and hybrid intelligent techniques, leads us to categorize the fusion techniques into four categories, namely Simple, evolutionary, hybrid intelligent and statistical learning approach.

For all techniques presented in this chapter, we note by $\boldsymbol{n_m^i}$ the normalized score provided by the $\boldsymbol{m^{th}}$ classifier at the $\boldsymbol{i^{th}}$ test, and by $\boldsymbol{f_i}$ the fused score.

3.3.1 Simple Approach

In this approach many state-of-the-art techniques have been investigated into the matching scores fusion, namely, and not limited to: Product rule, Sum rule, Majority voting rule, Min rule, Max rule and Brute force search (BFS).

3.3.1.1 Product Rule

This fusion technique computes the fused score by multiplying the scores for all modalities involved. It is mathematically defined as:

$$\boldsymbol{f_i = \prod_{m=1}^{M} n_m} \qquad (\mathbf{3.8})$$

3.3.1.2 Sum Rule

Using this technique the fused score is computed by adding the scores for all modalities involved. The computation here is defined as:

$$\boldsymbol{f_i = \sum_{m=1}^{M} n_m} \qquad (\mathbf{3.9})$$

3.3.1.3 Maximum Rule

Maximum rule method selects the score having the largest value amongst the modalities involved. It is defined mathematically as:

$$\boldsymbol{f_i} = \mathbf{max}\left(\mathrm{n_i^1}, \mathrm{n_i^2}, \dots, \mathrm{n_i^M}\right) \quad \forall \mathrm{i} \qquad (\mathbf{3.10})$$

3.3.1.4 Minimum Rule

Minimum rule method selects the score having the least value amongst the modalities involved. It is defined mathematically as:

$$\boldsymbol{f_i} = \mathbf{min}\left(\mathbf{n_i^1}, \mathbf{n_i^2}, \dots, \mathbf{n_i^M}\right) \quad \forall \mathbf{i} \qquad (\mathbf{3.11})$$

3.3.1.5 Brute Force Search BFS

Brute Force Search or exhaustive search, also known as generate and test, is a trivial but very general problem-solving technique that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement **[55]**, until it finds one that is acceptable or until a pre-set maximum number of attempts or a stopping criteria (the search interval).

3.3.1.5.1 Advantage and disadvantage of BFS

BFS is an exhaustive search algorithm. It is simple to implement. And it can be applied to any search problem.

Another advantage of BFS algorithm is its capability to test all the possible solutions by exploring the whole search interval, hence, if there is an optimal solution in this interval, BFS will definitely find it out.

One of the drawbacks of BFS algorithm that it is a behind search, it spends lots of time to explore the whole search interval even if the optimal solution is already found, and especially if the search space is large.

3.3.1.5.2 Brute Force Search for Multimodal biometric scores fusion

In this method, weights are calculated heuristically using exhaustive search and assigned to the modalities involved in the fusion scheme. This fusion technique can be only used in the case of having two matcher types **[02]**. This technique can be formulated with the following equation:

$$\boldsymbol{f} = \mathbf{w} * \mathbf{n_1} + (\mathbf{1} - \mathbf{w}) * \mathbf{n_2} \qquad (\mathbf{3.12})$$

where $\boldsymbol{f}$ is the fused score.

$\boldsymbol{n_1}, \boldsymbol{n_2}$: are the normalized scores of the tow matchers involved.

w: is a weighting factor in the interval **[0, 1]**. The weight (**w**) is calculated heuristically, by exhaustive search in order to obtain the tow weights that minimize the Equal Error Rate (EER) on the development data.

3.3.2 Evolutionary approach

This section presents some evolutionary techniques for multimodal biometric score level fusion. These techniques are employed to determine the optimal fusion strategy and the corresponding fusion parameters, various evolutionary methods has been discussed in the literature, namely and not limited to, Genetic Algorithms (GA) and Particle swarm optimization (PSO).

3.3.2.1 Genetic Algorithms

Genetic algorithms (GAs) were invented by **John Holland** in the 1960s and were developed by Holland and his students and colleagues at the University of Michigan in the 1960s and the 1970s. Holland presented the genetic algorithm as an abstraction of biological evolution and gave a theoretical framework for adaptation under the GA **[24]**.

Using the genetic algorithms, the problem solutions should be represented as genomes (or chromosomes).

3.3.2.1.1 GA Operators

The Genetic Algorithms create a population of solutions and apply genetic (biological-like) operators such as **[01]**:

- **Reproduction:** Generates a population of candidates (chromosomes) in some region of the space; i.e. exploration.
- **Crossover:** This operator randomly chooses a locus and exchanges the subsequences before and after that locus between two chromosomes to create two offspring for the next generation.
- **Mutation:** Simulate small random variation of the genotype. Mutation can occur with some probability, usually very small (e.g., 0.001).
- **Selection**: According to the fitness function, this operator selects chromosomes for reproduction. The fitter is the chromosome, the more times it is likely to be selected to be reproduced.

Each chromosome in a GA population can be thought of as a point in the search space of candidate solutions. The GA processes populations of chromosomes, successively replacing one such population with another **[24]**.

The GA requires a fitness (Cost or Objective) function that assigns a score (fitness) to each chromosome in the current population. The fitness of a chromosome depends on how well that chromosome solves the problem.

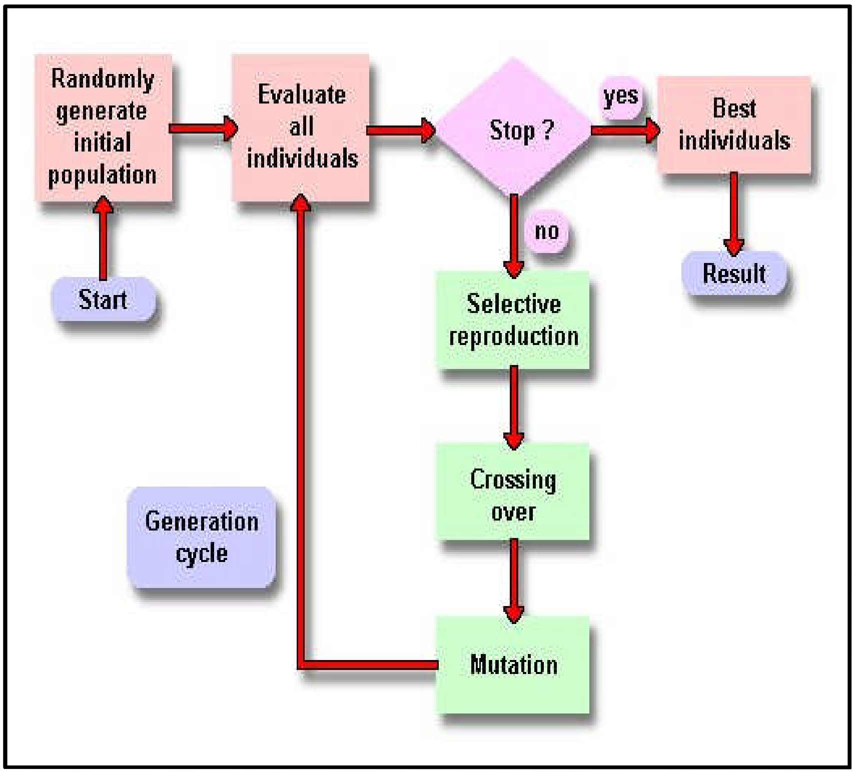


Figure 3.3: Genetic Algorithm Flowchart.

3.3.2.1.2 Advantages and disadvantages of GAs

GA has a number of advantages:

- It can quickly scan a vast solution set.
- For an optimization problem, Genetic Algorithms are capable to find the global optimum solution in a multi-dimensional space without worrying about local minima.

GA has some drawbacks too:

- The major disadvantage of GA is that the algorithm uses a very large amount of processing time **[64]**.

3.3.2.1.3 Genetic Algorithms for Multimodal biometric scores fusion

The algorithm starts with generating an initial population of chromosomes (weights) $\boldsymbol{W_i^0} = (\boldsymbol{w_1}, \boldsymbol{w_2})$ **,** which are used to calculate the fused score (***f***) such as **[01]**:

$$f = w_1 * n_1 + w_2 * n_2 \tag{3.13}$$

where $\boldsymbol{n_1, n_2}$: are the normalized scores of the tow matchers involved.

$\boldsymbol{w}$: is a weighting factor in the interval **[0, 1]**.

For each chromosomes candidate $\boldsymbol{W_i}$, we calculate the fitness function **EER (*f*)**, and then select the best individuals $\boldsymbol{W_i^0}$ for which **EER (*f*)** are minimal. The reproduction (mutation and cross-over) will be performed on these individuals. At this step a new population ***i*** of chromosomes $\boldsymbol{W_i^j}$ is created for the next generation ***j;***

where : ***i=1…N, N***is the population size.

j=1…M, M is the maximum number of generations.

GA Algorithm

```
Begin
    • Generate random population of chromosomes (weights) $\boldsymbol{W_i^0} = (\boldsymbol{w_1}, \boldsymbol{w_2})$ ;
    • Compute fused scores$\boldsymbol{f} = \boldsymbol{w_1} * \boldsymbol{n_1} + \boldsymbol{w_2} * \boldsymbol{n_2}$;
    • Compute and evaluate the Fitness Function EER (f) for each individual $\boldsymbol{W_i^0}$
For  i=1 to M  do  // M is the maximum number of generations.
Begin
    • Select some individuals $\boldsymbol{W_i^0}$ for reproduction  // according to fitness function.
    • Perform crossover    // with a crossover probability.
    • Perform Mutation    // with a mutation probability.
    • Accept new generation // according to fitness function.
End.
End.
```

3.3.2.2 Particle Swarm Optimization (PSO)

Particle swarm optimization is a population based evolutionary algorithm proposed by Doctor Kennedy and Eberhart in 1995, which is based on swarm intelligence **[20]**. It was inspired by social behavior of flocks of birds when they are searching for food. In PSO, the potential solutions, called particles, fly through the problem space exploring for better regions **[17]**.

Due to its simplicity and easy implementation, the PSO algorithm can be used widely in the fields such as function optimization, the model classification, machine learning, neutral network training, the signal processing, vague system control, automatic adaptation control, etc. **[20].**

3.3.2.2.1 Principle of Particle Swarm Optimization Algorithm

PSO is a stochastic, population based optimization technique aiming at finding a solution to an optimization problem in a search space. Each candidate solution is therefore modeled by particle in a search space. Each particle adjusts its trajectory by making use of its individual memory and of the knowledge gained by its neighbors to find the best solution. Each particle tests a possible solution to the multidimensional problem as it moves through the problem space. The movement of the particles is influenced by two factors: the particle's best solution **(pbest)** and the global best solution found by all the particles **(gbest) [21].** The particle interacts with all the neighbors and stores in its memory optimal location information.

After each iteration the pbest and gbest are updated if a more optimal solution is found by the particle or population, respectively. This process is continued iteratively until either the optimal result or the stopping criterion is achieved.

Each particle in the D-dimensional space is defined as:

$$X_m = (x_{m1}, x_{m2}, x_{m3}, \dots x_{mD}) \qquad (\mathbf{3.14})$$

Where the **m** represents the particle number and the **D** is the space dimension.

The memory of the previous best position is represented as:

$$P_m = (P_{m1}, P_{m2}, P_{m3}, \dots\ P_{mD}) \qquad (\mathbf{3.15})$$

The velocity along each dimension is represented as:

$$V_m = (V_{m1}, V_{m2}, V_{m3}, \dots V_{m4}) \qquad (\mathbf{3.16})$$

After each iteration, the velocity is updated. The particle's movement is influenced by its own position $\boldsymbol{P_m}$, as well as its global position $\boldsymbol{P_g}$.

The velocity can be represented by the following equation:

$$V_{id}^{new} = w * V_{md}^{old} + c_1 * rand_1(\,) * \left(pbest_{md} - X_{md}^{old}\right) + c_2 * rand_2(\,) * \left(gbest_{md} - X_{md}^{old}\right) \qquad (3.17)$$

The position is updated using the following equation:

$$X_{id}^{new} = X_{id}^{old} + V_{id}^{new} \qquad (\mathbf{3.18})$$

Where $\boldsymbol{w}$ is the inertia weight, optimizing the choice of inertia weights provides a balance between global and local exploration and exploitation, and results in less iteration on average to find sufficiently optimal solution **[27]**.

$\boldsymbol{c_1}, \boldsymbol{c_1}$ **:** The acceleration constants that represent the weighting of the stochastic acceleration terms that pull each particle toward ***pbest*** and ***gbest*** position, early experience led to set the constant $\boldsymbol{c_1}$=$\boldsymbol{c_2}$ **=2.0** for almost all applications**[27]**.

$\boldsymbol{rand_1}(\,), \boldsymbol{rand_2}(\,)$**:** Random numbers between (**0, 1**).

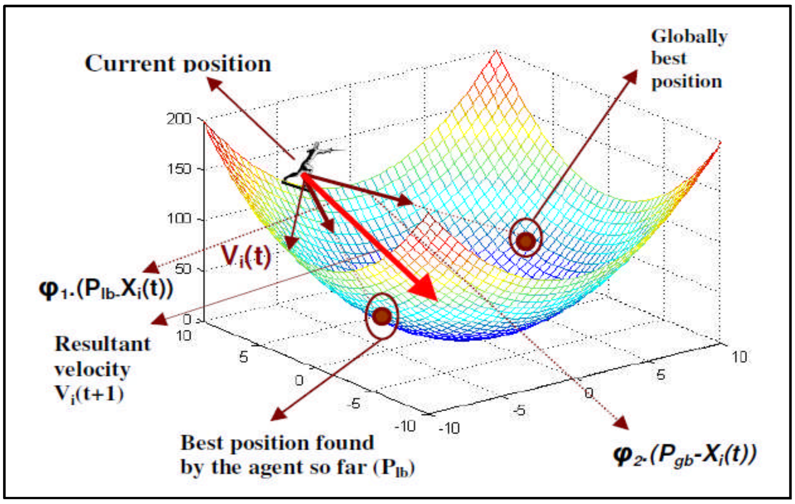

Current position
Globally best position
200
150
100
50
0
$V_i(t)$
$\varphi_1.(P_{lb}-X_i(t))$
Resultant velocity $V_i(t+1)$
10
5
0
-5
-10
-10
-5
0
5
10
Best position found by the agent so far (P_{lb})
$\varphi_2.(P_{gb}-X_i(t))$

Figure 3.5: Illustrating the velocity updating scheme of basic PSO.

PSO Algorithm

```
1. Initialize
(a) Set constants $\boldsymbol{w}$, $\boldsymbol{C_1}, \boldsymbol{C_2}$.
(b) Randomly initialize particle positions $\boldsymbol{x_0^i} \,\epsilon\, \boldsymbol{D}$ in $\mathbb{R}^{\boldsymbol{n}}$
(c) Randomly initialize particle velocities $\boldsymbol{0} \le \boldsymbol{v_0^i} \le \boldsymbol{v_0^{max}}$
(d) Set k=1
2. Optimize
(a) Evaluate Fitness function value $\boldsymbol{f_k^i}$ using design space coordinates $\boldsymbol{x_k^i}$ .
(b) If $\boldsymbol{f_k^i} \le \boldsymbol{f_{best}^i}$ then $\boldsymbol{f_{best}^i} = \boldsymbol{f_k^i}$ , $\boldsymbol{\mathcal{P}_k^i} = \boldsymbol{x_k^i}$ .
(c) If $\boldsymbol{f_k^i} \le \boldsymbol{f_{best}^g}$ then $\boldsymbol{f_{best}^g} = \boldsymbol{f_k^i}$, $\boldsymbol{\mathcal{P}_k^g} = \boldsymbol{x_k^i}$.
(d) If stopping condition is satisfied then goto 3.
(e) Update all particles velocities $\boldsymbol{v_k^i}$ for $i$=1,….,P
```

```
    (f) Update all particles positions $x_k^i$ for $i= I,\ldots,P$
    (g) Increment k
    (h) Goto 2(a)
3. Terminate
```

3.3.2.2.2 Advantages and Disadvantages of the Basic PSO Algorithm [20]

- **Advantages:**

- The main advantage of PSO is the fast convergence **[62]**.
- PSO have no overlapping and mutation calculation. The search can be carried out by the speed of the particle. During the development of several generations, only the most optimist particle can transmit information onto the other particles, and the speed of the researching is very fast.
- PSO is easy to implement and there are few parameters to adjust.
- Other advantages of PSO are that PSO is rapidly converging towards an optimum, simple to compute, easy to implement and free from the complex computation in genetic algorithm (e.g., coding/decoding, crossover and mutation) **[64]**.

- **Disadvantages**

- The method easily suffers from the partial optimism, which causes the less exact at the regulation of its speed and the direction.
- The main disadvantage of the gbest topology is that it is unable to explore multiple optimal regions simultaneously **[62]**.
- PSO sometimes is easy to be trapped in local optima, and the convergence rate decreased considerably in the later period of evolution; when reaching a near optimal solution, the algorithm stops optimizing, and thus the accuracy the algorithm can achieve is limited **[64]**.
- PSO algorithms operate by the notion of following a leader to scan the search-space. This movement of following certain particles of a population can become a disadvantage in problems where there are many local optimal fronts **[65]**.

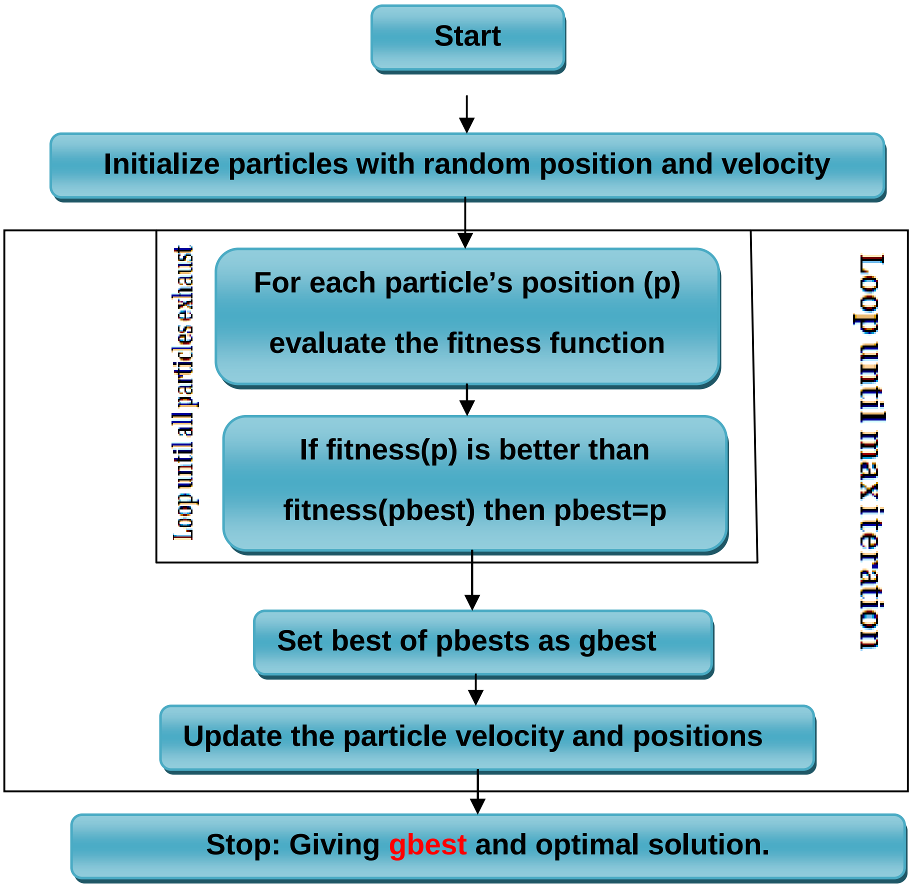

Start
Initialize particles with random position and velocity
For each particle's position (p) evaluate the fitness function
If fitness(p) is better than fitness(pbest) then pbest=p
Loop until all particles exhaust
Set best of pbests as gbest
Update the particle velocity and positions
Loop until max iteration
Stop: Giving gbest and optimal solution.

Figure 3.6: Particle swarm optimization flowchart.

3.3.2.2.3 Multimodal biometric scores fusion using PSO

The PSO is employed to dynamically select the appropriate or the optimal weights (w_2, w_2) necessary to minimize the fitness function (EER of the fused score).

The performance of each particle is measured using a predefined fitness function, which is related to the problem to be solved.

3.3.3 Hybrid Intelligent Approach

A hybrid intelligent system is one that combines at least two intelligent technologies, for example, combining a neural network with a fuzzy system results in a hybrid Neuro-fuzzy Inference System, which also called Adaptive Neuro-Fuzzy Inference System (ANFIS), which is one of the promising and powerful machine learning technique.

In this section we will illustrate the principle of ANFIS classifier and its use as a matching scores level fusion in a multimodal biometric system.

3.3.3.1 Adaptive Neuro-Fuzzy Systems

ANFIS stands for "Adaptive Neuro-Fuzzy Inference Systems", as originally proposed in **[30]**, ANFIS is a fuzzy inference system implemented in the framework of adaptive networks. By using a hybrid learning procedure, ANFIS can construct an input-output mapping based on both human knowledge (in the form of fuzzy if-then rules) and stipulated input-output data pairs. ANFIS is a fuzzy system that uses a learning algorithm derived from or inspired by neural network theory to determine its parameters (fuzzy sets and fuzzy rules) by processing data samples.

The performance of this method is like both ANN and FL. In both ANN and FL case, the input pass through the input layer (by input membership function) and the output could be seen in output layer (by output membership functions). Therefore, ANFIS uses either backpropagation or a combination of least squares estimation and backpropagation for membership function parameter estimation **[30]**.

The advantages of FL for grade estimation is clear because it prepare a powerful tool that is flexible and in lack of data with its ability which is if-then rules would able to solve the problems. One of the biggest problems in FL application is the shape and location of membership function for each fuzzy variable which solve by trial and error method only. In contrast, numerical computation and learning are the advantages of neural network, however, it is not easy to obtain the optimal structure (number of hidden layer and number of neuron in each hidden layer, momentum rate and size) of constructed neural network and also this kind of artificial intelligent is more based on numerical computation rather that than symbolic computation **[23]**.

Both FL and NN have their advantages, therefore, it is good idea to combine their ability and make a strong tool and also a tool which improve their weakness as well as lead to least error. Jang **[30]** combined both FL and NN to produce a powerful processing tool named NFSs which is a powerful tool that has both NN and FL advantages.

3.3.3.1.1 ANFIS Architecture

We assume the fuzzy inference system under consideration has two inputs **x** and **y** and one output **z**. Suppose that the rule base contains two fuzzy if-then rules of Takagi and Sugeno’s type.

Rule 1:

$$\text{If } x \text{ is } \mathrm{A}_1 \text{ and } y \text{ is } \mathrm{B}_1 \text{ ,then } f_1 = p_1 x + q_1 y + r_1 \qquad (\mathbf{3.19})$$

Rule 2:

If x is A_2 and y is B_2 ,then $f_2 = p_2x + q_2y + r_2$ $\quad(\mathbf{3.20})$

Figure 3.4(a) illustrates the reasoning mechanism for the Sugeno model. The corresponding equivalent ANFIS architecture is shown in Figure 3.4(b). In this diagram, the output of the $\boldsymbol{i^{th}}$ node in layer **1** is denoted as $\boldsymbol{O_i^1}$ **.**

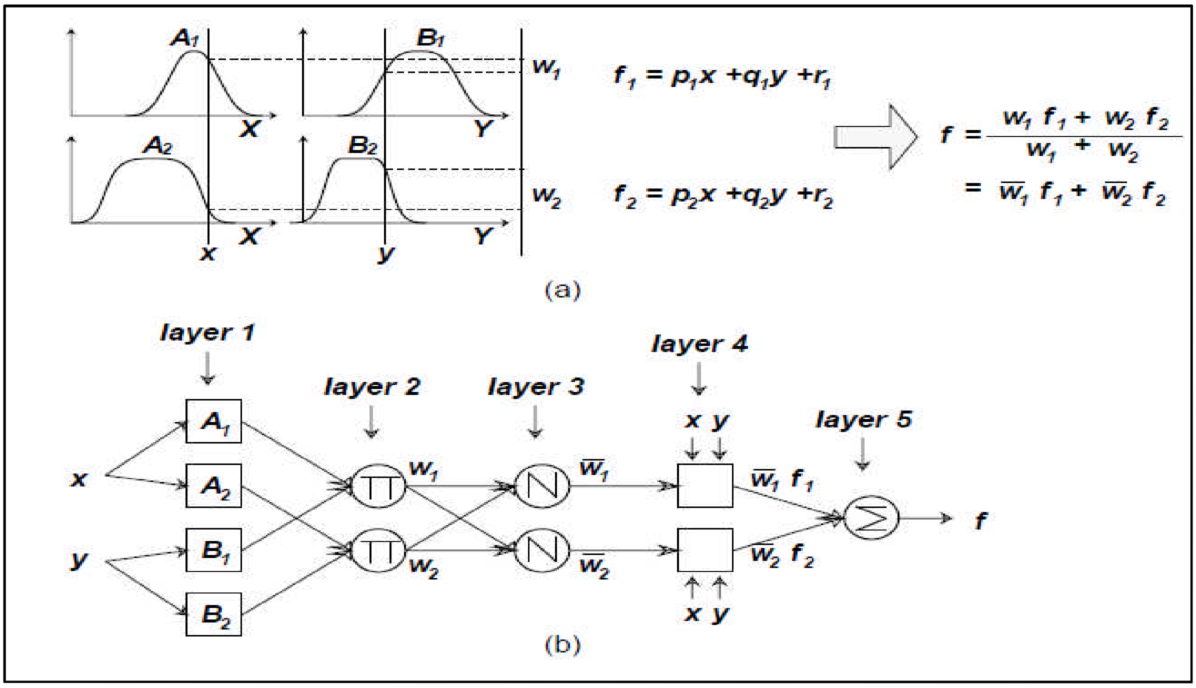


Figure 3.4: (a) Type-3 fuzzy reasoning. **(b)** Equivalent ANFIS (type-3 ANFIS).

- **Layer 1**(fuzzification layer):

Every node ***i*** in the layer ***1*** is an adaptive node. The outputs of layer **1** are the fuzzy membership grade of the inputs, which are given by:

$O_i^1 = \mu A_i(x)$ with $i = 1{,}2$ $\quad(\mathbf{3.21})$

$O_i^1 = \mu B_{i-2}(y)$ with $i = 3{,}4$ $\quad(\mathbf{3.22})$

- ***x, y*** : the inputs to node ***i***.
- $\boldsymbol{A_i, B_i}$: the linguistic labels (small, large, etc.) associated with this node function.
- $\boldsymbol{\mu A_i(x)}$and $\boldsymbol{\mu B_{i-2}(x)}$**:** any appropriate parameterized membership functions.
- $\boldsymbol{O_i^1}$ **:** the membership grade of a fuzzy set **,** and it specifies the degree to which the given input ***x*** satisfies the quantifier $\boldsymbol{A_i}$ **.**

Usually we choose $\boldsymbol{\mu A_i(x)}$ to be bell-shaped with maximum equal to 1 and minimum equal to 0, such as **[30]** :

$$\mu A_i(x) = \frac{1}{1+\left[\left(\frac{x-c_i}{a_i}\right)^2\right]^{b_i}} \qquad (\mathbf{3.23})$$

Or

$$\mu A_i(x) = exp\left\{-\left[\left(\frac{x-c_i}{a_i}\right)^2\right]^{b_i}\right\} \qquad (\mathbf{3.24})$$

Where $\{\boldsymbol{a_i}, \boldsymbol{b_i}, \boldsymbol{c_i}\}$ is the parameter set. As the values of these parameters change, the bell-shaped functions vary accordingly, thus exhibiting various forms of membership functions on linguistic label $\boldsymbol{A_i}$.

- **Layer 2** (product layer):

Every node ***i*** in the layer ***2*** is a fixed node labeled **Π**whose output is the product of all the incoming signals, which can be represented as:

$$O_i^2 = w_i = \mu A_i(x) \text{ x } \mu B_i(y) \quad withi = 1,2 \qquad (\mathbf{3.25})$$

Each node output represents the firing strength of a fuzzy control rule.

- **Layer 3** (normalization layer):

Every node ***i*** in the layer ***3*** is a fixed node labeled **M.** The ***ith*** node calculates the ratio of the ***ith*** rule's firing strength to the sum of all rules' firing strengths:

$$\overline{w_i} = \frac{w_i}{w_1 + w_2}, \quad with\ i = 1,2 \qquad (\mathbf{3.26})$$

For convenience, outputs of this layer will be called normalized firing strengths.

- **Layer 4** (defuzzification layer) :

Every node ***i*** in the layer **4** is an adaptive node. The output of each node in this layer is simply the product of the normalized firing strength and a first order polynomial.

$$O_i^4 = \overline{w_i} f_i = \overline{w_i}(p_i x + q_i y + r_i) \qquad (\mathbf{3.27})$$

Where $\overline{\boldsymbol{w_i}}$ is the output of layer ***3***, and$\{\boldsymbol{p_i}, \boldsymbol{q_i}, \boldsymbol{r_i}\}$is the parameter set. Parameters in this layer will be referred to as consequent parameters.

- **Layer5** (summation or total output neuron):

Every node ***1*** in the layer **5** is a fixed node labeled **Σ**, which computes the total output as the summation of all incoming signals.

$$O_i^5 = overall\ output = \sum_{i=1}^{2} \overline{w_i}\, f_i = \frac{\sum_{i=1}^{2} w_i f_i}{\sum_{i=1}^{2} w_i} \qquad \mathbf{(3.28)}$$

3.3.3.1.2 Learning algorithm of ANFIS

Using the gradient method to identify the parameters in an ANFIS is generally slow and likely to become trapped in local minima. In **[30]** hybrid learning rule, which combines the gradient method and the least squares estimate (LSE) for the estimation of the premise and consequent parameters, was proposed.

From the type-3 ANFIS architecture (Figure 3.4), it is observed that given the values of premise parameters, the overall output can be expressed as linear combinations of the consequent parameters.

- In the forward pass of the hybrid learning algorithm, functional signals go forward till layer 4 and the consequent parameters are identified by the least squares estimate.
- In the backward pass, the error rates propagate backward and the premise parameters are updated by the gradient descent. Table 3.1 summarizes the activities in each pass.

---	Forward pass	Backward pass
Premise parameters	Fixed	Gradient descent
Consequent parameters	Least squares estimate	Fixed
Signals	Node outputs	Error rates

Table 3.1: Tow passes in the hybrid learning procedure for ANFIS.

The details of the hybrid learning procedure that is used in an ANFIS are given in **[30, 32]**.

3.3.3.1.3 Advantages and disadvantages of ANFIS algorithm

- **Advantages:**
  - ANFIS permits the usage of neural network topology together with fuzzy logic and uses the advantages of both methods **[79]**.
  - Since ANFIS combines both neural network and fuzzy logic. It is a very powerful approach for building complex and nonlinear relationship between a set of input and output data.
- **Disadvantages:**
  - One of the problems with the ANFIS design is that a large amount of training data might be required to develop an accurate system, depending always on the research study.
  - The efficiency of the ANFIS approach depends on the estimated parameters of premise and consequent parts. Moreover, the membership functions associated with each input and output node cannot be adjusted; only the values of the rules can be **[79]**.

3.3.3.1.4 ANFIS for Multimodal biometric scores fusion

The fuzzy inference system generated by the ANFIS can be used to determine the final result of the biometric system (Genuine/Imposter), where the matching scores correspond to face and voice modalities were used as input data, and as out, the final fused score is obtained to make the final decision (tow classes classification),

3.3.4 Statistical approach

In this section we will present Support Vector Machine (SVM) as one of the powerful techniques introduced to the field of Statistical Learning Theory and its application in the area of multimodal biometric score level fusion.

3.3.4.1 Support Vector Machine (SVM)

In the problem of binary classification, the goal of Statistical Learning Theory is to separate the two classes by a function induced from available examples (training set). Classical learning approaches are designed to minimize the so-called empirical risk (i.e. error on the training set) and therefore follow the Empirical Risk Minimization (ERM) principle. Neural Nets are the most common example of ERM. The SVM on the other hand is based on the principle of Structural Risk Minimization (SRM) which states that better generalization abilities (i.e. performances on unknown test data) are achieved through a minimization of the upper bound of the generalization error **[34, 35]**.

In this section, we will introduce SVM for decision fusion in three steps. First we will show how a simple classifier (Optimal Separating Hyperplane) is used to generate a linear separating surface for linearly separable data. This principle is then generalized for non-linearly separable data. Finally we will generalize this to the case of a non-linear separating surface (non-linear SVM).

3.3.4.1.1 Linear Support Vector Machines for Linearly Separable Case:

The basic idea of the SVMs is to construct a hyperplane as the decision plane, which separates the positive (+1) and negative (-1) classes with the largest margin, which is related to minimizing the VC dimension of SVM.

It is the simplest case of SVM: linear machines trained on linearly separable data. Therefore consider the problem of separating a set of training data $\boldsymbol{\mathcal{D}}$ a set of $\boldsymbol{n}$ points of the form:

$$\boldsymbol{\mathcal{D}} = \{(\boldsymbol{X_i}, \boldsymbol{y_i})\} \setminus \boldsymbol{X_i} \in \mathbb{R}^{\boldsymbol{p}}, \boldsymbol{y_i} \boldsymbol{\epsilon} \{\{-\mathbf{1}, \mathbf{1}\}\}_{\boldsymbol{i=1}}^{\boldsymbol{n}} \qquad (\mathbf{3.29})$$

Where: the label vector $\boldsymbol{y_i}$ is either **1** or **-1**, indicating the class to which the point $\boldsymbol{X_i}$ belongs.

The feature vector $\boldsymbol{X_i}$ is a p-dimensional real vector. We wish to find the maximum-margin hyperplane that divides the points having $\boldsymbol{y_i}$**=1** from those having$\boldsymbol{y_i}$**= -1**.

Any hyperplane can be written as the set of points X satisfying

$$\boldsymbol{W}.\boldsymbol{X} + \boldsymbol{b} = \mathbf{0} \qquad (\mathbf{3.30})$$

where < **.** > denotes the dot product and **w** in the normal vector to the hyperplane. The parameter **b** determines the offset of the hyperplane from the origin along the normal vector.

There are an infinite number of hyperplanes that could partition the data into two classless. According to the SRM principle, there will just be one optimal hyperplane: the hyperplane lying half-way the maximal margin (we define the margin as the sum of distances of the hyperplane to the closest training points of each class). The solid line on figure 3.5 (b) represents this Optimal Separating Hyperplane.

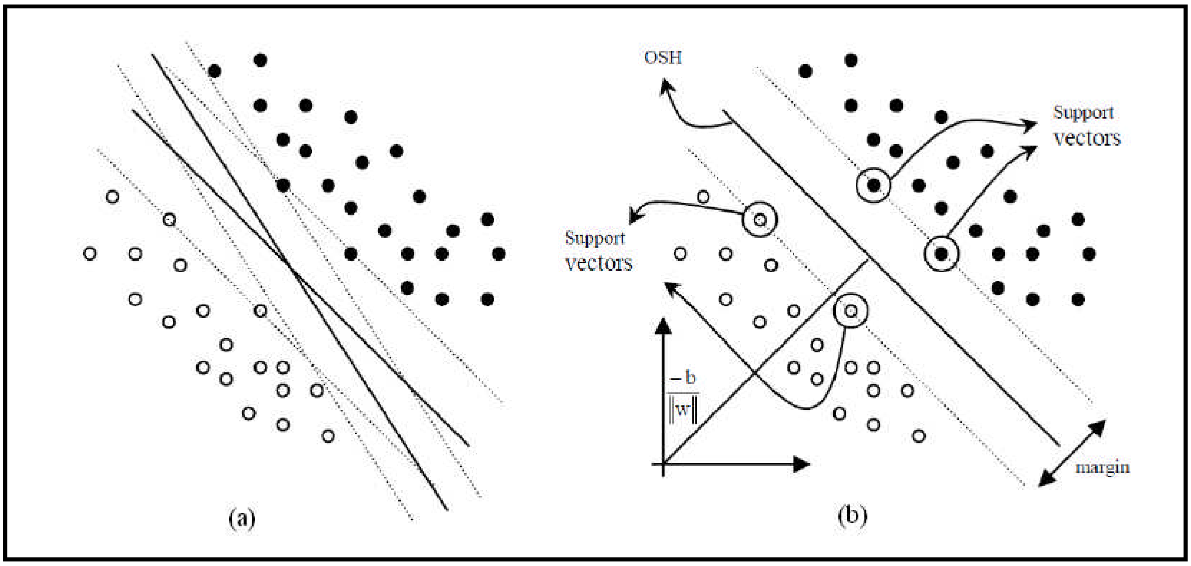


Figure 3.7: (a) Some of the possible linear hyperplanes that separate two linearly separable classes.
(b) Optimal Separating hyperplane and respective margins (dashed lines).

Note that only the closest points of each class determine the Optimal Separating Hyperplane. These points are called Support Vectors (**SV**).

It has been shown **[36]** that the maximal margin can be found by minimizing $\mathbf{1/2\|W\|^2}$

$$\boldsymbol{min}\{\mathbf{1/2}\|\boldsymbol{W}\|^{\mathbf{2}}\} \qquad (\mathbf{3.31})$$

The Optimal Separating Hyperplane can be found by minimizing (3.31) under the constraint (3.32) that the training data is correctly separated.

$$\boldsymbol{Y_i}.(\boldsymbol{X_i}.\boldsymbol{W}+\boldsymbol{b}) \geq \mathbf{1}, \forall \boldsymbol{i} \qquad (\mathbf{3.32})$$

This is a Quadratic Programming (QP) problem for which standard techniques (Lagrange Multipliers, Wolfe dual) can be used **[11]**.

3.3.4.1.2 Linear SVM for non-linearly separable data

The concept of the Optimal Separating Hyperplane can be generalized for the non-separable case by introducing a cost for violating the separation constraints (3.32). This can be done by introducing positive slack variables ξ_i in constraints (3.32), which then become:

$$Y_i.(X_i.W+b) \geq 1-\xi_i\,,\forall i \qquad (3.33)$$

If an error occurs, the corresponding ξ_i must exceed unity, so $\sum_i \xi_i$is an upper bound for the number of classification errors. Hence a logical way to assign an extra cost for errors is to change the objective function (3.31) to be minimized into:

$$min\left\{\frac{1}{2\|W\|^2}+C.(\sum_i \xi_i)\right\} \qquad (3.34)$$

where C is a chosen parameter. A larger C corresponds to assigning a higher penalty to classification errors. Minimizing (3.34) under constraint (3.33) gives the Generalized Optimal Separating Hyperplane. This still remains a Quadratic problem.

3.3.4.1.3 Non-linear SVM

In the case where decision function is not a linear function of the data, the data will be mapped from the input space (i.e. space in which the data lives) into a high dimensional space (feature space) trough a non-linear transformation (kernel function).In this (high dimensional) feature space, the (Generalized) Optimal Separating Hyperplane is constructed. This is illustrated on figure 3.6.

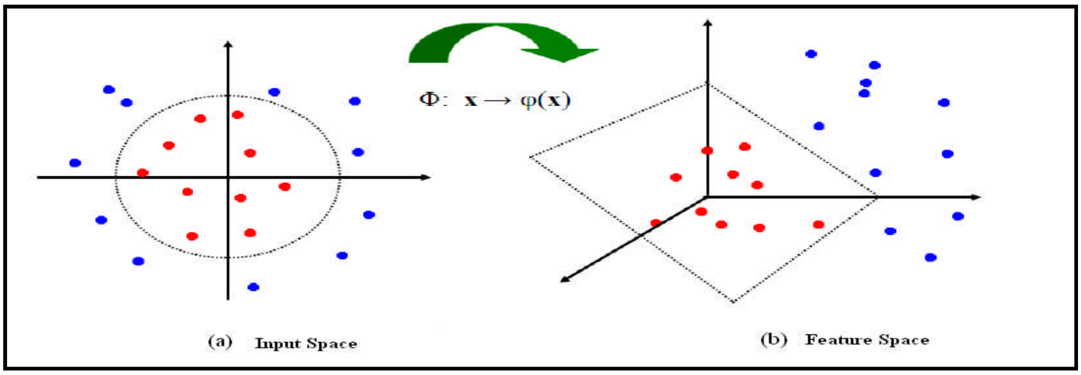


Figure 3.8: Feature space is related to input space via a nonlinear map Φ, causing the decision surface to be nonlinear in the input space.

This non-linear transformation is performed in implicit way trough so-called kernel functions. The use of implicit kernels allows reducing the dimension of the problem and overcoming the co called “dimension curse” **[36]**. The kernels must satisfy some constraints in order to be valid (Mercer’s Condition **[34]**). For binary classification following kernel are most often used:

Kernel	$K(x, x_i)$
Linear	$x^T . x_i$
Radial Basis Function	$\exp(-\gamma\|x - x_i\|^2), \gamma > 0$
Inverse multiquadratic	$\frac{1}{\sqrt{\|x - x_i\| + \eta}}$
Polynomial of degree *d*	$((x^T . x_i) + \eta)^d$
Sigmoidal	$\tanh(\gamma(x^T . x_i) + \eta), \quad \gamma > 0$

Table 3.2: Commonly Used Kernel Functions.

3.3.4.1.4 Advantages and disadvantages of SVM

- **Advantages**

- Good generalization ability for small training sets
- The control on capacity is obtained by maximizing the margin inspired by SRM.
- The absence of local minima that comes from convexity **[81]** of the quadratic optimization problem.
- Margin-based formalism can be extended to a large class of problems (regression, structured prediction, etc.).

- **Disadvantages:**

- The choice of the kernel is crucial for the success of all kernel algorithms because the kernel constitutes prior knowledge that is available about a task.
- Both training and testing speed of the high algorithmic complexity and extensive memory requirements of the required quadratic programming in large-scale tasks.

3.3.4.1.5 Matching score level fusion using SVM

After the normalization stage, we construct the scores vector$[\boldsymbol{n_1}, \boldsymbol{n_2}]$, where $\boldsymbol{n_1}$and $\boldsymbol{n_2}$ represent to the normalized scores of face and voice to be fused. Support vector machine (SVM) based fusion rule is applied to combine two matching scores to generate a single scalar score which is used to make the final decision (genuine or impostor).The design of a SVM trained fusion scheme consists in estimation of the function $\boldsymbol{f}: \boldsymbol{R^2} \to \boldsymbol{R}$ to maximize the separability of genuine and impostors score distributions.

3.4 Recent works on Multimodal biometrics fusion

In recent years, several approaches have been proposed in the literature for multimodal biometric authentication system with different biometric traits and with different fusion mechanism. Multimodal biometrics has received a considerable attention from both research communities and the market. Since, the heart of multimodal biometric system relies on fusing the information from different biometric traits, all the work reported on multimodal biometric system was confined to four different levels of fusion. Due to the advantages offered by the score level fusion, the discussions are focused on this level of fusion.

This section review the outcomes of some recent investigations carried out to date in the field of multimodal biometrics fusion with a brief description of the work performed.

1. In **2003**, Fierrez-Aguilar and Ortega-Garcia **[22]** have introduced a multimodal biometrics fusion system which integrates face verification system based on a global appearance representation scheme, a minutiae-based fingerprint verification system, and an online signature verification system based on HMM modeling of temporal functions. They have used two fusion methods namely, sum-rule and support vector machine (SVM) user independent and user dependent, at the matching score level. The EERs obtained using only one modality of the face, the online signature, and the finger print verification systems were 10%, 4%, and 3%, respectively, while using the sum-rule, the SVM user-independent, and the SVM user-dependent fusion approaches has resulted an EERs of 0.5%, 0.3%, and 0.05%, respectively.

2. In **2004**, Lau et al **[50]** have presented a multimodal biometric system combining speaker verification, fingerprint verification with face identification. The authors used a fuzzy logic based approach, in order to consider the effect of external conditions on the system. With more details they have implemented fuzzy logic module to calculate the weights for each recognition subsystem to realize the weight sum rule.

Their experimental studies showed that fuzzy logic fusion generated a further improvement of 19% relative to fusion by weighted average scores, which corresponds to an EER range of (0.31% to 0.81%).

3. In **2005**, Y. Chen and S. Lai **[17]** proposed an SVM-based multimodal fusion schemes for multimodal biometric verification based on the information from the face and speech experts. For the facial feature extraction, Principle Component Analysis (PCA) was used to compute the eigenface features from face images, and the face expert is comprised only one main component. For the speech feature extraction, the feature vector consists of Mel Frequency Cepstral Coefficients (MFCC).

The performance of concatenation fusion and opinion fusion compared with the same database, and it was shown that SVM-based fusion systems outperform the traditional GMM-based opinion fusion system.

4. In **2007**, Alsaade, et al., **[19]** has presented an investigation into the effects, on the accuracy of multimodal biometrics, by introducing unconstrained cohort normalization (UCN) into the score-level fusion process. The study has demonstrated that the capabilities provided by UCN can significantly improve the accuracy of fused biometrics. This paper, on the other hand, experimentally compares the effectiveness of two different score normalization techniques with the UCN for enhancing the accuracy of multimodal biometrics fusion under clean mixed-quality and degraded data conditions. The focus of the study is on the score-level fusion of face and voice biometrics using SVM (support vector machine).

5. In **2010**, A. Rahmoun et al **[02]** have investigated the improvement of multimodal biometric verification using genetic Algorithms (GAs). GA was used as a score-level fusion technique to integrate the face and voice modalities, the proposed technique was compared with Brute Force Search (BFS) one. To perform the fusion task, firstly the matching scores were mapped into interval [0, 1] using the Min-Max normalization methods, then the fusion schemes were applied to the normalized scores with and without subjecting them to the Unconstrained Cohort Normalization (UCN) process.

To make a comparative study and investigate the effectiveness of the two proposed techniques, their experimental studies were performed on the same databases under three data conditions namely clean, varied, and degraded data condition, and the fusion results (in terms of EER) obtained using GA were 0.00% for clean data, 0.39% for varied data and 11.03% for degraded data. These results have shown that using GA proceeded by UCN has led to considerable accuracy improvement compared with BFS base fusion.

6. In **2011,** Mezai et al **[40]** combined Speech and face matching scores using Dempster-Shafer Theory (DS), for person verification. This method which was widely used in classifiers fusion but it was little used in multimodal biometrics fusion. DS transforms the scores obtained from face and voice verification algorithms into evidences and then combines them. Their experiments were conducted on the XM2VTS Benchmark database, and the obtained results showed that the HTER of the proposed fusion varies from 0.433% to 2.875%. However the performances of the face and voice classifiers vary from1.88% to 6.22% and 1.148% to 6.208% respectively. The proposed method gave better performances compared to the likelihood ratio based fusion and the famous sum rule preceded by Z-score or Min-Max normalization, but it was outperformed by simple sum rule preceded by Tanh normalization.

7. In **2011,** Mehdi Parviz and M. Shahram **[57]** have proposed boosting-based multimodal biometric systems score fusion methods using AdaBoost and bipartite version of RankBoost abilities to optimize the Area under ROC Curve (AUC). They have investigated boosting based method not only as a classifier, but also as an algorithm to optimize AUC in multimodal biometrics.

In order to compare the performance of the two boosting-based fusion methods, the authors have selected three benchmark methods from each category. From transformation based methods, SUM rule with min-max normalization, from density based methods, GMM, and from classifier based methods, SVM. Their experimental results were conducted over XM2VTS and NIST databases and they have concluded that AdaBoost and RankBoost reach higher performance compared to Likelihood Ratio (LLR), SUM rule and Linear SVM. Furthermore, AdaBoost achieves performance comparable to that of RankBoost.

3.5 Conclusion and summary

This Chapter enabled us to introduce a theoretical review of certain number of multimodal biometrics fusion techniques. We have focused on biometrics fusion at the matching score level, dividing the existing fusion approaches into four main categories, classical, evolutionary hybrid intelligent and statistical approach. For the classical approach we have provided five fusion schemes namely product rule, sum rule, maximum rule, minimum rule and BFS. As an evolutionary approach we have presented two fusion strategies namely GAs and PSO. We have also introduced ANFIS classifier as a hybrid intelligent system and SVM classifier as a statistical approach.

Range normalization is needed to transform the matching scores into a common domain before combining them. Through this chapter, we have given a brief description about some effective and widely used range-normalization techniques, these techniques include min-max, z-score, decimal scaling, double sigmoid, median and tanh normalization schemes. We have seen that the min-max, decimal scaling and z-score normalization schemes are efficient, but are not robust to outliers. On the other hand, the median normalization scheme is robust but inefficient. Only the double sigmoid and tanh-estimators have both the desired characteristics.

We have also presented the principle and effectiveness of the UCN normalization process and its usefulness in suppressing the biometric scores for impostors in relation to those for the clients, so enhancing the accuracy of the biometric verification system.

By the end of this chapter, we have provided some recent works and investigations carried out to date in the field of multimodal biometric fusion.

In the next chapter, we will investigate and discuss the results in terms of EERs of applying some of the fusion techniques discussed in this chapter, and compare their performance in enhancing the accuracy of multimodal biometric system in either clean, varied and degraded data quality condition, using publicly available scores datasets.

Chapter

04

Experimental Setup and Results Discussion

***Abstract**: This Chapter experimentally investigates the effectiveness of PSO and GA algorithms as two evolutionary techniques for multimodal biometric sores level fusion using face and voice modalities. These two techniques are compared with BFS, ANFIS, and SVM fusion techniques. Firstly, this chapter provides an overview of some benchmark multimodal biometric databases, namely XM2VTS, TIMIT, NIST and BANCA. This chapter also describes the main steps followed to perform each of the five fusion techniques. Finally, based on the EERs obtained from the investigations carried out in this chapter, it reveals that in the case of using clean data, the two proposed evolutionary techniques works as expected in improving the performance of the fused biometrics, and in the case of using varied data, the 3rd degree SVM classifier results in the same EER as PSO and outperforms the GA algorithm. This chapter also shows that UCN offers considerable improvements to the accuracy of multimodal biometrics in clean, varied and degraded data conditions.*

***Résumé :** Ce chapitre étudie expérimentalement l'efficacité de PSO et GA comme deux techniques évolutionnaires pour la fusion biométrique multimodale du visage et la voix au niveau des scores. Ces deux techniques sont comparées aux BFS, ANFIS et SVM. Tout d'abord, ce chapitre donne un aperçu de certaines bases de données biométriques multimodales, à savoir XM2VTS, TIMIT, NIST et BANCA. Ce chapitre décrit également les principales étapes suivies pour réaliser chacune des cinq techniques de fusion. Enfin, en se basant sur les EERs obtenus à travers des différents testes effectués, ce chapitre révèle que dans le cas de l'utilisation des données propres, les deux techniques évolutionnaires proposées fonctionne comme prévu dans l'amélioration de la performance de la fusion des données biométriques, et dans le cas de l'utilisation de données variées, les résultats 3eme degré SVM classificateur donne le même EER que PSO et surpasse l'algorithme GA. Ce chapitre montre également que l'UCN offre des améliorations considérables à la précision de la biométrie multimodale dans les conditions propres, variés et dégradées.*

4.1 Introduction

In this chapter we will experimentally investigate the effectiveness of introducing two evolutionary based fusion techniques, namely PSO and GA into the enhancement of the accuracy and reliability of multimodal biometric system that combine face and voice biometrics scores in the recognition mode of verification and identification. The performance achieved by these two evolutionary methods will be compared to those achieved using a simple BFS technique, a hybrid intelligent technique (ANFIS) and a statistical learning method (SVM).

This chapter is divided into two main sections. In the first Section, we will describe the datasets used in our experimental investigations, and discuss the essential stages followed to implement each of the five techniques involved. In the second section, the performance of these fusion strategies will be evaluated and compared by the means of Equal Error Rate (EER), DET and ROC curves and under three different data quality conditions namely, clean, varied and degraded condition. Before fusing them, the scores must be mapped into the same range using the well-known Min-Max normalization technique.

To tackle to the problem of biometric data variation, UCN normalization process will be introduced to enhance the accuracy of multimodal biometrics under uncontrolled environments, so the fusion schemes are applied to the biometric scores with and without subjecting them to the UCN process.

4.2 Experimental Setup

In this section will present firstly, some publicly available (benchmark) datasets used for the performances evaluation and comparison of the selected biometric systems, and secondly we will present the parameters settings necessary to tune each technique involved in our multimodal biometric fusion systems.

4.2.1 Multimodal biometric Databases

Currently, many multimodal person authentication databases containing of information which allows the evaluation of multimodal biometric systems are reported in the literature, these are of utmost importance to define common benchmarks that enable consistent comparison of competing recognition strategies. In this section, the most important publicly available multimodal biometric databases will be briefly described.

4.2.1.1 BANCA Database

The **BANCA** database is a large, realistic and challenging multimodal database intended for training and testing multimodal verification systems **[51]**. The BANCA database was captured in four European languages and two modalities (face and voice). For recording both high and low quality microphones and cameras were used. The subjects were recorded in three different scenarios: controlled, degraded, and bad, over 12 different sessions, in a time distance of three months. An associated BANCA evaluation protocol is also available **[15]**.

4.2.1.2 XM2VTS Database

The **XM2VTS** database (extended M2VTS) was acquired in the context of the M2VTS project (Multi-Modal Verification for Teleservices and Security applications). The database contains speech and face images from 295 people. Every subject was recorded in four sessions over a period of four months.

The XM2VTS evaluation protocol specifies training, evaluation, and test sets, the training set is used to create client and impostor models for each person. The evaluation set is used to learn the verification decision thresholds. In case of multimodal systems, the evaluation set is also used to train the fusion manager. For both cases, the training set has 200 clients, 25 evaluation impostors, and 70 test impostors. The two configurations differ in the distribution of client training and client evaluation data **[15]**.

4.2.1.3 TIMIT Database

The **TIMIT** (Texas Instruments Massachusetts Institute of Technology) database allows identification to be done under almost ideal conditions.

The TIMIT database consists of 630 speakers, 70 % male and 30 % female from 10 different dialect regions in America. Each speaker has approximately 30 seconds of speech spread over ten utterances. The speech was recorded using a high quality microphone with no session interval between recordings **[37]**.

4.2.1.4 NIST Database

NIST Biometric Scores Set-Release 1 (BSSR1) is a set of raw output similarity scores from two 2002 face recognition systems and one 2004 fingerprint system, operating on frontal faces. And left and right index live-scan fingerprints, respectively. The release includes true multi modal score data, i.e., similarity scores from comparisons of faces and fingerprints of the same people. The data are suited to the study of score-level fusion-based multimodal, Multi-algorithmic, multi-sample and repeated-sample biometrics **[54]**.

4.2.2 Design and implementation

In this section, we will briefly define the programming languages used to implement our prototype. We will present the main interface of this prototype. The main steps necessary to perform and evaluate each fusion technique involved will be also explained.

4.2.2.1 Development Tools

To evaluate the performance of each technique involved, we use tow development languages, namely Borland **C++ Builder 6** and **Matlab**. The first one used for the design of the main interface, and the second one used for the selected fusion technique performing, the final results computing and the performance curves plotting.

1. **MATLAB**

MATLAB (MATrix LABoratory) is a high level language and interactive environment for scientific computations, algorithms development, data visualization and analysis and numerical calculation. MATLAB places at the disposal of the developer the fundamental operations (vector and matrix) necessary for the engineering problems. It allows a fast program development and execution.

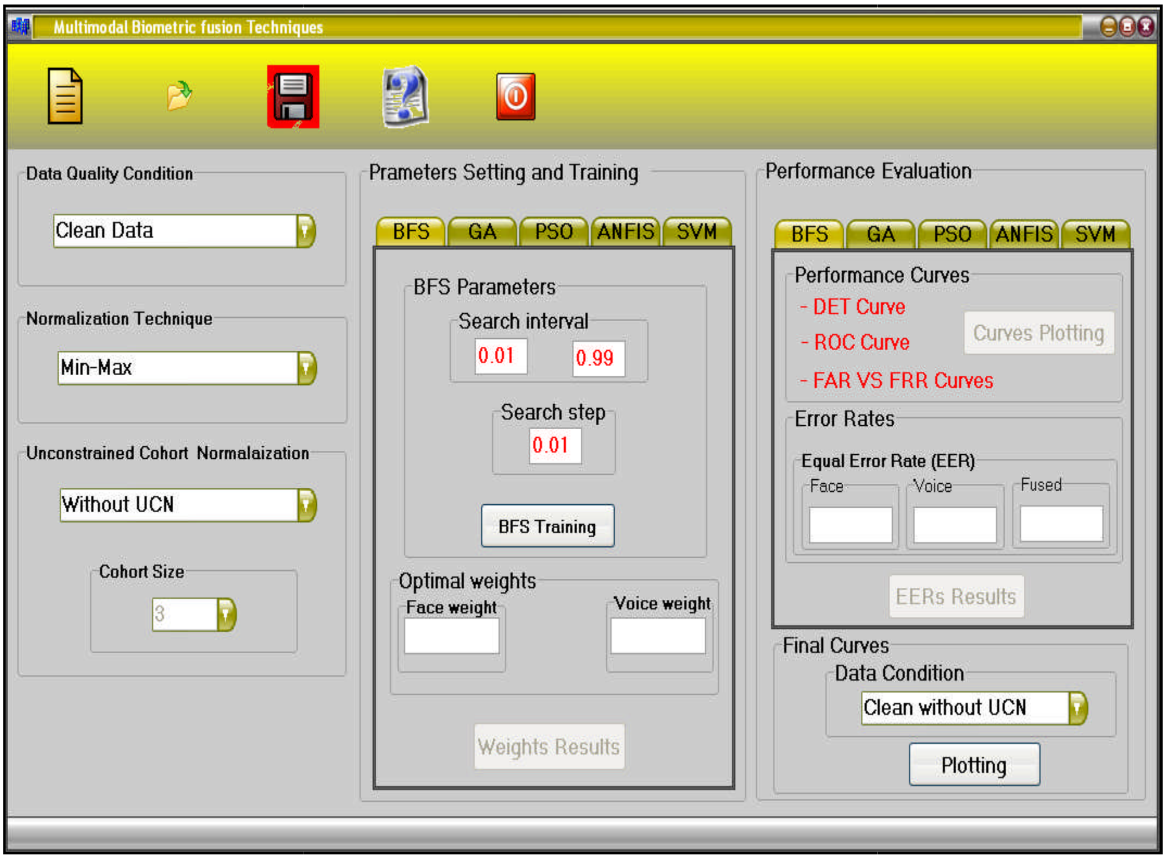
By using MATLAB, we can solve scientific computation problems more quickly than the traditional programming languages, because it is not necessary to carry out the low level programming tasks, like the variables declaration, the data type's specification and the memory allocation. MATLAB has excellent prototyping and plotting functionality contains convenient and very robust matrix operation packages **[09]**.

2. **Borland c++ builder 6**

C++ Builder is a rapid application development (RAD) product for writing C++ applications. Using C++Builder you can write C++ computer applications for the Microsoft Windows operating systems more quickly and more easily than was ever possible before. You can create Win32 console applications or Win32 GUI (graphical user interface) programs **[58]**. C++ Builder has Integrated Development Environment (IDE) to provide a friendly interface for creating computer programs.

4.2.2.2 The main interface of our prototype

In our experimentations, we have used C++ builder to create a convivial user interface that enable the user to use our prototype more easily and in a correct manner. We try to design an interactive interface that permits the user to deal with our fusion system, either by choosing the appropriate technique, setting its parameters, invoking Matlab and getting the final results.



Data Quality Condition: Clean Data

Normalization Technique: Min-Max

Unconstrained Cohort Normalaization: Without UCN

Cohort Size: 3

Search interval: 0.01 0.99

Search step: 0.01

Data Condition: Clean without UCN

Figure 4.1: The main interface of our Biometrics Fusion prototype.

4.2.2.3 The fusion process

Our fusion system is divided into two main phases, development (learning) phase and test phase. Before performing the fusion task, we have to choose the data condition and the normalization methods.

1. Selection of the data condition

In our experiments, the performance of each fusion technique is evaluated under three different data conditions, namely clean, varied and degraded data. The first and the second datasets are formed by using scores for clean face images together with scores for either clean or degraded utterances. The third one is based on the use of scores for degraded face images and degraded utterances. So firstly, we have to choose one of the following data qualities:

- **Clean data:**

The scores considered for the face and voice modalities were extracted from the **XM2VTS** (clean face images) and **TIMIT** (clean utterances) databases respectively. Using these biometric data sets, a total number of **140** client tests and **19460** (i.e., 140 x [140-1]) impostors tests is used for the development stage. The corresponding number of clients and impostors used in the testing phase for investigating the performance for the fusion schemes involved is **140** and **19460** respectively.

- **Varied data:**

The scores sets considered for the face and voice modalities were extracted from the **XM2VTS** (clean images) and the 1-speaker detection task of the **NIST** Speaker Recognition Evaluation 2003 (degraded speech) databases respectively. Using these data sets, a total number of **140** client tests and **19460** (i.e., 140 x [140-1]) impostors tests is used for the development stage. The corresponding number of clients and impostors used in the testing phase for investigating the performance for the fusion schemes involved is **140** and **19460** respectively.

- **Degraded data:**

The datasets considered for the face and voice modalities in this investigation are extracted from the **BANCA** and **NIST** Speaker Recognition Evaluation 2003 databases respectively. Using these biometric datasets, a total of 26 subjects have been used for the experiments. The face recognition scores are obtained based on images captured in four sessions, and affected by two different forms of distortion **[54]**. Based on these and the corresponding score data for NIST, a development score dataset is formed for the experiments. This consists of **104** client tests and **2600** (i.e. 4 x {26 x (26-1)}) impostors tests. The corresponding number of client and non-client tests used in investigating the performance for the proposed schemes is **104** and **2600** respectively.

2. Selecting the normalization technique

The development and the test scores must be mapped into the range [0, 1], for this purpose, scores are introduced to the **Min-Max** normalization technique.

After the normalization process, the fusion is performed either with or without subjecting the normalized scores to the **UCN** process. In the case of choosing UCN method, the cohort size must be predetermined, it takes three different values: 1, 2 or 3.

3. The development stage

In this stage the development scores are used to compute or to tune the appropriate parameters necessary for each fusion method involved (PSO, GA, BFS, ANFIS and SVM). These parameters are then saved to be used in the test phase. In our experiments, each fusion technique was trained using the following parameters:

- **BFS**

Before starting the BFS training, two main parameters must be adjusted, the **min** and **max** values of the search interval (search space) from which the weights will be taken, and the search **step** which determine the number of values that will be taken from this selected interval.

In our study, in order to perform the BFS algorithm, we set the min value to **0.01**, the max value to **0.9** and the search step to **0.01**.

- **GA**

To run our genetic algorithm, we have four parameters that must be predetermined. The **population size**, which refers to the number of initial chromos (weights in our problem) that will be randomly generated to calculate the fused, scores (fitness functions). The **Max generation** is the stopping criteria which determine the maximum number of generations the genetic algorithm runs for. Finally we have the **crossover** fraction which specifies the fraction of each population, other than elite children, that are produced by crossover. and the mutation rate which represents the probability Rate to mutate an individual selected to be mutated.

In this experimental study, we set the population size to **100,** the Max generations to **100,** the single point crossover rate to **0.8** and the uniform mutation rate to **0.01.**

- **PSO**

Particle Swarm Optimization algorithm has a number of parameters that determine its behavior and effectiveness in optimizing the fusion problem, from these parameters we can find: **The swarm size** which represents the number of particles in the search space. **The iterations number** which refers to the stopping condition or criterion and determines the maximum **number** of iterations the PSO algorithm runs for. **The inertia weight (ω)** which can be used to control the PSO's speed. **The acceleration constants c_1** and **c_2**, also called the learning factors, where the first represents the maximum step size towards the personal best position while the second is the maximum step size towards the global best position in just one iteration.

To evaluate and test the performance of the PSO algorithm the swarm size was set to **7**, the iteration number was set to **30,** the inertia weight was set to **1** and the acceleration constants was fixed **as $c_1=c_2=2$**.

- **ANFIS**

To set the stopping criteria for the ANFIS training, the number of training **Epochs** and the training **Error Tolerance** must be predetermined, so the training process stops whenever the maximum epoch number is reached or the training error goal is achieved. In our test the epoch number was set to **10** and the error goal was set to **0.**

- **SVM**

The SVM classifier was trained using a **linear kernel** function and the optimal hyperplane was found using the **quadratic programming** (QP) method.

Once the training has finished, it returned a model containing information about the trained support vector machine (SVM) classifier.

4. The verification and test stage

To test and evaluate the performance and accuracy of **BFS**, **GA** and **PSO** as score-level fusion techniques, the optimal weights (face and voice weights) obtained in the development stage will be used to perform an optimized weighting fusion scheme at this stage.

For the same purpose, **ANFIS** and **SVM** classifiers will respectively use the ANFIS structure and SVM model respectively obtained in the development stage to classify the normalized test scores.

To evaluate the performance and accuracy of each fusion technique evolved in this experimental study, the results obtained in terms of EERs, DET and ROC curves will be shown at this verification stage.

In order to experimentally investigate and compare the performance and reliability of each biometrics fusion technique involved in this study, the main stages followed are represented in the following flowchart:

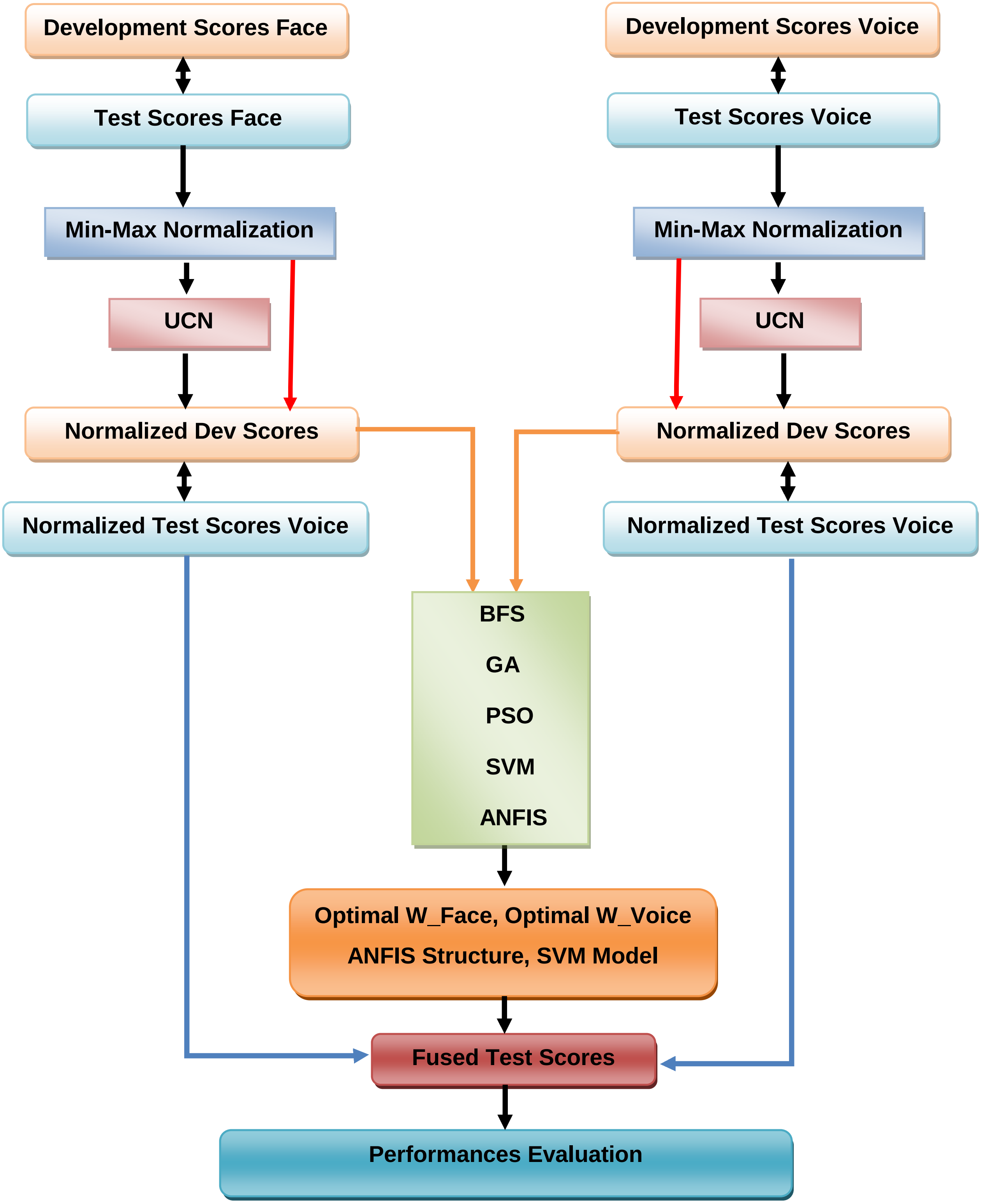


Figure 4.2: Multimodal biometric score-level fusion flowchart.

4.2.3 Results and Discussions

In this section, the performance of each technique involved will be discussed and compared using a commonly used biometric performance evaluation criteria discussed in chapter two. We will use the Equal Error Rate (EERs), the lower the EER is the better are the system's performances achieved, To represent, visualize and directly compare the performance of all fusion technique involved, two performance curves will be used, namely DET and ROC curve.

4.2.3.1 Fusion under clean data condition

In this section, the purpose of the experiments is to investigate the performance and efficiency of the two evolutionary based fusion techniques involved (GA and PSO) along with the three other fusion schemes discussed previously (SVM, BFS and ANFIS) in enhancing the accuracy and reliability of multimodal biometric fusion when the biometric scoresets was obtained in a clean data conditions (free from degradation).

Table 4.1 shows the Equal Error Rates (EERs) obtained for the verification experiments using the two individual biometric scores (face and voice) and their fusion using the five different above mentioned fusion schemes. Before combining them, the scores were mapped into the same range (**[0, 1]**) using the Min-Max normalization scheme, after that, each fusion technique was performed with and without subjecting the scores to the UCN normalization process.

Method EER (%)	Face (XM2VTS)	Voice (TIMIT)	GA	PSO	ANFIS	BFS	SVM
Without UCN	3.57	2.55	0.04	0.03	0.71	0.05	2.09
With UCN	1.43	0.00	0.00	0.00	0.00	0.00	0.30

Table 4.1: Results on the clean data at the Equal Error Rate (EER).

In general, Comparing the results showed in the second line from **table 4.1**, it can be seen that fusing the scores leads to a significant improvement in the verification accuracy (EERs), either by using the two evolutionary techniques (GA and PSO) or the three others:

simple BFS, hybrid intelligent (ANFIS) and statistical learning method (SVM). These fusion methods results in EERs which are better than the best single modality involved (the face with EER equal to **3.57%**). This improvement in performance is significant and it underscores the benefit of multimodal biometrics systems.

We also notice that there was no considerable difference between the verification results obtained by using each of the five fusion techniques concerned. All the EERs obtained were satisfactory (very small or equal to zero), and this explains the effect of the data condition (clean) on the accuracy and reliability of the biometric system.

It is clearly seen that the application of the evolutionary approach based fusion methods, namely GAs and PSO as a fusion technique at the matching score level results in better EERs (**0.04%** and **0.03%** respectively), the reason for such significant results offered by these two population based techniques is shown to be due to their capability as an optimization techniques in exploring the whole searching space, finding the optimal solutions (face and voice weights in this case) without worrying about the local minima and in converging rapidly to the global best solution.

PSO is an efficient algorithm in converging toward the best solutions, and GA is able to converge away from bad ones **[67]**.

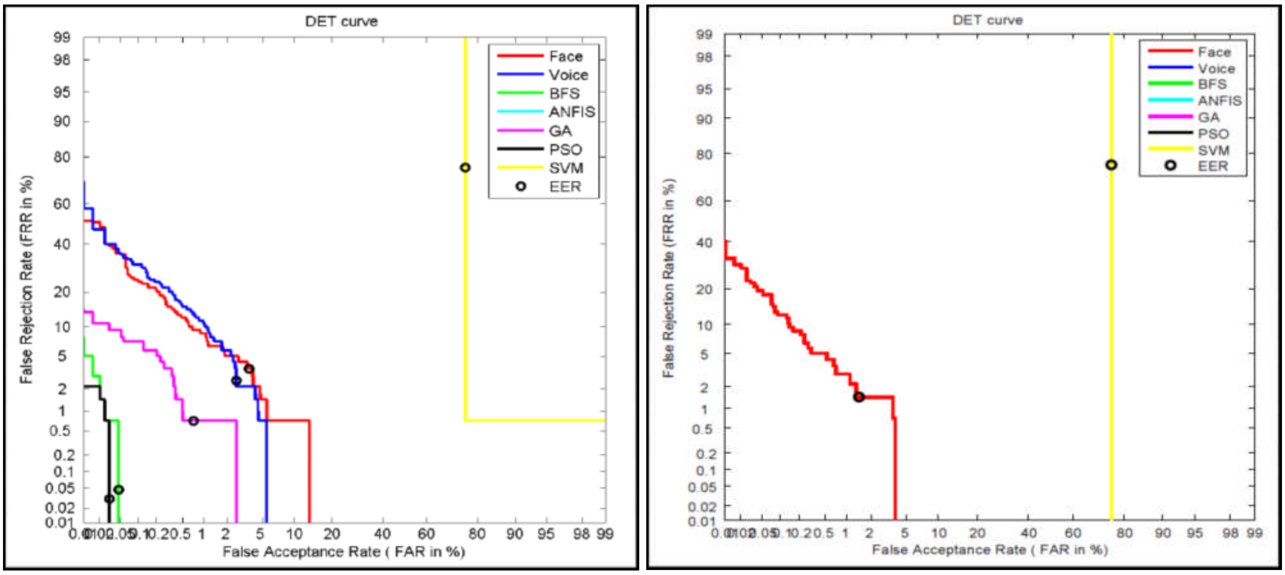
It can be also seen that using the simple BFS as a fusion process results in an acceptable error rate (**0.05%**) compared to two other hybrid intelligent (ANFIS) and statistical (SVM) techniques. It is difficult to explain this result, but it might be related to the ability of this simple BFS algorithm in exploring the whole search interval in an exhaustive manner.

It is obvious that the worst result so far was obtained using linear SVM (**2.09%**), and a possible explanation for this might be that using third degree polynomial SVM is not suitable to find the optimal separating hyperplane in such a case, so the testing scores (clients and impostors) were not separated effectively. Another possible fact behind such findings is the insufficient memory of the PC used to perform SVM classifier (3Go). I was obliged to divide the scoreset into two subsets, and use only one subset to evaluate the performance of SVM classifier.

Moreover, it is observed that the application of UCN normalization process is beneficial even under clean data condition, where there is no variation effect. UCN has resulted in reducing the verification EERs for the single modalities and for multimodal biometric. The EER was even reduced to zero for the first four fusion schemes (BFS, GA, PSO and ANFIS) considered and for the voice verification, and was considerably reduced for the SVM method.

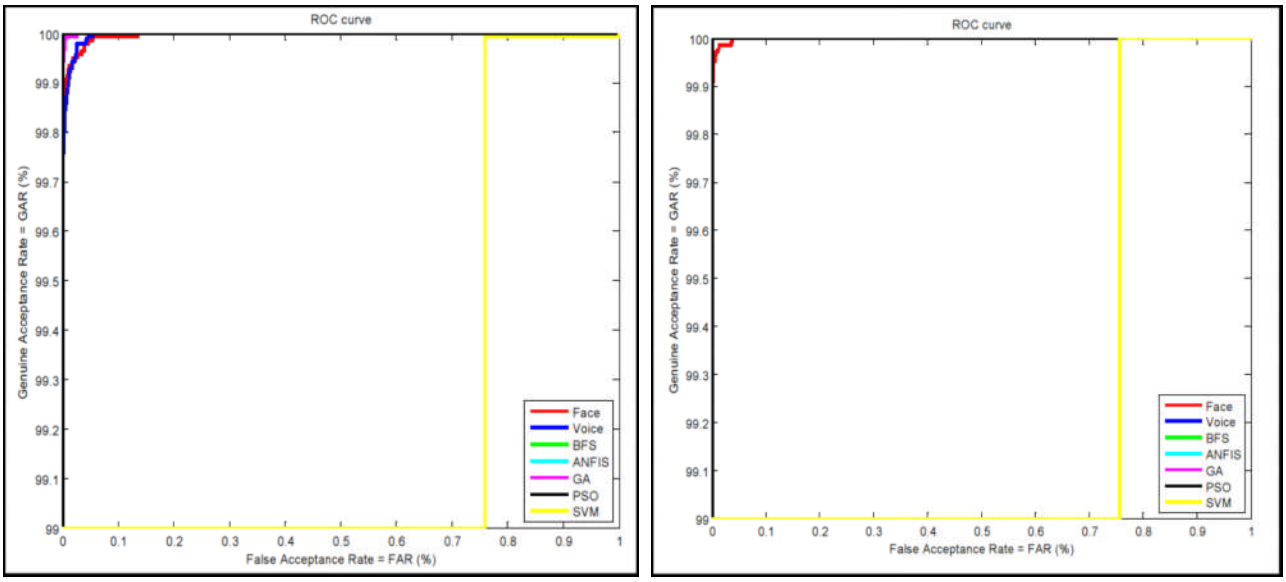
This effectiveness of UCN under clean data condition is due to their ability to suppress the scores for impostors in relation to those for true users and its performance with the voice modality. However, the corrective effect that UCN have on the face modality is seen to be also considerable **[19]**.

Figure 4.3 and **Figure 4.4** Show the DET and ROC curves respectively, visualizing and comparing the tow single modalities (face and voice) together with the five fusion schemes involved under clean data quality condition, with and without subjecting the scores to the UCN normalization procedure.



(a) **(b)**

Figure 4.3: (a) DET curves for different fusion techniques under clean data quality condition without UCN. **(b)** DET curves for different fusion techniques under clean data quality condition with UCN.



(a) **(b)**

Figure 4.4: (a) ROC curves for different fusion techniques under clean data quality condition without UCN. **(b)** ROC curves for different fusion techniques under clean data quality condition with UCN.

From the DET curves presented in figure 4.3, it can be noted that in order to have a minimal error rate, the principal goal of biometric matcher is to make bring the curve closer to the point corresponds to (0, 0), hence, more the curve is close to this point, more reliable the biometric system is. In the ROC curves presented in figure 4.4, the optimal point is at the upper left of the plot, and the curves related to the well performing systems tend to bunch together near this corner **[68]**.

According to these two curves, it is clear that the single biometrics are always outperformed by their multimodal equivalents. It can be seen that most of the fusion techniques (BFS, PSO, ANFIS and GA) achieve better performance compared with the single biometrics.

The curves presented in figure 4.3(b) and figure 4.4(b) illustrate the considerable performance improvements achieved through the use of UCN process, either with the single modalities or the five fusion techniques involved in this study. It is also observed that we cannot see the DET curves related to voice modality, GA, ANFIS, PSO, BFS, and this is due to their EERs that are equal to 0%.

4.2.3.2 Fusion under Varied Data condition

In this section, the purpose of the experiments is to investigate the effectiveness of the five fusion techniques involved in enhancing the performance of multimodal biometric fusion when the qualities of the biometric datasets are in different conditions (clean and degraded).

Table 4.2 shows the Equal Error Rates (EERs) obtained for the verification experiments using the two single biometric scores and their fusion using the five different above mentioned fusion schemes (GA, PSO, ANFIS, BFS and SVM). Before combining them, the scores were mapped into the same range (**[0, 1]**) using Min-Max normalization scheme, after that, each fusion technique was performed with and without subjecting the scores to the UCN normalization process.

Method EER (%)	Face (XM2VTS)	Voice (NIST)	GA	PSO	ANFIS	BFS	SVM
Without UCN	**3.57**	**31.43**	**3.34**	**2.91**	**3.17**	**3.05**	**2.91**
With UCN	**1.43**	**10.71**	**0.71**	**0.71**	**1.43**	**1.43**	**0.85**

Table 4.2: Results on the varied data at the Equal Error Rate (EER).

From **table 4.2**, it should be pointed out that the EER obtained for the face modality is exactly the same as in the previous experiment, but due to the use of degraded voice scores, the verification accuracy for the voice modality has been decreased.

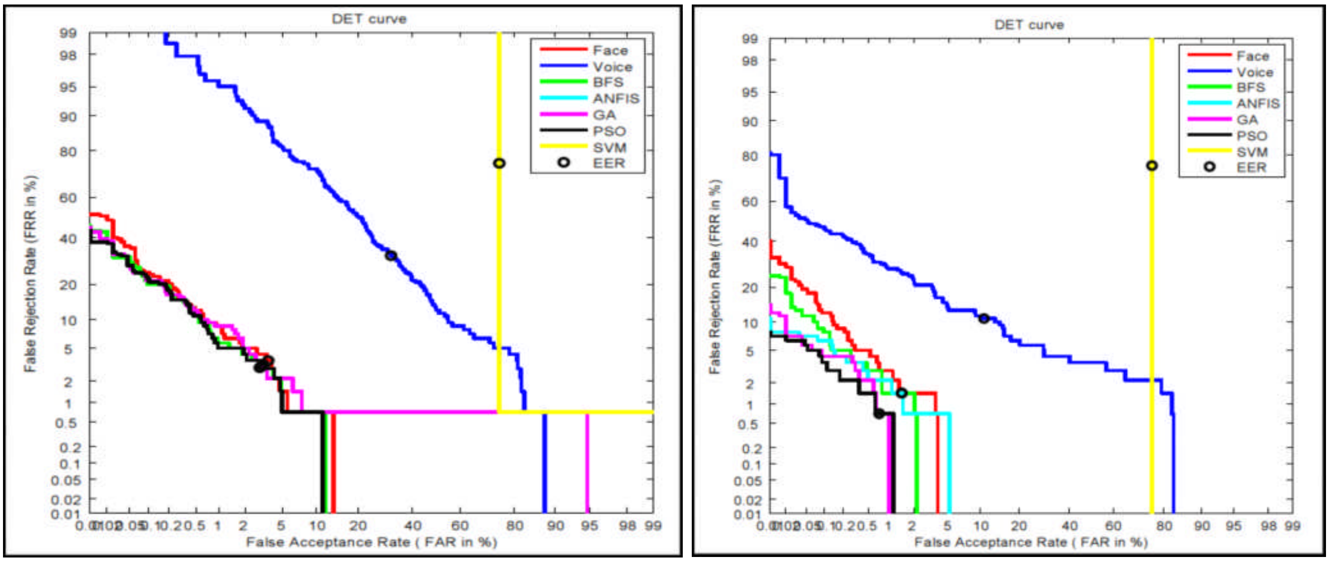
Moreover, it is clearly seen that fusing the scores using each of the five methods considerably improve the performance of the biometric system, and this can be explained by the fact that, multimodal biometric systems improve the verification accuracy compared to its unimodal counterpart even under varied scores, and this benefit can be achieved from the complementary information of the combined modalities, which confirms the concept**[69]** that the information obtained from different modalities complement each other. In this case, the clean face data complement the degraded voice data.

It can also observed that using PSO as an evolutionary fusion scheme under varied data is still beneficial and results in the best EER value (**2.91%**), but GA technique was outperformed by the other three techniques (SVM, ANFIS and BFS). However, when the fusion process accomplished with subjecting the biometric scores to UCN, both GA and PSO result in the best EER (**0.71%**).

It can be seen also that the EER (**2.91%**) obtained using third degree polynomial SVM classifier is comparable to those obtained using PSO algorithm, and this confirm the findings of some earlier studies reporting it as one of the most effective methods for multimodal biometric fusion **[11]**.

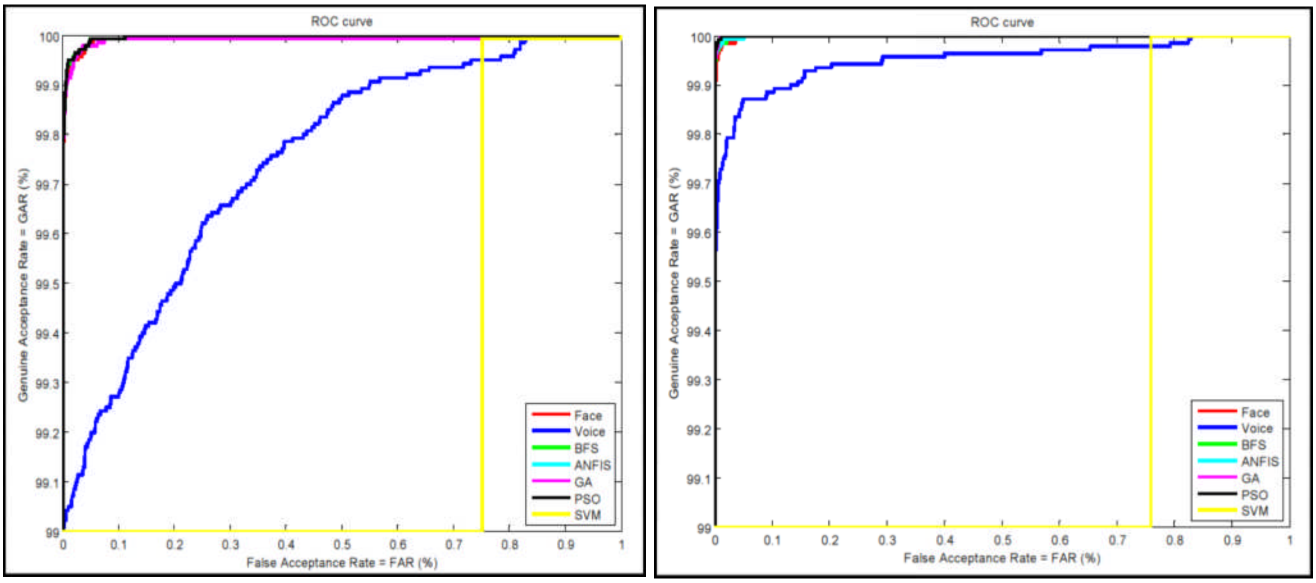
From the third line of **Table 4.2,** it can be seen that the use of UCN has again resulted in the reduction of the verification EERs for the individual modalities as well as for the fused biometrics. This usefulness UCN is due to its performance with the voice modality (degraded), and its capability to enhance the client scores affected by data degradation, and suppressing the impostor scores in relation to the client ones.

Figure 4.5 and **Figure 4.6** Show the DET and ROC curves respectively, visualizing and comparing the tow single modalities (face and voice) together with the five fusion schemes involved under varied data quality condition, with and without subjecting the matching scores to the UCN normalization procedure.



(a) **(b)**

Figure 4.5: (a) DET curves for different fusion techniques under varied data quality condition without UCN. **(b)** DET curves for different fusion techniques under varied data quality condition with UCN.



(a) **(b)**

Figure 4.6: **(a)** ROC curves for different fusion techniques under varied data quality condition without UCN. **(b)** ROC curves for different fusion techniques under varied data quality condition with UCN.

Figure 4.5(a) and figure 4.6(b) clearly show that multimodal biometrics still provide higher accuracy compared to its unimodal counterpart, even under varied data condition.

Figure 4.5(b) and figure 4.6(b) clearly show the significant increase in the reliability of fused biometrics obtained through the use of UCN. The plots in this figure also illustrate the considerable performance improvements achieved through the use of UCN with the individual modalities, which is the cause of the above mentioned enhancement in the accuracy of fused biometrics.

4.2.3.3 Fusion under Degraded Data condition

In this section, the purpose of the experiments is to investigate the effectiveness of the five fusion techniques in enhancing the performance of multimodal biometric fusion when the biometric datasets are in degraded condition.

Table 4.3 shows the Equal Error Rates (EERs) obtained for the verification experiments using the two individual biometric scores and their fusion using the five different above mentioned fusion schemes. Before combining them, the scores were mapped into the same range (**[0, 1]**) using Min-Max normalization scheme, after that, the fusion was performed with and without subjecting the matching scores to the UCN process.

Method EER (%)	Face (BANCA)	Voice (NIST)	GA	PSO	ANFIS	BFS	SVM
Without UCN	**45.19**	**26.92**	**27.23**	**27.62**	**34.62**	**27.19**	**48.00**
With UCN	**43.27**	**23.92**	**23.88**	**22.12**	**30.77**	**23.85**	**47.03**

Table 4.3: Results on the degraded data at the Equal Error Rate (EER).

Based on the results showed in table 4.3, it can be observed that using degraded face database leads to a considerable reduction in the accuracy of the face verification relative to the corresponding one in the previous sections.

From this table, it is quite apparent that without subjecting the scores to the UCN process, fusion methods such as GA, PSO and BFS result in unexpected EERs, which are worse than the best individual modality involved (voice with EER equal to **26.92%**). Hence, under such biometrics data condition (highly degraded), it is preferable to use the best single modality (Voice in this case) alone, rather than multimodal biometric solutions. Based on these results, along with those obtained in **[14]**, it is clear that the fusion strategies may not necessarily lead to the improvement of the verification accuracy offered by the best single modality involved.

It can be also seen in table 4.3 that using third-degree polynomial SVM as a fusion scheme leads to an EER which is worse even than the worst single biometric classifier (face with EER equal to **45.19%**), and this catastrophic EER value can be explained by the condition under which the scores are integrated. The degraded biometric data may not be separated using SVM classifier with polynomial kernel function.

It can be seen from the second line of table 4.3 that the use of UCN has again resulted in the reduction of the verification EERs for the individual modalities as well as for the fused biometrics. UCN achieves this by a combination of enhancing the client scores when these are affected by data degradation.

These results are in agreement with the earlier suggestions **[14]** that the use of UCN in degraded data conditions is beneficial.

The effectiveness of UCN under degraded conditions is due to its two major characteristics. Firstly it is an efficient mean in enhancing the scores when the test data is degraded, and secondly, it suppresses the scores from impostors in relation to those for clients **[18]**.

Figure 4.7 and **Figure 4.8** Show the DET and ROC curves respectively, visualizing and comparing the tow single modalities (face and voice) together with the five fusion schemes involved under degraded data quality condition, with and without subjecting the scores to the UCN normalization procedure.

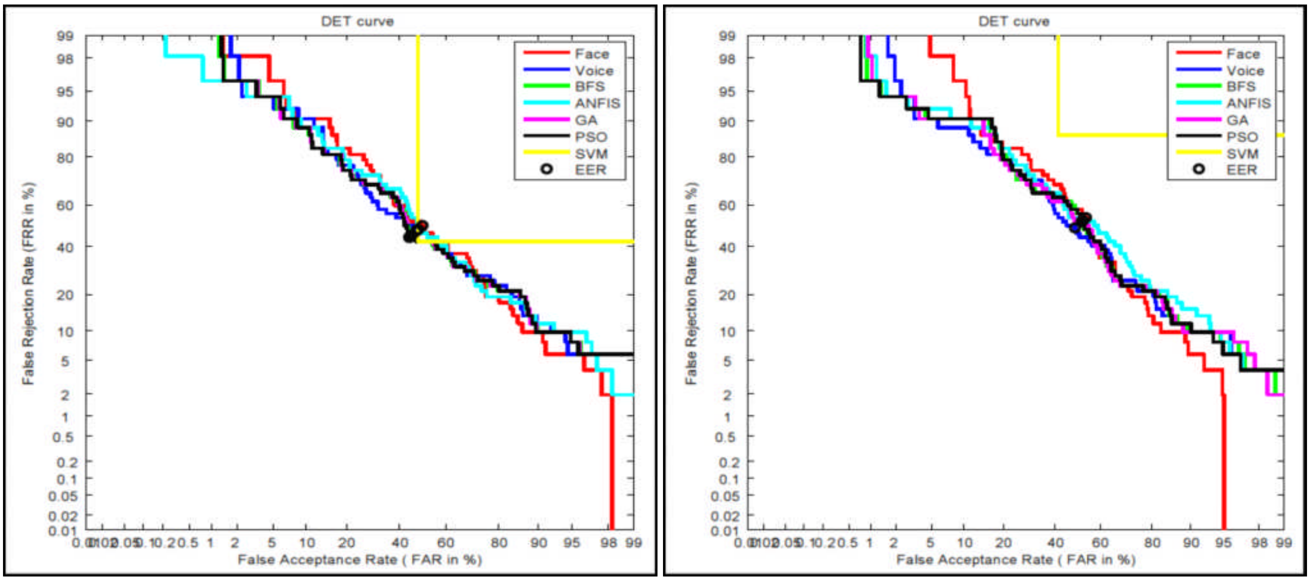
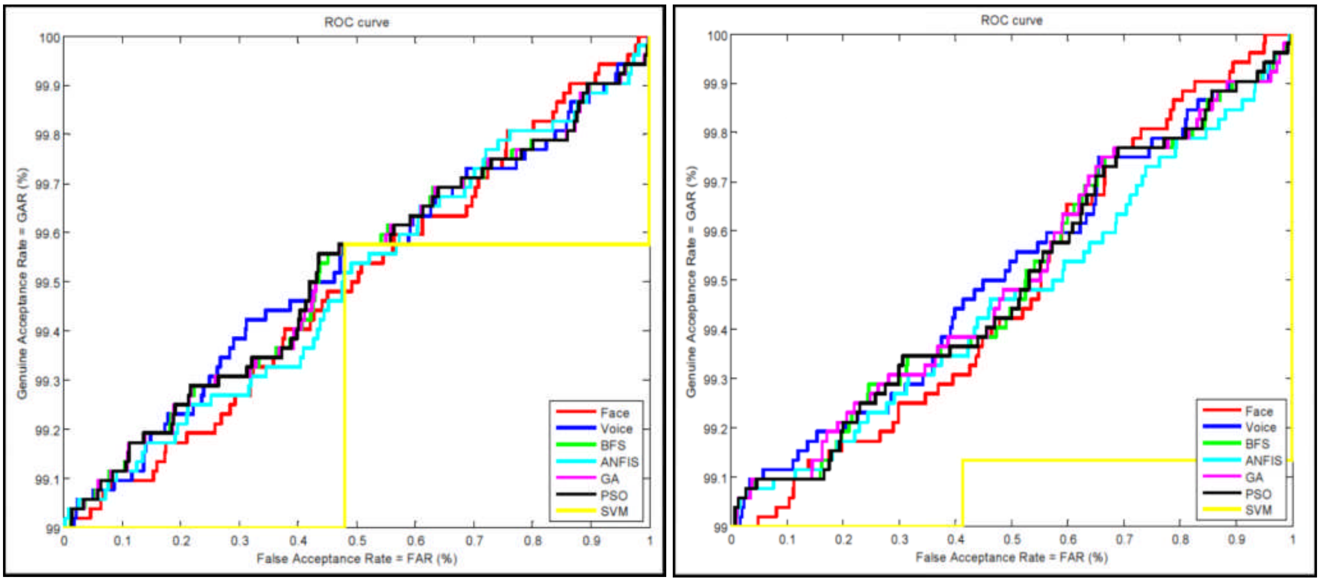


Figure 4.7: (a) DET curves for different fusion techniques under degraded data quality condition without UCN. **(b)** DET curves for different fusion techniques under degraded data quality condition with UCN.



(a) **(b)**

Figure 4.8: (a) ROC curves for different fusion techniques under degraded data quality condition without UCN. **(b)** ROC curves for different fusion techniques under degraded data quality condition with UCN.

The DET and ROC plots in Figure 4.8 and Figure 4.8 respectively further emphasize the role of UCN in enhancing the robustness of our fused biometrics. In fact, it is observed that all fusion techniques involved did not work as expected, because the fused biometrics accuracy is highly influenced by the worse of the two modalities involved and does not even match the performance of the better of the two individual modalities. However, by applying UCN to the individual modalities, the accuracy is slightly improved.

4.3 Summary and Conclusion

In this chapter, we have experimentally investigated the effectiveness of introducing PSO and GA algorithms as two evolutionary techniques into multimodal biometric sores level fusion using face and voice modalities. These two techniques was compared with a simple BFS, a hybrid intelligent (ANFIS) and a statistical learning (SVM) fusion techniques.

Firstly, we have provided an overview of the main existing multimodal biometric databases, in particular, the databases used in this Thesis namely, XM2VTS, TIMIT, NIST and BANCA. We have briefly presented the programming languages used to implement our prototype. These languages include Borland c++ builder and Matlab, the first was used to design our main interface and the second was used to perform the fusion techniques involved and calculate the evaluation criteria (EER, ROC and DET curves).

We have fully described the main steps followed to perform each of the five fusion schemes, starting with the selection of the biometrics data quality condition (Clean, Varied or degraded), selecting Min-Max as a rang-normalization technique and choosing whether the normalized scores will be subjected into UCN normalization process or not, the cohort size (1, 2 or 3) must be determined if the scores will be subjected to UCN.

Then, as any biometric system, two main stages were followed to perform each fusion technique involved, the development stage and the test stage. In the development stage, the parameters necessary to perform each fusion scheme are adjusted, in the test stage the verification accuracy of each method was evaluated and compared.

Based on the above investigations carried out under three different data conditions, it can be concluded that, in the cases of clean data, the two proposed evolutionary technique works as expected in enhancing the performance of our multimodal biometric system, they result in the best EERs. Nevertheless, in the case of varied data, the third degree polynomial SVM outperforms the GA algorithm and results in the same EER as PSO. Based on the experimental investigations, it has been shown that UCN offers considerable improvements to the accuracy of multimodal biometrics in clean, varied and degraded data conditions.

Conclusion and Future Work

1. Conclusion

Multimodal Biometric systems combine multiple source of information from different biometric traits to achieve better performances and overcome the limitations of unimodal biometric systems. Various fusion levels and scenarios are possible in multimodal system. It is however, reported in the literature that fusion strategies work better at the matching score level.

This Thesis, Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) has been proposed as two evolutionary techniques for combining data obtained from face and voice modalities. Before combining them, the scores were mapped into the same range using the well-known Min-Max normalization process.

To investigate the effectiveness of the suggested approach, the performance achieved using the two evolutionary techniques was compared with those obtained using a simple BFS, ANFIS as a hybrid intelligent technique and SVM as a statistical learning technique. The validity of the five techniques involved in this study was demonstrated considering three different criteria (EER, ROC curves and DET curves) at the state-of-the-art of biometric performance evaluation.

Another issue of concerns in this thesis is the effect of the data variation on the verification performance of the biometric systems. Such variations are reflected in the corresponding biometric scores. Therefore, in this thesis, UCN has been presented as a Normalization scheme to reduce the effects of data degradation in multimodal fusion.

After giving the background and motivation of this Thesis in the general introduction, chapter 1 introduced the basic of biometrics systems, and multimodal biometrics. Some general tools for performance evaluation of biometric systems were presented in Chapter 2. In chapter 3, the proposed techniques and some state-of-the-art fusion methods were theoretically presented and illustrated. By the end of this chapter some recent works and investigations carried out in the area of multimodal biometric fusion were provided.

In chapter 4, our tests, carried out on five well-known multimodal biometric databases (XM2VTS, TIMIT, NIST and BANCA). Based on the experimental results presented in this chapter, it has been concluded that:

- Higher accuracy is the basic advantage of multimodal biometrics over unimodal biometrics.
- Our proposed evolutionary based fusion techniques provided a considerable performance gain over the other fusion techniques particularly in the case of using clean data.
- The use of 3rd degree polynomial SVM is a very performing, promising and resulted in the same EER as GA fusion technique.
- Subjecting the scores to UNC normalization process, reduced the effects of data variation and reduced the EERs for both single biometrics and multimodal biometrics fusion under clean, varied and degraded conditions.

2. Recommendations for Future Work

Based on the findings of this thesis, the following research directions and recommendations appear promising in our future work:

- Ant Colony Optimization (ACO) algorithm is another evolutionary technique that had never been introduced into multimodal biometric fusion, using such technique for the weighting fusion schemes optimization may result in the reduction of the verification error rates.
- A hybrid (GA/PSO) algorithm, may lead to the improvement of the verification accuracy of our multimodal biometric system by combining the strengths of particle swarm optimization with genetic algorithms. The hybrid algorithm combines the velocity and position update rules of PSOs with the ideas of selection, crossover and mutation from GAs.
- The Algerian government intends for the biometric passport which contain a contactless smart card chip that holds a digitized photo, fingerprints and signature. Fusing the matching scores obtained from each of the three single modality, May reduce the verification error rates.
- A good compromise between computational costs of the algorithm and the overall performance is strongly needed. There are several approaches that can be used to speed up the system computation without sacrificing its performance.

References

[01] A. Rahmoun, F. Alsaade, ***A Method to enhance multimodal biometrics using neural networks and genetic algorithms***, In Proceeding of International Conference Signal and Image Processing (SIP), 2009.

[02] A.Rahmoun, F. Alsaade, M. Zahrani, ***On Improving Multimodal Biometrics Verification Using Genetic Algorithms***, In Proceeding of the 3rd International Conference on E-Medical Systems, E-Medisys'10, Fes, Morocco, May 2010.

[03] G. Kumar, M. Imran, ***Research Avenues in Multimodal Biometrics,*** In International Journal of Computer Applications, Volume RTIPPR, Issue 1, pp. 1-8, 2010.

[04] A.K. Jain, P. Flynn, A. Ross, ***Handbook of Biometrics,*** Springer, New York, USA, 2008.

[05] J. Fierrez-Aguilar, ***Adapted Fusion Schemes for Multimodal Biometric Authentication***, PhD Thesis, University of Madrid, 2006.

[06] N. Poh, S. Bengio, ***Database, protocols and tools for evaluating score-level fusion,*** Pattern Recognition, Volume 39, Issue 2, pages 223–233, 2006.

[07] A. Jain, K. Nandakumara, A. Ross, ***Score normalization in multimodal biometric systems ,***In Pattern Recognition, volume 38 Issue 12, pp.2270-2285, Jan. 2005.

[08] L. Allano**, *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles,*** PhD thesis, Institut National des Télécommunications, 2009.

[09] M. Elhaddad M. Benamar, ***Conception et réalisation d'une plateforme biométrique multimodale basée sur la fusion en scores,*** Engineering thesis, INI, Alegria, Septembre 2008.

[10] A.Ross, K.Nandakumar, and A.K. Jain, ***Handbook of Multibiometrics,*** Springer Heidelberg edition, New York, USA, 2006.

[11] B.Gutschoven, P.Verlinde, ***Multi-Modal Identity Verification using Support Vector Machines (SVM)***, Proc. of the 3rd Intl. Conf. on Information Fusion, 2000.

[12] F. Karray, J. A. Saleh, M. N. Arab and M. Alemzadeh, ***Multi Modal Biometric Systems: A State of the Art Survey***, Fourth International Conference on Computational Intelligence, Robotics and Autonomous Systems, New Zealand, Nov. 2007.

[13] A. Ross, A.K. jain, ***Information Fusion In Biometrics***, In Pattern Recognition Letters , Volume 24 ,Issue 13, pp. 2115-2125, Sep. 2003.

[14] F. Alsaade, ***Score-Level Fusion for Multimodal Biometrics***, PhD thesis, University of Hertfordshire, United Kingdom, 2008.

[15] M. Faundez-Zanuy, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, ***Multimodal Biometric Databases: An Overview***, IEEE Aerospace and Electronic Systems Magazine, Volume 21, Issue 8 Pages: 29 – 37, Aug. 2006.

[16] R. Snelick, U. Uludag, A. Mink, M. Indovina, A.K. Jain**, *Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems*,** IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, pp. 450-455, 2005.

[17] C. Yan-Ying and L. Shang-Hong, ***Audio-Visual Information Fusion for SVM-Based Biometric Verification*,** In the 9th International Workshop on Cellular Neural Networks and Their Applications, pp. 300 -303, May 2005.

[18] F. Alsaade, ***Enhancement of Multimodal Biometric Systems Using an Improved Unconstrained Cohort Normalisation*,** Scientific Journal of King Faisal University (Basic and Applied Sciences), Vol. 11 ,No. 1 , 2010.

[19] F. Alsaade, M. Ariyaeeinia, A. S. Malegaonkar, M. Pawlewski, and S. G. Pillay, ***Enhancement of multimodal biometric segregation using unconstrained cohort normalization***, In Pattern Recognition, Volume 41, Issue 3, pp.814-820, 2008.

[20] Q. Bai, ***Analysis of Particle Swarm Optimization Algorithm*,** Computer and Information Science, Vol 3, No 1, Feb. 2010.

[21] K. Veeramachaneni, L. A. Osadciw, and P. Varshney, ***An Evolutionary Algorithm Based Approach for Dynamic Thresholding in Multimodal Biometrics*,** In Proceedings of First International Conference on Biometric Authentication, pp. 671-677, Hong Kong, July 2004.

[22] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, ***Fusion Strategies in Multimodal Biometric Verification,*** Proceedings of the IEEE International Conference on Multimedia and Expo, ICME ’03, pp. 5 - 8, 2003.

[23] P. Tahmasebi, A. Hezarkhani, ***Application of Adaptive Neuro-Fuzzy Inference System for Grade Estimation; Case Study, Sarcheshmeh Porphyry Copper Deposit, Kerman, Iran,*** Australian Journal of Basic and Applied Sciences, 4(3): pp. 408-420, 2010**.**

[24] M. Mitchell, ***An Introduction to Genetic Algorithms***, MIT Press edition, February 1998.

[25] A.K. Jain, R. Bolle and S. Pankanti, ***BIOMETRICS: Personal Identification in Networked society,*** Kluwer Academic Publishers, 1999.

[26] F. Alsaade, A. Ariyaeeinia, A. Malegaonkar and S. Pillay, ***Qualitative fusion of normalized scores in multimodal biometrics***, Pattern Recognition Letters, Volume 30, Issue 5, Pages 564‑569, 2009.

[27] R. C. Eberhart and Y. Shi, ***Particle swarm optimization: developments, applications and resources***, Proceedings of IEEE Congress on Evolutionary Computation 2001 IEEE service center, Piscataway, NJ, Seoul, Korea, 2001a.

[28] A. K. Jain and A. Ross, ***Multibiometric Systems,*** Communications of the ACM, Special Issue on Multimodal Interfaces , Vol. 47, No. 1, pp. 34-40, January 2004.

[29] C. Sanderson, K. K. Paliwal, ***Information Fusion and Person Verification using speech and face information,*** Research Paper IDIAP-RR 02-33, IDIAP, September 2002.

[30] R. J. Jyh-Shing, ***ANFIS: Adaptive-Network-Based Fuzzy Inference System,*** in IEEE Transactions on Systems, Man and Cybernetics, Volume 23, Issue 3, pp 665 – 685, 1993.

[31] C. G. Andrade, ***Investigation and Comparing Multimodal Biometric Techniques***, Master thesis at the University of Johannesburg, 2002.

[32] R. J. Jyh-Shing, ***Neuro-Fuzzy Modeling Architectures, Analyses and Applications,*** PhD thesis, University of California, Berkley, USA, July 1992.

[33] A. J. Mansfield, J. L. Wayman***, Best Practices in Testing and Reporting Performance of Biometric Devices,*** Version 2.01, Report, Biometrics Working Group, UK, Aug. 2002.

[34] V. N. Vapnik, ***Statistical Learning Theory***, Springer, 1998.

[35] N. Christianini and J. Shawe-Taylor, ***An Introduction to Support Vector Machines and Other Kernel-based Learning Methods***, Cambridge University Press, 2000.

[36] V. Vapnik, ***The Nature of Statistical Learning Theory***, Springer Verlag, 1999.

[37] B. R. Wildermoth and K. K. Paliwal, ***GMM Based Speaker Recognition on Readily Available Databases***, In Proc Microelectronic Engineering Research Conf, Brisbane, Nov 2003.

[38] R. Cappelli, D. Maio and D. Maltoni, ***Combining Fingerprint Classifiers,*** in Proceedings of the First International Workshop on Multiple Classifier Systems, pp.351-361, June 2000.

[39] T. Kinnunen, E. Karpov, P. Fränti, ***Efficient Online Cohort Selection Method for Speaker Verification,*** Proceeding of 8th International Conference on Spoken Language Processing (ICSLP), Vol. III, pp. 2401-2402, Korea, Oct. 2004.

[40] L. Mezai, F. Hachouf, M. Bengherabi, ***Fusion of Face and Voice Using the Dempster-Shafer Theory for Person Verification***, 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), pp 103 -106, Tipaza, Algeria, May 2011.

[41] N. Srinivas, K. Veeramachaneni and L. A. Osadciw, ***Fusing Correlated Data from Multiple Classifiers for Improved Biometric Verification,*** 12th International Conference on Information Fusion, FUSION '09, pp 1504-1511, Seattle, July 2009.

[42] P.J. Phillips, A. Martin, C.L. Wilson, and M. Przybocki, ***An Introduction to Evaluating Biometric Systems,*** IEEE Computer Magazine, pp.56-63, February 2000.

[43] A. Mayoue, ***Biosecure Tool Performance Evaluation of a Biometric Verification System,*** version 1.0,

[44] SYRIS Technology Corp, ***Technical document about FAR, FRR and EER***, Version 1.0, 2004.

[45] N. Poh and S. Bengioa ,***Estimating the Confidence Interval of Expected Performance Curve in Biometric Authentication Using Joint Bootstrap***, IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, Vol. 2, pages 137-140, Honolulu, April 2007.

[46] B. O'mullane, ***Biometric Performance Display and Comparison Tool,*** BioPerf Manual.

[47] N. Poh and S. Bengio, ***A Score-Level Fusion Benchmark Database For Biometric Authentication,*** In Proceedings of the 5th international conference on Audio- and Video-Based Biometric Person Authentication, AVBPA'05, pp 1059-1070 , 2005.

[48] ***Biometric Technology Application Manual,*** Volume1, National Biometric Security Project, 2008.

[49] J. Ashbourn, ***Guide to Biometrics for Large-Scale Systems, Technological, Operational, and User-Related Factors***, Springer-Verlag, London, 2011.

[50] C.W. Lau, B. Ma, H.M. Meng, Y.S. Moon, Y. Yam, ***Fuzzy Logic Decision Fusion in a Multimodal Biometric System,*** In: Proceedings of the 8th International Conference on Spoken Language Processing (ICSLP), October 2004.

[51] E. Bailly-Bailliére et al., ***The BANCA Database and Evaluation Protocol***, Lecture Notes in Computer Science, Vol. 2688, 2003, pp. 625-638.

[52] H. Byun1 and L. Seong-Whan, ***Applications of Support Vector Machines for Pattern Recognition: A Survey,*** LNCS 2388, pp. 213-236, 2002.

[53] M.C. Fairhurst, F. Deravi, J. George, ***Towards optimised implementations of multimodal biometric configurations,*** Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, CIHSPS'2004, pp. 113-116, Venice, Italy, July 2004.

[54] NIST image group's Biometric Scores Set, September, 2004,
http://www.nist.gov/itl/iad/ig/biometricscores.cfm, accessed Oct. 24, 2012.

[55] C. Paar, J. Pelzl, ***Understanding Cryptography,*** Springer, 2010.

[56] L. Nanni and A. Lumini, ***A supervised method to discriminate between impostors and genuine in biometry: A Textbook for Students and Practitioners,*** International Journal on Expert Systems with Applications Volume 36, Issue 7, pp. 10401–10407, 2009.

[57] M. Parviz and M.S. Moin, ***Boosting Approach for Score Level Fusion in Multimodal Biometrics Based on AUC Maximization***, In Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Issue 1, pp. 51-59 2011.

[58] K. Reisdorph and K. Henderson, ***Teach Yourself Borland C++Builder in 21 Days***, Sams publisher, 1997.

[59] Genetic Algorithms, 30 May 2006, **http://subsimple.com/genealgo.asp**, accessed Oct. 24, 2012.

[60] F. Alsaade***, Neuro-Fuzzy Logic Decision in a Multimodal Biometrics Fusion System,*** Scientific Journal of King Faisal University (Basic and Applied Sciences), Vol.11 No.2 14, 2010.

[61] J. Kittler, M. Hatef, R. Duin, and J. Matas, ***On combining classifiers***, IEEE Trans. on Pattern Analysis and Machine Intelligence, Volume 20, Issue 3, pp. 226–239, March 1998.

[62] J. Kennedy and R.C. Eberhart with Y. Shi, ***Swarm Intelligence,*** Morgan Kaufmann Publishers, San Francisco, USA, 2001.

[63] ***Particle Swarm Optimization,*** http:// www2.cs.uh.edu/~lyons19/Advantages.htm, Accessed on April 30, 2012.

[64] X. Yang, J. Yuan, J. Yuan, H. Mao, ***A modified particle swarm optimizer with dynamic adaptation,*** Journal of Applied Mathematics and Computation, Vol. 189 , pp. 205-1213, 2007.

[65] W.R.M.U.K Wickramasinghe and X. Li***, Choosing Leaders for Multi-objective PSO Algorithms Using Differential Evolution,*** Lecture Notes in Computer Science, Volume 5361 pp. 249-258, 2008.

[66] N. Morizet and J. Gilles, ***A New Adaptive Combination Approach to Score Level Fusion for Face and Iris Biometrics Combining Wavelets and Statistical Moments,*** International Symposium on Visual Computing (ISVC), pp. 661-671, Las Vegas, US, 2008.

[67] R. Mazouni and A. Rahmoun, ***On Comparing Verification Performances of Multimodal Biometrics Fusion Techniques,*** International Journal of Computer Applications Volume 33 No.7, pp. 24-29, Nov. 2011.

[68] A. Martin, G. Doddington, T. Kamm, M. Ordowsk, and M. Przybocki, ***The DET Curve in Assessment of Detection Task Performance***, in Proceeding Eurospeech, Volume 4, pp.1895-1898, Rhodes, Greece, 1997.

[69] A.K. Jain, ***Biometric authentication,*** Scholarpedia, 2008.

http://www.scholarpedia.org/article/Biometric_authentication, (Accessed on May 10, 2012)

[70] R. Snelick, , M. Indovina, , J. Yen, , A. Mink, , ***Multimodal Biometrics: Issues in Design and Testing,*** In Proceedings of the 5th International Conference on Multimodal Interfaces, Vancouver, pp. 68–72, Canada, 2003.

[71] F. Alsaade, ***A Study of Neural Network and its Properties of Training and Adaptability in Enhancing Accuracy in a Multimodal Biometrics Scenario***, Information Technology Journal, Volume 9, Issue 1, pp.188-191, 2010.

[72] P. Verlinde, G. Chollet, ***Comparing Decision Fusion Paradigms Using k-NN Based Classifiers, Decision Trees and Logistic Regression in a Multimodal Identity Verification Application,*** In Proceedings of the 2nd International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA), pp.189-193, Washington DC, 1999.

[73] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, ***Fuzzy fusion in multimodal biometric systems***, in Proceeding of 11th International Conference on Knowl.- Based Intell. Inf. Eng. System, pp. 108-115, Berlin, Germany 2010.

[74] A.K. Jain, A. Ross, and S. Prabhakar, ***An introduction to biometric recognition,*** IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., vol. 14, no. 1, pp. 4-20, Jan. 2004.

[75] A.K. Jain, A. Ross, and S. Pankanti, ***Biometrics: A Tool for Information Security***, IEEE Transactions on Information Forensics and Security, volume 1, no. 2, June 2006.

[76] M. Indovina, U. Uludag, R. Snelick, A. Mink and A.K. Jain, ***Multimodal Biometric Authentication Methods: A COTS Approach***, Proceeding Multi-Modal User Authentication (MMUA), 99-106, 2003.

[77] R. Tronci, G. Giacinto and F. Roli, ***Selection of experts for the design of multiple biometric systems***, Lecture Notes in Computer Science, 4571, pp 795-809, 2007.

[78] L. Latha, S. Thangasamy, ***Efficient approach to Normalization of Multimodal Biometric Scores***, International Journal of Computer Applications, Vol. 32, No.10, pp. 57-64, Oct. 2011.

[79] P. Tahmasebi and A. Hezarkhani, ***Application of Adaptive Neuro-Fuzzy Inference System for Grade Estimation; Case Study, Sarcheshmeh Porphyry Copper Deposit, Kerman, Iran,*** Australian Journal of Basic and Applied Sciences, Volume 4 Number 3, pp. 408-420, 2010.