Order N^o : ...../...../.....

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF KASDI MERBAH OUARGLA

Faculty of New Information Technologies and Communication

Department of Electronics and Telecommunications

THESIS

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

3rd Cycle LMD Doctorat

In : Communication and Signal Processing

By : **Maarouf KORICHI**

Theme

Biometrics and Information Security for a Secure Person Identification

Soutenue publiquement le : 22/06/2019 devant le jury composé de:

F.Z. LAALAM	*Professor*	*at U. K. M. O.*	*President*
A. MERAOUMIA	*MCA*	*at Tebessa University*	*Thesis Director*
K.E. AIADI	*Professor*	*at U. K. M. O.*	*Thesis Co-director*
H. BENDJENNA	*Professor*	*at Tebessa University*	*Examiner*
F.CHEBARA	*MCA*	*at U. K. M. O.*	*Examiner*
F. CHARIF	*MCA*	*at U. K. M. O.*	*Examiner*

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

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DE KASDI MERBAH OUARGLA

Faculté Des Nouvelles Technologies de l'Information et de la communication

Département De l'électronique et des télécommunications

THÈSE

Thèse présentée en vue de l'obtention du diplôme de

Doctorat 3ème Cycle LMD

Filière : **Electronique**

Spécialité : **Communication et Traitement du signal**

Par : **Maarouf KORICHI**

Thème

Biométrie et Sécurité de l'Information pour une Identification Sûre des Personnes

Soutenue publiquement le : 22/06/2019 devant le jury composé de:

F.Z. LAALLAM	*Professeur*	*à l'U. K. M. O.*	*Présidente*
A. MERAOUMIA	*Maître de conférence/A*	*à l'Université de Tebessa*	*Directeur de Thèse*
K.E. AIADI	*Professeur*	*à l'U. K. M. O.*	*Co-directeur de Thèse*
H. BENDJENNA	*Professeur*	*à l'Université de Tébessa*	*Examinateur*
F. CHEBBARA	*Maître de conférence/A*	*à l'U. K. M. O.*	*Examinateur*
M.L. KHERFI	*Maître de conférence/A*	*à l'U. K. M. O.*	*Examinateur*
D. SAMAI	*Maître de conférence/A*	*à l'U. K. M. O.*	*Invité*


بسم الله الرحمن الرحيم


وقل رب زدني علما


صدق الله العظيم

To my parents:Ommi Rebiha and Abi Mohamed Abdelkader for having always supported me and encouraging me to go as far as possible in my studies. May Allah protect them,

To my little family : My wife KRID Keltoum and my little prince Mohamed Maher, I am very grateful to Allah for being with me and for constant support for me, I ask Allah to protect them

To my brothers and sisters: Atallah,Mohamed,Meriem,Zohra,Zineb, Aicha and Abdelghani for there support, help and encouragement,

and to all my friends,

Many thanks to those I love and those who helped, encouraged and loved me in return.

Maarouf Korichi

Acknowledgment

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

It has been an auspicious journey for me to arrive at this point. I am really short of words now, but I take this opportunity to express my sincere thanks to my thesis supervisor, `Dr.MERAOUMIA Abdellah` *with whom, I learned to analyze, criticize, and express myself as clearly as possible. I wouldn't be exaggerating to say that he took as much efforts as me for this research work. Particularly, he taught me how to think like a researcher, especially in the beginning of my thesis. His belief in me throughout this work kept me inspired.*

I also want to thank my thesis co-director `Prof.Kamal Eddine AIADI`*, It has been an honor and pleasure to work with him.*

I would particularly like to thank all the jury members who have accepted to preside and read this work. `Prof.Laallam Fatma Zohra` *from Ouargla University as jury president,* `Prof.Hakim Bendjenna` *from Tebessa University,* `Dr.Chebbara Fouad` *from Ouargla University,* `Dr.KHERFI Mohamed Lamine` *from Ouargla University.*

I owe my deepest gratitude to `Dr.Samai Djamal` *for his eminent support and encouragement throughout my research project.*

I also extend my sincere acknowledgments to all teachers of the Department of Electronics and Communications from KASDI Merbah University in Ouargla for their support and advice.

My thanks also go to all my colleagues and friends, especially `Khaled BENSID`*, for their support and help.*

Finally, my thanks go to all those who contributed in any way to the outcome of this work.

Abstract

Secure information systems are critically important to modern day businesses and societies. From banking systems and medical systems to infrastructures surveillance or an e-application system. However, various solutions were proposed in the literature to achieve a secure information system. The most two known means used is this field are Biometric and Cryptography. Unfortunately, and despite their effectiveness, those two techniques suffer from different limitations. biometric systems possess problems such as non-revocability, non-template diversity, and possibility of privacy compromise where the strengthen of the Cryptography system is depends on the secrecy of the cryptographic key. The secret cryptographic key is generally too long for a user to remember and not strongly linked to its identity. To overcome those two drawbacks, it is proposed to combine between biometric and cryptography. The system in which biometrics are combined with cryptography is called Biometric-Crypto System.

In this thesis, we are motivated by the important interest in the Biometric-Crypto system conception. At his context, this work treats two research areas. The first part is devoted to the conception of the biometric based identification system. As the crucial task in those systems is the feature extraction task. Various feature extractions descriptors were proposed to extract such information of the user biometric modalities where the aim is to enhance the system performance in term of accuracies, time processing and the system database size. For that, in this work, a new extension of the Local Binary Pattern called 3DLBP which extract directly the information from the color, MSP/HSP images. In addition, this work includes different conceptions of biometric system using different descriptors(such as HOG,BSIF and GABOR filters) based on different modalities(EAR,FKP, PLM) where the main objective of those systems is to ameliorate the performance of the biometric system in term of robustness, precision and accuracy.

The second part treats the Biometric-Crypto system performance and conception. In this thesis part, we propose a secure biometric-crypto scheme dedicated to online e-voting system. The fuzzy commitment concept associated with the PLM based on two representations (GL and NIR) is the core of our system. In this context, to enhance the discriminating capability of the PLM feature vectors, we propose the use of a binary feature descriptor called BPBSIF. Subsequently, the voters data is encrypted using a random key then this key is binding in the extracted feature vector using fuzzy commitment scheme. Then, in the central system, a new scheme for the key retrieval is implemented in order to extract this key which is used to decrypt the message and then treat it. The experimental results, using a database of 300 voters, showed that online e-voting based crypto-biometric system has higher performances in terms of accuracies and key retrieval.

Keywords: *Security, Biometrics, identification, Biometric-Crypto system, Encryption key, Fuzzy commitment, Data fusion, e-voting*

Résumé

Les systèmes d'information sécurisés sont extrêmement importants pour les entreprises et les sociétés modernes. Des systèmes bancaires et médicaux au service des infrastructures ou d'un système d'application éléctronique. Cependant, diverses solutions ont été proposées dans la littérature pour mettre en place un système d'information sécurisé. Les deux moyens les plus utilisés dans ce demaine sont la biométrie et la cryptographie. Malheureusement, et malgré leur efficacité, ces deux techniques souffrent de limitations différentes. Les systèmes biométriques présentent des problèmes tels que la non-révocabilité, la diversité des modèles et la possibilité de compromettre la confidentialité de la vie privée où le renforcement du système Cryptographique dépend de secret de la clé cryptographique.La clé cryptographique secrète est généralement trop longue pour être mémorisée par un utilisateur et n'est pas fortement liée à son identité. Pour surmonter ces deux obstacles, il est proposé de combiner la biométrie et la cryptographie. Le système dans lequel la biométrie est combinée à la cryptographie est appelé système Crypto-biométrique.

Dans cette thèse, nous sommes motivés par l'intérêt important porté à la conception du système Crypto-biometrique. A ce contexte, ce travail traite deux domaines de recherche. La première partie est consacrée à la conception du système d'identification biométrique. La tâche essentielle dans ces systèmes est la tâche d'extraction des caractéristiques. Diverses descripteurs d'extractions de caractéristiques ont été proposées pour extraire les informations des modalités biométriques de l'utilisateur, dont le but est d'améliorer les performances du système en terme de précision, du temps de calcule et la taille de la base de données du système. Dans ce travail, une nouvelle extension du Motif Binaire Local appelée 3DLBP, qui extrait directement les informations des images couleur, MSP / HSP. En outre, ce travail inclut une conception différente d'un système biométrique utilisant différents descripteurs (tels que HOG, BSIF et filtres de GABOR) basés sur différentes modalités (EAR, FKP, PLM) où l'objectif principal de ces systèmes est d'améliorer les performances du système biométrique. En termes de robustesse, de précision et d'exactitude.

La deuxième partie traite les performances et la conception du système Crypto-biométrique. Dans cette partie de la thèse, nous proposons un schéma crypto-biométrique sécurisé dédié au système de vote électronique en ligne. Le concept d'engagement flou associé au PLM basé sur deux représentations (GL et NIR) est le cœur de notre système. Dans ce contexte, afin d'améliorer la capacité de discrimination des vecteurs de caractéristiques PLM, nous proposons l'utilisation d'un descripteur binaire appelé BPBSIF. Par la suite, les données des électeurs sont cryptées à l'aide d'une clé aléatoire, puis cette clé est liée dans le vecteur de caractéristiques extrait à l'aide d'un schéma d'engagement flou. Ensuite, dans le système central, un nouveau schéma pour la récupération de clé est mis en œuvre afin d'extraire cette clé qui a été utilisée pour déchiffrer le message puis traitée. Les résultats expérimentaux, utilisant une base de données de 300 électeurs, ont montré que le système crypto-biométrique basé sur le vote électronique en ligne offre des performances plus élevées en termes de précision et de récupération des clés.

Mots clés : *Sécurité, biométrie, identification, système crypto-biométrique, clé de cryptage, engagement flou, fusion de données, vote électronique*

الملخص

تعد أنظمة المعلومات الآمنة ذات أهمية حاسمة لأعمال ومجتمعات اليوم الحديث. من الأنظمة المصرفية والأنظمة الطبية إلى مراقبة البنية التحتية أو نظام التطبيق الإلكتروني. ومع ذلك ، تم اقتراح حلول مختلفة في السابق لتحقيق نظام معلومات آمن. أكثر هذه الوسائل المعروفة شيوعًا في هذا المجال هي الأدوات البيومترية والتشفير. لسوء الحظ ، وعلى الرغم من فعاليتها ، تعاني هذه التقنيات من قيود مختلفة. تمتلك الأنظمة البيومترية مشكلات مثل عدم القدرة على الإلغاء والتنوع غير القالب وإمكانية اختراق الخصوصية حيث تعتمد تقوية نظام التشفير على سرية المفتاح المشفر. وعمومًا ، يكون مفتاح التشفير السري طويلاً جدًا على المستخدم أن يتذكره ولا يرتبط بقوة بهويته. للتغلب على هذه السلبيتين ، اقترح الجمع بين البيومترية والتشفير. ويطلق على النظام الذي يتم فيه دمج القياسات الحيوية مع التشفير اسم نظام التشفير-البيومتري.

في هذه الأطروحة ، تم تحفيزنا من خلال الاهتمام الهام بمفهوم نظام التشفير-البيومتري. في سياقه ، يعالج هذا العمل مجالين بحثيين. الجزء الأول مخصص لمفهوم نظام تحديد الهوية القائم على القياسات الحيوية. حيث أن المهمة الحاسمة في هذه الأنظمة هي مهمة استخراج الميزة. واقترحت مجموعة متنوعة من أدوات استخلاص الميزات لاستخراج هذه المعلومات من الطرائق البيومترية للمستخدم حيث تهدف إلى تحسين أداء النظام من حيث الدقة ، ومعالجة الوقت ، وحجم قاعدة بيانات النظام. لذلك ، في هذا العمل ، تم إضافة امتداد جديد للنمط الثنائي المحلي يدعى $3DLBP$ والذي يستخرج المعلومات مباشرة من الصور الملونة و الصور MSP/HSP . يتضمن هذا العمل أيضًا مفهومًا مختلفًا للنظام الحيوي باستخدام واصفات مختلفة (مثل $BSIF$, HOGو مرشحات $GABOR$) استنادًا إلى طرائق مختلفة (EAR وFKP وPLM) حيث يكون الهدف الرئيسي من هذا النظام هو تحسين أداء النظام البيومتري في المدى من المتانة والدقة والفاعلية.

الجزء الثاني يعالج أداء ومفهوم نظام التشفير-البيومتري. في هذا الجزء من الأطروحة ، نقترح خطة آمنة للتشفير الحيوي ، مخصصة لنظام التصويت الإلكتروني عبر الإنترنت. إن مفهوم الالتزام الغامض المرتبط بـ PLM المستند إلى تمثيلين (GL وNIR) هو جوهر نظامنا. في هذا السياق ، لتعزيز القدرة التمييزية لميزة PLM ، نقترح استخدام واصف ميزة ثنائية تسمى $BPBSIF$. بعد ذلك ، يتم تشفير بيانات الناخبين باستخدام مفتاح عشوائي ، ثم يكون هذا المفتاح مربوطا مع الميزة المستخرجة باستخدام نظام التزام ضبابي. ثم ، في النظام المركزي ، يتم تنفيذ مخطط جديد لاسترجاع المفتاح من أجل استخراج هذا المفتاح الذي يستخدم لفك تشفير الرسالة ثم معالجتها. وأظهرت النتائج التجريبية ، باستخدام قاعدة بيانات تضم 300 ناخب ، أن نظام التشفير البيومتري القائم على الاقتراع الإلكتروني على الإنترنت يتمتع بأداء أعلى من حيث الدقة والاسترداد الرئيسي.

الكلمات المفتاحية : الأمن ، القياسات الحيوية ، تحديد الهوية ، نظام التشفير-البيومتري، مفتاح التشفير ، الالتزام الضبابي ، دمج البيانات ، التصويت الإلكتروني

Contents

Abstruct iv

List of Figures xi

List of Tables xv

Abbreviations xvii

1 General Introduction 1

1.1 Background and Issues . . . 2
1.2 Motivations and Objectives . . . 4
1.3 Contribution of the Thesis . . . 4
1.4 Organization of the Thesis . . . 5

2 Biometric: When Identity Matters 7

2.1 Introduction . . . 7
2.2 Information security strategies . . . 7
2.3 biometrics: definitions and use . . . 8
2.3.1 Biometric . . . 9
2.3.2 Rising of biometric: a brief story . . . 9
2.3.3 Objectives associated with biometrics . . . 10
2.3.4 Use of biometrics . . . 10
2.4 Taxonomy of Biometric Modalities . . . 11
2.4.1 Physical biometrics (Morphological) . . . 13
2.4.2 Behavioral biometrics . . . 16
2.4.3 Biological biometrics . . . 18
2.4.4 Comparative Study Of different Biometric Techniques . . . 20
2.5 Biometric System Conception . . . 21
2.5.1 Enrollment, verification and identification . . . 21
2.5.2 Biometric system architecture . . . 22
2.5.3 *On-line* and *Off-line* Biometric system . . . 23
2.6 Multimodal Biometric Systems . . . 24

2.6.1 Unimodal Biometric System limitations . . . 24
2.6.2 Biometric Multi-modality . . . 25
2.6.3 Data Fusion principal . . . 26
2.6.4 Multimodal Biometric Sources . . . 26
2.6.5 Fusion levels . . . 28
2.7 Biometric System Evaluation . . . 30
2.7.1 Error Rate Metrics . . . 30
2.7.2 Curves of Performance . . . 31
2.8 Conclusion . . . 33

3 Information Security: From cryptography to Bio-cryptography 34
3.1 Introduction . . . 34
3.2 Cryptography: Encryption & Decryption . . . 35
3.3 Symmetric and Asymmetric Encryption . . . 35
3.3.1 Symmetric Encryption . . . 36
3.3.2 Asymmetric Encryption . . . 37
3.4 Problems related to Cryptography . . . 38
3.5 Biometric-Crypto systems: An Introduction . . . 39
3.5.1 Key Release based on Biometric . . . 41
3.5.2 Cryptographic Key Binding using Biometrics . . . 42
3.5.2.1 Fuzzy Vault schemes . . . 43
3.5.2.2 Fuzzy Commitment scheme . . . 45
3.5.3 Cryptographic Key Generation from Biometrics . . . 47
3.5.4 Biometric-crypto system: discussion and chalenges . . . 49
3.5.5 Security analysis of biometric-Crypto Systems . . . 50
3.6 Conclusion . . . 50

4 Biometric feature selection 51
4.1 Introduction . . . 51
4.2 Feature Extraction Task . . . 52
4.2.1 Objective . . . 52
4.2.2 Biometric features types . . . 52
4.2.2.1 Lines based approaches . . . 53
4.2.2.2 Texture based approach . . . 53
4.2.2.3 Shape based approach . . . 53
4.3 Properties of Biometric Features . . . 54
4.3.1 Biometric system obligations . . . 54
4.3.2 Information security obligations . . . 55
4.4 Person identity authentication using biometric features . . . 55
4.4.1 Objective . . . 56

4.4.2 Feature Extraction Techniques . . . 56
4.4.2.1 Line based approach: Gabor filter response overview . . . 56
4.4.2.2 Texture based approach : Binarized Statical Image features (BSIF) overview . . . 58
4.4.2.3 Shape based approach: Histogram of Oriented Gradient (HOG) overview . . . 59
4.4.3 Proposed Feature Extraction Technique . . . 59
4.4.3.1 Objective . . . 60
4.4.3.2 Original Local Binary Pattern (LBP) overview . . . 60
4.4.3.3 3D Local Binary Pattern (3DLBP) . . . 62
4.5 Conclusion . . . 64

5 Experimental Results and Discussion 65
5.1 Introduction . . . 65
5.2 The biometrics modalities used . . . 66
5.3 Database Description . . . 68

I Biometric Identification System Test Results 70
5.4 Introduction . . . 71
5.5 General system description . . . 71
5.6 System performance evaluation . . . 72
5.6.1 Ear Identification System Using Gabor Filter Responses . . . 72
5.6.2 FKP based identification system using HOG features . . . 75
5.6.3 Palmprint based identification system . . . 80
5.7 3D-LBP based Biometric system . . . 83
5.8 Summary and comparative study . . . 90

II Biometric Crypto-system based E-voting Protocol 91
5.9 Introduction . . . 92
5.10 *e-voting* system Description . . . 92
5.10.1 Enrollment phase . . . 93
5.10.2 Sending & data encryption process . . . 94
5.10.3 Receipting & data decryption process . . . 95
5.10.4 Multimodal System . . . 95
5.11 System performance evaluation . . . 96
5.11.1 BPBSIF based unimodal system evaluation: . . . 96
5.11.2 Biometric-Crypto system security analysis . . . 98
5.11.2.1 Biometric-Crypto system with greater databases . . . 103
5.12 Conclusion . . . 105

6 Conclusions, Perspectives, and Future Directions **106**

A Region Of Interest (ROI) Extraction **108**
A.1 Image preprocessing . . . 108
A.2 Palmprint preprocessing . . . 108
A.3 Finger-Knuckle Print (FKP) ROI Extraction . . . 112
A.4 EAR Region Of Interest Extraction . . . 116

B Experimental Databases **118**
B.1 The used databases description . . . 118
B.2 Palmprint database . . . 118
B.3 Finger-Knuckle Print (FKP) Database . . . 121
B.4 IIT Delhi Ear Database . . . 122

C Matching and Normalization process **124**
C.1 Introduction . . . 124
C.2 Feature Matching . . . 124
C.2.1 Hamming Distance . . . 125
C.2.2 Euclidean Distance . . . 125
C.2.3 Chi-Square distance . . . 125
C.3 Normalization process . . . 126

D Data Classifiers **127**
D.1 Support Vector Machine (SVM)- A brief overview . . . 127
D.2 K-Nearest Neighbors (KNN) . . . 130

E Personal Contributions **132**
E.1 Publications . . . 132
E.2 International Communications indexed in the IEEE xplore database . . . 132
E.3 International Communications with international reading committees . . . 133

Bibliography **134**

List of Figures

2.1 Some biometrics modalities. . . . 11
2.2 Empreinte digitale. . . . 13
2.3 Hand Geometry. . . . 13
2.4 Finger Knuckle-Print. . . . 14
2.5 Palmprint. . . . 14
2.6 The Face. . . . 15
2.7 Iris. . . . 15
2.8 Retina. . . . 16
2.9 Ear. . . . 16
2.10 Voice. . . . 17
2.11 Signature. . . . 17
2.12 Keystroke dynamics. . . . 18
2.13 Gait. . . . 18
2.14 DNA. . . . 19
2.15 Hand Vein. . . . 19
2.16 Facial Thermography. . . . 19
2.17 Biometric System Structure. . . . 21
2.18 Some Unimodal Biometric System limitations. . . . 25
2.19 Some Unimodal Biometric System limitations. . . . 27
2.20 Multi-modal biometric system fusion levels. . . . 29
2.21 Distributions of genuine users scores and impostor scores 31
2.22 Receiver Operating Characteristic (ROC): (*a*) GAR against FAR when the decision threshold varies, (*b*) FRR Variation according to the FAR when the decision threshold varies 32
2.23 Cumulative match characteristic curve (CMC). . . . 32

3.1 Basic idea of cryptography. . . . 35
3.2 Basic idea of symmetric cryptography. . . . 36
3.3 Basic idea of Asymmetric cryptography. . . . 37
3.4 Categorization of Biometric template protection schemes. . . . 39
3.5 Key Release based on biometrics. . . . 41
3.6 Cryptographic key Binding using biometrics. . . . 43

3.7 Typical fingerprint Fuzzy vault Encoding and Decoding. 44
3.8 Typical fingerprint Fuzzy commitment Encoding and Decoding. 46
3.9 Cryptographic key generation from biometrics. 48

4.1 Block diagram of the feature extraction process based on Gabor filter responses using EAR images. 57
4.2 Basic idea of the basic LBP operator. 61

5.1 Ear structure. 67
5.2 Representations used for the palmprint. 67
5.3 Finger Knuckle Prints (FKP): Index, Middle and Ring fingers. 68
5.4 Block diagram of the person identification system using palmprint images based on 3DLBP descriptor. 72
5.5 Results of Ear based unimodal open/closed set identification system. (a) The ROC curves with respect to the different feature vectors (b) The ROC curve in the case of V_{AM} based open set identification system and (c) the CMC curve in the case of V_{AM} based closed set identification system. 73
5.6 Results of Ear based multimodal open/closed set identification system. (a) The ROC curves, FRR against FAR, with respect to the unimodal and multimodal systems, (b) The ROC curves, GAR against FAR, with respect to the best case and (c) The CMC curves with respect to the unimodal and multimodal system. 75
5.7 FKP based unimodal *open/closed-set* identification test results under different fingers. (a) The ROC curves (FRR against FAR), (b) The ROC curves (GAR against FAR) and (c)The CMC curves. 76
5.8 FKP based multimodal *open/closed-set* identification test results under the best combinations (fusion at feature level). (a) The ROC curves (FRR against FAR), (b) The ROC curves (GAR against FAR) and (c) The CMC curves. 78
5.9 FKP based Multimodal *open/closed-set* identification test results under the best combinations (fusion at matching score level). (a) The ROC curves (FRR against FAR), (b) The ROC curves (GAR against FAR) and (c) The CMC curves. . 79
5.10 Performance of the best multimodal identification system.(a) Comparison between the unimodal and multimodal systems, (b) The genuine and impostor scores distribution and (c) The FAR against FRR by varying the decision threshold. 80
5.11 PLM based unimodal *open/closed-set* identification test results under different fingers. (a) The ROC curves (FRR against FAR), (b) The ROC curves (GAR against FAR) and (c)The CMC curves. 81
5.12 PLM based unimodal *open/closed-set* identification test results under different fingers. (a) The ROC curves (FRR against FAR), (b) The ROC curves (GAR against FAR) and (c)The CMC curves. 82

5.13 LBP based *open-set* biometric identification test results.(*a*) Performance comparison between different spectral bands, (*b*) RGB based multimodal *open-set* identification performance and (*c*) RGBN based multimodal *open-set* identification performance. 84
5.14 3DLBP based *open-set* biometric identification test results.(*a*) Performance comparison between different combinations, (*b*) Comparison between LBP and 3DLBP descriptor in the case of RGB combination and (*c*) Comparison between LBP and 3DLBP descriptor in the case of RGBN combination. 87
5.15 3DLBP based *open-set/closed-set* biometric identification test results. (*a*) ROC curve for the best case (four bands), (*b*) CMC curve for the best case (four bands) and (*c*) Genuine and impostor distance distribution. 87
5.16 3DLBP based Edge features in various images at several thresholds. 89
5.17 Proposed online e-voting system based on PLM images and a fuzzy commitment based symmetric cryptography. 92
5.18 Framework of the proposed feature extraction method. 93
5.19 Flowchart of access verification and template generation process in customer terminal. 94
5.20 BPBSIF based Unimodal *open/closed-set* identification test results under different bands. (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*)The CMC curves. 97
5.21 Biometric-Crypto system genuine key retrieval rate under the two representation GL and NIR. 101
5.22 Biometric-Crypto system impostor key retrieval rate under the two representation GL and NIR. 101
5.23 Unimodal/Multimodal Biometric-Crypto system test results evaluation comparison under different key sizes 104

A.1 Image filtering 109
A.2 Image binarization 109
A.3 Contour in a binary image. *(a)* type 8 connectivity, *(b)* type 4 connectivity, and *(c)* the algorithm application 110
A.4 Hand Edge. 110
A.5 Key Point localization. 111
A.6 Image Rotation. 111
A.7 Palmprint ROI localization. 111
A.8 Palmprint ROI Extraction. 112
A.9 Filtering and Sub-sampling of the image finger. 112
A.10 X axis determination. 113
A.11 The extracted sub-image before the ROI extraction. 113
A.12 The obtained Edge image. 114
A.13 Curves on the finger image. 114

A.14 Image obtained by the coding application of the convex direction.. 114
A.15 Y Axis determination. 115
A.16 ROI Localization in the finger image. 115
A.17 ROI Extraction from the finger image. 116
A.18 Various steps in a typical EAR Region Of Interest (ROI) extraction algorithm. 117

B.1 2D palmprint capture device developed by PolyU [29]. (*a*) acquisition device and (*b*) schematic diagram of the device. 119
B.2 Some sample images of the PolyU-PLM-2D database 119
B.3 Multispectral image acquisition device (MSP) developed by PolyU [131]. (*a*) Acquisition device and (*b*) schematic diagram of the device. 120
B.4 Some sample images of the PolyU-PLM-MSP database 121
B.5 FKP image acquisition device developed by PolyU [132]. (*a*) Acquisition device and (*b*) schematic diagram of the device. 121
B.6 Some sample images of the PolyU-FKP database 122
B.7 Some sample images of the IIT Delhi EAR database 123

D.1 Separating Hyperplane 128
D.2 Best Hyperplane Separating 128
D.3 Case of no separately data 129
D.4 Support Vector Classifier 129
D.5 An example of KNN classification 131

List of Tables

2.1 Comparison between different existing security methods 8
2.2 Properties of biometric modalities according to the following properties: (U) Universality, (N) Uniqueness, (P) Permanence, (C) Collectability, (A) Acceptability, (E) Performance (the number of stars in the performance column is related to the obtained value of Equal Error Rate (EER) in the state of the art (Extract from[25])) 12
2.3 Advantage and Disadvantage of Biometric Techniques 20

3.1 Comparison of fuzzy commitment and fuzzy vault. 47
3.2 Comparison between key binding and key generation schemes 49

5.1 Ear based unimodal open set identification system performance. 73
5.2 Ear based unimodal closed set identification system performance. 73
5.3 Ear based multimodal open set identification system performance 74
5.4 Ear based multimodal closed set identification system performance 75
5.5 FKP based unimodal identification test results 76
5.6 Performance of the FKP based multimodal *Open/Closed-set* identification system (Fusion at Feature Level) 77
5.7 Performance of the FKP based multimodal *Open-set* identification system (Fusion at Matching score Level) 79
5.8 Performance of the FKP based multimodal *Closed-set* identification system (Fusion at Matching score Level) 79
5.9 PLM based unimodal identification test results 81
5.10 Performance of the PLM based multimodal *Open-set* identification system . . 82
5.11 Performance of the PLM based multimodal *Closed-set* identification system . 82
5.12 LBP based unimodal identification test results 84
5.13 Performance of the LBP based multimodal *open/closed-set* identification system (RGB combinations) 85
5.14 Performance of the LBP based multimodal *open/closed-set* identification system (RGBN combinations) 85
5.15 3DLBP-based identification test results 87
5.16 3DLBP time processing performance 88

5.17 Performances comparison of our proposed systems with the state-of-the-art . 90
5.18 BPBSIF based unimodal identification test results 97
5.19 GL based Biometric-Crypto system performance evaluation 99
5.20 NIR based Biometric-Crypto system performance evaluation 100
5.21 Biometric-crypto system based multimodal test results evaluation(duplicated Key) 103
5.22 Biometric-crypto system based multimodal test results evaluation(Separated Key) 103

Abbreviations

ATM	:	Automating Telling Machine
AES	:	Advance Encryption Standard
BSIF	:	Binarized Statical Image Feature
BPBSIF	:	Bit-Palne BSIF
CCD	:	Charged Coupled Device
CMC	:	Cumulative Match Curve
DCTNet	:	Discrete Cosine Transform Network
DES	:	Data Encryption Standard
DNA	:	Deoxyde Nucleic Acid
DWT	:	Discrete Wavelet Transform
EER	:	Equal Error Rate
FAR	:	False Acceptance Rate
FKP	:	Finger Knuckle Print
FMR	:	False Mach Rate
FNMR	:	False Non Match Rate
FRR	:	False Rejection Rate
GAR	:	Genuine Acceptance Rate
GL	:	Grey Level representation
HOG	:	Histogram of Oriented Gradiant
HSP	:	HyperSpectral Palmprint
ICANet	:	Independent Component Analysis Network
LDANet	:	Linear Descriminent Analysis Network
LIF	:	Left Index Finger
LMF	:	Left Middle Finger
MSP	:	MultiSpectral Palmprint
NIR	:	Near Infra-Red
PCA	:	Principal Component Analysis
NIR	:	Near Infra-RED
PCA	:	Principal Component Analysis
PCANet	:	Principal Component Analysis Network
PIN	:	Personal Identifier Number
PLM	:	Palmprint
RC4	:	Rivest Cipher 4
RFID	:	Radio Frequency IDentification
RGB	:	Red-Green-Blue
RGBN	:	Red-Green-Blue-NIR
RIF	:	Right Index Finger
RMF	:	Right Middle Finger
ROC	:	Receiver Operating Characteristic
ROI	:	Region Of Interest
ROR	:	Recognition One Rate
RPR	:	Recognition Perfect Rate
RSA	:	Rivest-Shamir-Adleman
SVM	:	Support Vector Machine
3DLBP	:	3D Local Binary Pattern

Chapter 1

General Introduction

NOWADAYS , we are living in an extremely small world . Individuals are highly mobile, constantly connected to each other, and their daily lives are highly influenced by the information technologies in particular mobile devices and social networking. In such societies, most of the services are delivered electronically via smart machines that can be accessed remotely. These include banking, e-commerce, governmental-services to citizens, hotel booking, social aids, and many other fields related to work,commerce, traveling, defense, education, business and social relationships.

Recently, emerging e-applications play a central and important role in the rapid and continued growth of development in several world countries. Several applications can be integrated in this field among others, we can cite e-commerce, e-banking, e-voting and e-government. A reliable e-applications would always ensure the security of the shared information which is becoming as a common and increased challenges in all applications. Indeed, the exchanged information are, generally, sensitive and must be secured. In addition, the identity of the users transmitting this information must be authenticated accurately in the receiver end. A simple way to satisfy these requirements is to use Biometric-Crypto systems [1]. These systems allow binding a secure key to the biometric data to obtain a so called secure sketch from which no information regarding the biometric data or the key can be recovered.

Generally, the knowledge of user identity in the majority of network-related tasks which is necessary in e-application scheme, represents a necessary phase before providing the required services. One of the most known means to establish the identity of system user's is the use of such information related to human physiological or behavioral characteristics or which is known as Biometric such as fingerprint ,face, voice, gait, signature, palpmrint and ...etc [2]. On the other hand,in order to secure the information during transmission or storage, the cryptography is deployed. Cryptography is a great tool which provides security, privacy, and anonymity [3].

Biometric-Crypto system combines between biometric and cryptographic in order to benefit from proprieties of those two techniques. Also, the combination between them can overcome the drawback of biometric and cryptography. The aim of this dissertation is focused and interested in the conception of Biometric-Crypto system in term of construction, evaluation and implementation.

1.1 Background and Issues

Biometrics is a global technique to establish the identity of a person by measuring its physical or behavioral characteristics. Various types of biometric characteristics can be found in the literature, some of them are more reliable then the others, but all must be tamper-proof and unique to be representative of one and only one individual. In addition, biometrics can guarantee superior security and permanent accessibility of information at any point in its life cycle.

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. In cryptographic based system, a message is defined as plaintext (or sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption. The algorithm used for performing Encryption and Decryption is known as cipher(or cypher).

In general, Cryptography is used to guarantee the information security by providing security, privacy, and anonymity during transmission or storage. The information security of a cryptographic-based system is to depend on the secrecy of the cryptographic key as the encryption and decryption algorithms are public. If the cryptographic key is compromised, then the message also becomes known to an adversary (i.e. attacker).So, the keeper of the cryptographic key should be a legitimate user and must kept it in secure manner from the attackers. At this point, two authentication mechanisms are deployed, knowledge based (e.g., passwords) or possession based (e.g., token, smart card, etc.).These authenticators are assigned to the user identity and do not necessarily indicate the presence of the person to whom they belong. Therefore, they can be easily forgotten, stolen or may be guessed out with the help of dictionary attacks by an attacker, and in this situation, the system cannot distinguish between the attacker and a legitimate user [4]. Also, for security reasons, the cryptographic key in such cryptographic algorithm is concept to be long (e.g., key size is 128, 162 or 256 bits for Advance Encryption Standard (AES) algorithm) which leads to the difficulty of memorizing the secret key by the system users.

As an alternative solution to overcome the drawbacks of those problems related to cryptographic key management, researchers have advocated user's biometric traits to manage cryptographic keys. This advocating for using biometric traits is due to its inherent potentiality to differentiate a legitimate individual from a fraudulent impostor[4]. For that biometric is integrated with traditional cryptography to enhance the information security. One can call the system that uses jointly biometric and cryptography for information security as *Biometric-Crypto systems* where the authentication is guaranteed by biometrics and information security is guaranteed by the traditional cryptography [5]. The interaction between biometric and cryptography is to replace the traditional cryptography authentication with biometric authentication to remove the limitation of memorizing cryptographic key as well as maintaining the secrecy of the key without compromising the strength of cryptographic key.

According to the literature review, Biometric-Crypto system can be integrated into three ways namely [6]: *1) Key Release*, *2) Key Binding* and *3) Key Generation*. In Key release schemes, biometric authentication is completely decoupled from the key release mechanism. The Biometric Template and the cryptographic key are stored into a central database or in a smart card or token as separate entities. To release the cryptographic key, a successful Biometric matching is needed, which means that the secret key is released only when a legitimate user attempt to access the system.

For the Key Binding schemes, a transformation is applied on the biometric template in order the hide the secret key. The secret key is released from the cryptographic construct(Template+secret key) if and only if the genuine biometric is provided. It is noted that the cryptographic key is externally generated and completely independent to the biometrics. Moreover, it will be infeasible to extract the cryptographic key or biometrics template from the cryptographic construct without sufficient knowledge about either the biometrics or the key. At this point, to use the cryptographic key, only legitimate users are allowed to access the key. In biometric key binding based Biometric-Crypto systems, two well known practical examples for such schemes are fuzzy commitment [7] and fuzzy vault [8]. Based on a cryptography key, the first scheme allows to secure biometric templates represented as binary vectors, whereas the second allows to secure biometric templates represented as an unordered set of points.

Finally, for the last Biometric-Crypto system schemes, Key generation schemes use the biometric traits to extract directly the cryptographic key for encryption and decryption . Because of biometric template is used to construct the cryptographic key which is inherent to an individual, it is impractical to guess out the original key or generate the key from impostor's biometrics [9].

1.2 Motivations and Objectives

During this thesis, two main goals we attempt to achieves it. The first main goal deals with the conception of biometric based identification system. Moreover, the main task in the conception of biometric system is the choice of feature extraction methods. For that, various features extractions techniques was proposed and applied. In addition, different experiments were conducted to carry out the levels of precision, robustness, and efficiency of the selected techniques.

The second main objective was focused on the construction of e-application(such as e-voting) based Biometric-Crypto system. For that, we are interested in the use of second schemes of Biometric-Crypto system which is the Key Binding schemes where the fuzzy commitment algorithm is used. At this way, the main purpose is concerned with the conception of an Encryption/Decryption cryptographic system (cryptographic key generation) using the biometric traits. In this subject, several biometric modalities (palmprint, fingerprint, finger-Knuckle-print (FKP), iris, ...) can be used. The encryption system must allow the user to choose the identification mode (biometric modality).

1.3 Contribution of the Thesis

The main and major contribution of this thesis can be summarized as follows:

- In this work, we design and concept a new Feature extraction descriptor based on the Local Binary Pattern feature descriptor, the new descriptor is called 3DLBP. Our 3DLBP descriptor extract texture patterns for a color or multi/hyper-spectral images similar to the way that LBP operator extract texture for gray-scale images. Thus, our proposed method extracts directly the feature vector from the entire image (using all spectral bands) instead one band at each time (separately). This methodology allows to reduce the feature vector size and to decrease the time processing. Our proposed descriptor can give different information from a variety of spectral bands and can improve the performance of the system because each spectral band highlights specific features of the image.
- During the realization of this thesis, we tried to construct different biometric identification system which had the ability to distinguish between a legitimate and impostor user's with high degrees in term of accuracy, precision and robustness. For that, different biometric modalities and different feature extraction were proposed and applied. The chosen biometric modalities are palmprint, FKP and Ear modality, that choice is according to the hight obtained performance in term of Universality, Uniqueness, Permanence, Collectability and Acceptability compared to the other modalities. On the

other hand, the chosen features descriptors are based on being able to extract different images of features such as principal lines, texture, and appearance with a high level of accuracy.

- Finally, we design an approach to construct an e-application based Biometric-Crypto system which is an e-voting system. The major concern of the e-voting system (especially online e-voting system) is to effectively minimize the violation of the vote operation and to protect voter information against any kind of frauds [10]. For that, we concept an approach of palmprint based cryptographic key binding from palmprint data of voter where the fuzzy commitment scheme is used as an encryption algorithm.

1.4 Organization of the Thesis

The introductory chapter (**Chapter 1**) describes the basic models of cryptography and limitation of the traditional cryptography is studied. This chapter also describes the objective of the thesis. The major contribution of this thesis are also mentioned briefly. This chapter is followed by five other chapters in succession, the contents of which are briefly described below.

The basic concepts of biometric and biometric technologies are introduced in **Chapter 2**. The different information security strategies are firstly presented. Then a description of the concepts and the use of biometrics is presented. After that,the performance as well as the general architecture of a biometric system and its limitation were discussed. This section is fellowed by a section containing the multimodal biometric and its different concepts. Finally, this chapter is concluded by the metrics used foe the evaluation of the biometric system.

Chapter 3 deals with Cryptography and the biometric template protection schemes. Initially, this chapter presents a brief introduction to cryptography. followed by a presentation of the various vulnerabilities of the biometric system. After that , in the fellowed section the different categorizations of template protection schemes are presented.Also, this chapter include a descriptions of the three mode of Biometric-Crypto system.

Each biometric identification system involves the use of such biometric modalities and such feature extraction descriptor or classifiers. **Chapter 4** will present a theoretical explanation of the used biometric traits and the proposed feature descriptors and classifiers that have been used during the realization of this work.

Chapter 5 deals with the presentation of the obtained experimental results. The experiments were devised into two parts, the first part treats the efficiency of the proposed biometric identification systems. For that, various experiments were carried out using the biometrics modalities and features descriptors that had been discussed in the first part. Besides, this

chapter include a multimodal system experiments at three different fusion levels to overcome the drawbacks of the unimodal system.

The second part of experiments explains our third approach of cryptographic key binding schemes based on fuzzy commitment approach using a combination of two techniques in order to generate a binary template applied to an *e-voting* system. At the beginning of this chapter, we have showed and discussed in detail the *e-voting* system framework together with the experiments conducted to evaluate the performance of the *e-voting* system. At the end of this chapter, we analyze the security of this approach.

Finally, **Chapter 6** concludes the thesis and indicates the further research directions.

Chapter 2

Biometric: When Identity Matters

2.1 Introduction

INFORMATION security basically ensures the confidentiality, integrity, and availability of information. It essentially provides the necessary protection to information and the supporting processes, systems, and infrastructures from various forms of possible threats and vulnerabilities. Information security is fundamentally based on user authentication whereby an individual's identity is identified/verified through either one of the three-following means: "**by something he knows,**" "**by something he has**" or "**by something he is**" (or through combinations of any of the three means). The last authentication method "something he is" is also known as Biometrics [11].
This chapter introduces biometric and biometric technology. First, we present the concepts and the use of biometrics. Subsequently, we discuss the performance as well as the general architecture of a biometric system. After that, we present the limitations of these systems. To overcome these limitation we have introduced the notion of multimodal biometric and its different types. Finally. the issues related to the evaluation of the biometric system are cited.

2.2 Information security strategies

Proper user identification/verification is a crucial part of several application of any system's security such as physical buildings, access control and information systems. As it was mentioned previously, user identification/authentication has been traditionally based on [12]:

- Something that the user knows (typically a PIN, a password or a passphrase).

- something that the user has (e.g., a key, a token, a magnetic or smart card, a badge, a passport).

These traditional methods of the user authentication unfortunately do not authenticate the user as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier[13]. On the other hand, the third means of identification, which is biometric, has quickly established itself as the most pertinent technology for identifying individuals in a fast and reliable way. Biometric characteristics are (or rather should be) unique and not duplicable or transferable. While the advantages of biometric authentication definitely look very attractive, there are also many problems with biometric authentication that one should be aware of[14].

Table 2.1 allows us to compares the previous means of information security. It is clear that biometrics are real alternatives of traditional ways (keys, badges and other identities). They make it possible to verify that the user (the involved person) is the person he claims to be.

TABLE 2.1: Comparison between different existing security methods

Method	Example	Proprieties
What user know	User ID Password PIN	Shared Many passwords are easy to guess Forgotten
What user have	Cards Badges Keys	shared Can be duplicated lost or stolen
What user know + have	ATM card + PIN	shared PIN is a weak link (writing the PIN on the card)
What user is	Fingerprint Face Iris Voice	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

From this table, one can say that the biometrics is the most comprehensive means of identification because it increasingly connects an identity to a natural person by means of their own physical characteristics(behavioral or biological)[15].

2.3 biometrics: definitions and use

The modern world is facing major challenges, particularly within the field of information security to confirm their protection, privacy and security. One of the best solutions that have

proven their effectiveness and efficiency in this field is the biometric. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions[16, 17].

2.3.1 Biometric

Biometric is an emerging field where technology improves our ability to identify or check a person. It refers to an identification and verification technology that consists of transforming a biological, morphological or behavioral characteristic into a digital print. Its objective to attest to the uniqueness of a person from the measure of an unchangeable or immeasurable part of his body. Or one can say that biometric refers to the morphological (e.g., face, palmprint, fingerprint, iris, etc.), behavioral (e.g., voice, signature, gait, keystroke dynamics, etc.) or biological (e.g., DNA) characteristics that distinguish one person from another[18, 19].

2.3.2 Rising of biometric: a brief story

The use of biometrics could be traced back to 31000 years ago when the prehistoric men used handprints as a signature for their paintings. In China dynasties, the documents were signed using fingerprints. Joao de Barros, a 14th-century Spanish explorer and writer described that the Chinese merchants used fingerprints for business transactions. Furthermore, they took fingerprints of the hands and feet of young children on paper using ink to distinguish them from each other. It is one of the oldest methods of biometrics in practice and is still used today. In the commercial trade of Babylon, 3000 years BC, the same system was used. In pre-Columbian America, many architects also left traces of their colorful hands on the walls of converted caves[20, 21].

In 1890, Alphonse Bertillon described a new system called 'Bertillonage,' to identify convicted criminals and turned biometrics into a distinct field of study. He used different body measurement such as the size of the skull or the length of their fingers to identify individuals; this system faced some problems when it was discovered ; some people shared the same measurements and therefore were convicted by mistake. By the late 1800s, known as fingerprinting was developed known as fingerprinting; this used fingerprint patterns and ridges to identify individuals, this characteristic was found to be unique for each and therefore more reliable in identification[22, 23].

Today, biometric systems are being widely developed and deployed to provide greater security to users. There is an increased awareness of the value of biometric systems. Biometrics which has advanced a lot in the past few years. Some of the features that are used at

present include face recognition, voice recognition, speech recognition, Retina scan, iris scan, signature identification, fingerprint etc.[24].

2.3.3 Objectives associated with biometrics

Several reasons can justify the use of biometrics[18]:

1. **High security:** Combined with other technologies such as encryption or smart card, some systems make it very difficult to attempt fraud.
2. **Comfort:** By simply replacing traditional methods, such as a password, biometrics makes it possible to respect the basic rules of security. And when these rules are respected, biometrics prevent administrators from answering many requests for password changes.
3. **Security / Psychology:** In some cases, especially for e-commerce, the user has no confidence. It is essential for e-commerce players to convince consumers to make transactions. One means of biometric authentication could change the consumer behavior.

This complementarity makes it possible to imagine an efficient, integrated and highly dissuasive systems. If it is technically easy to discover a password or fraudulently obtain an access badge or a magnetic card, it is almost impossible to modify, steal or copy a human physiological or behavioral characteristic.

2.3.4 Use of biometrics

The scope of biometrics is very vast. Indeed, all the domains that need to verify or determine the identity of people that are concerned. This is why we attempt to find applications of biometrics to manage access to physical resources (such as access to secure locations) and logical access (such as e-commerce). Biometric is also of a great importance to several countries (Europe, the United States, etc.) to produce safer identity documents, such as the national identity card or the biometric passport. Note that, in Algeria, the biometric passport is now deployed. It incorporates an RFID (Radio-frequency identification) chip that contains at least two biometric traits: a fingerprint and a digital face image. Finally, biometrics does not only have security-oriented applications, but also applications that facilitate the daily lives of users. Thus, biometric is used in some airports so that regular customers are allowed to save time and to not waste it during boarding.

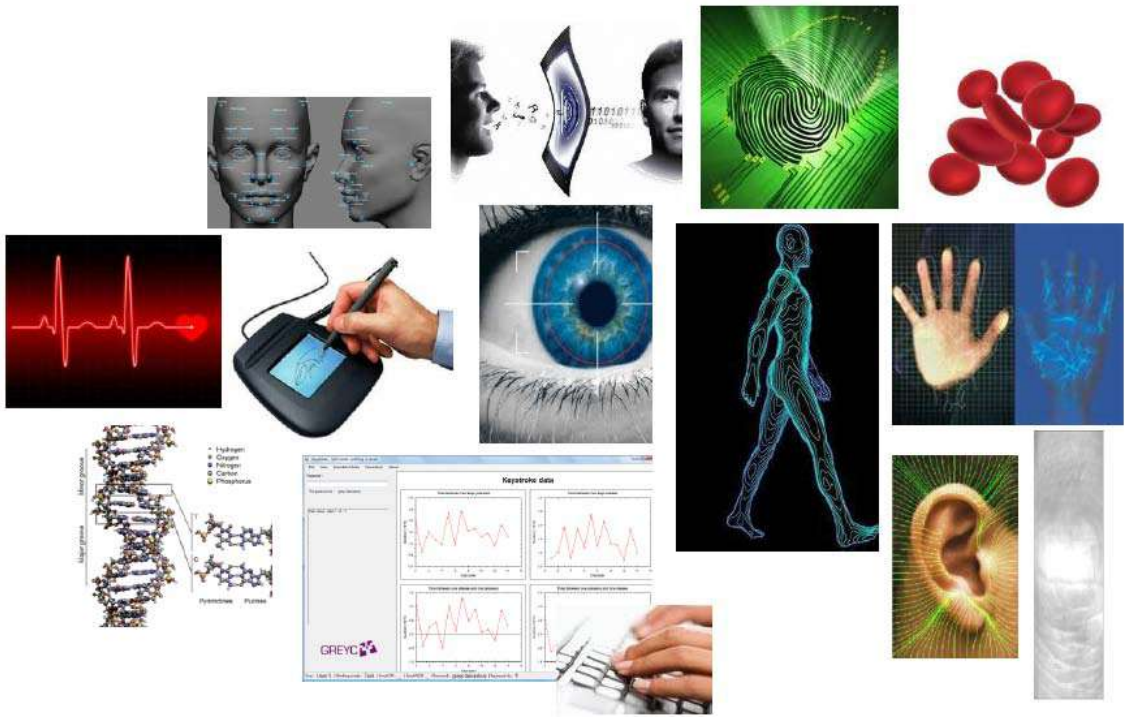


FIGURE 2.1: Some Biometrics Modalities.

2.4 Taxonomy of Biometric Modalities

The biometric characteristics by which the identity of an individual can be verified are called biometric modalities. Figure 2.1 illustrates an example of some biometric modalities. These modalities are based on the analysis of data related to the individual and are classified into three categories: Morphological biometrics is based on specific physical features that, for all people, are permanent and unique (fingerprint, face, palmprint, iris, etc.). Behavioral biometrics is based on the analysis of an individual's behavior (gait, keystroke dynamics, signature, etc.). Biological biometrics is based on the analysis of biological data related to the individual (saliva, DNA, etc.). In practice, any morphological or behavioral characteristic can be considered a biometric characteristic, so far as it satisfies the following properties[11]:

- ▷ **Universality:** all persons to be identified must possess it.
- ▷ **Uniqueness:** the information must be as dissimilar as possible between the different people.
- ▷ **Permanence:** the information collected must be present throughout the life of an individual.
- ▷ **Collectability:** the information must be collectable and measurable to be used for comparisons.

- ▷ **Acceptability:** the system must respect certain criteria (acquisition facility, rapidity, etc.), to be used.

Biometric modalities do not possess all these properties, Or they may possess them but with different degrees.. Table 2.2, extracted from[25], compares the main biometric modalities according to the following properties: universality, uniqueness, permanence, collectability, acceptability and performance. This table shows that no modality is ideal and that they can be adapted to particular applications. For example, DNA-based analysis is one of the most effective techniques for verifying or identifying an individual's identity[39]. Nevertheless, it cannot be used for logical or physical access control for reasons of computational time, but also, because no one would be ready to give a little blood to do the verification. The choice of the modality is thus carried out according to a compromise between the presence or the absence of some of these properties according to the needs of each application. Note that the choice of biometric modality may also depend on the local culture of users. In Asia, methods requiring physical contact such as fingerprints are rejected for hygienic reasons while contactless methods are more widespread and accepted.

TABLE 2.2: Properties of biometric modalities according to the following properties: (U) Universality, (N) Uniqueness, (P) Permanence, (C) Collectability, (A) Acceptability, (E) Performance (the number of stars in the performance column is related to the obtained value of Equal Error Rate (EER) in the state of the art (Extract from[25]))

Biometric information	U	N	P	C	A	E
DNA	Yes	Yes	Yes	Not really	Not really	*****
Blood	Yes	No	Yes	Not really	No	*
Gait	Yes	No	Not really	Yes	Yes	***
Keystroke	Yes	Yes	Not really	Yes	Yes	****
Voice	Yes	Yes	Not really	Yes	Yes	****
Iris	Yes	Yes	Yes	Yes	somewhat	*****
Retina	Yes	Yes	Yes	Yes	somewhat	*****
Face	Yes	No	Not really	Yes	Yes	****
Hand Geometry	Yes	No	Yes	Yes	Yes	****
Hand veins	Yes	Yes	Yes	Yes	Yes	*****
Ear	Yes	Yes	Yes	Yes	Yes	*****
Fingerprint	Yes	Yes	Yes	Yes	Yes	****

The different biometric techniques have in common is to establish the identity of a person by analyzing its proper characteristics. With the introduction of digitization, these techniques have been refined, but their principle remains the same.

In the next subsections, we will give an overview of biometric modalities that can be classified into three main categories i.e. physical (morphological), behavioral or biological characteristics. There are numbers of modalities in these categories which can be used according to the application.

2.4.1 Physical biometrics (Morphological)

The morphological biometric modalities are based on the identification of physiological traits that, for every person, are unique and permanent. This category groups the hand (for fingerprint, palmprint, finger knuckle print and hand geometry), the eye (for iris and retina) and the face. This list can be extended by other modalities such as the shape of the ear, the finger veins of the hand, ... etc.

❶ **Fingerprint:**Fingerprint biometrics ([26]) is probably the most usual form of biometrics available today. It can be considered the oldest method of identity authentication and has been used since 1896. Following is the basis of fingerprint recognition. The fingertips have corrugated skin with a line like ridges flowing from one side of the finger to another. The flow of the ridges is non-continuous and forms a pattern. The discontinuity in the ridge flow gives rise to feature points, called minutiae, while the pattern of flow gives rise to classification patterns such as arches, whorls, and loops.(see Figure 2.2).

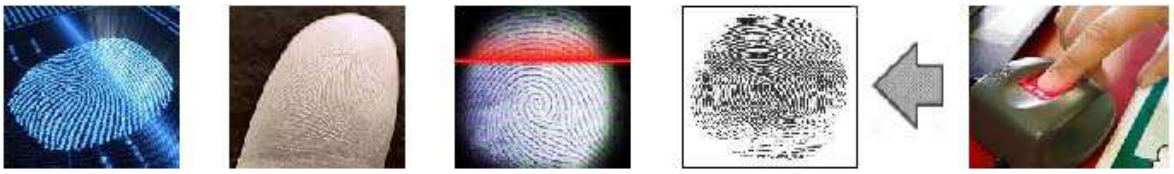


FIGURE 2.2: Empreinte digitale.

❷ **Hand Geometry:**Hand geometry[27] is the longest implemented biometric type, debuting in the market in the late 1980s. The systems are widely implemented for their ease of use, public acceptance, and integration capabilities. The devices use a simple concept of measuring and recording the length, width, thickness, and surface area of an individual's hand while guided on a plate. (Figure2.3). However, this biometric is subject to changes

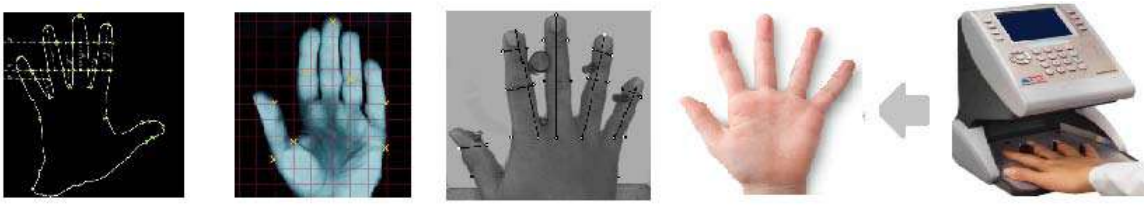


FIGURE 2.3: Hand Geometry.

in the shape of the hand associated with aging,real twin or even by people with close hand shapes.

❸ **Finger Knuckle-Print:** The finger back surface, also known as the dorsum of the hand or Finger Knuckle-print(FKP)[28], can be highly useful in user identification. The image-pattern formed from the finger-knuckle bending is highly unique and makes this finger knuckle surface a distinctive biometric identifier. The knuckle print modality contains distinctive features such as principal lines, secondary lines and ridges, which can be extracted from the low resolution images(see Figure 2.4). As another advantage of FKP biometric, the human hand contains several fingers, This is why , an ideal FKP identification system can be based on the fusion of these fingers in order to improve the identification accuracy.

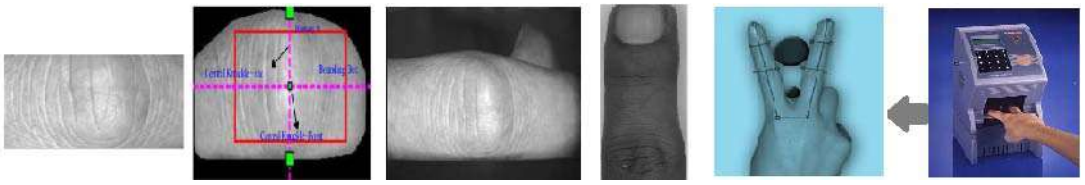


FIGURE 2.4: Finger Knuckle-Print.

❹ **Palmprint:**Palmprint [29] is the region between wrist and fingers and has features like principle lines, wrinkles, ridges, minutiae points, singular points, and texture pattern which can be extracted from a low resolution image. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints or even Finger Knuckle-Print.A palm print image is shown in Figure 2.5. Among the biometrics modalities, palmprint has received a wide attention from the researchers as a new biometric recognition technology.

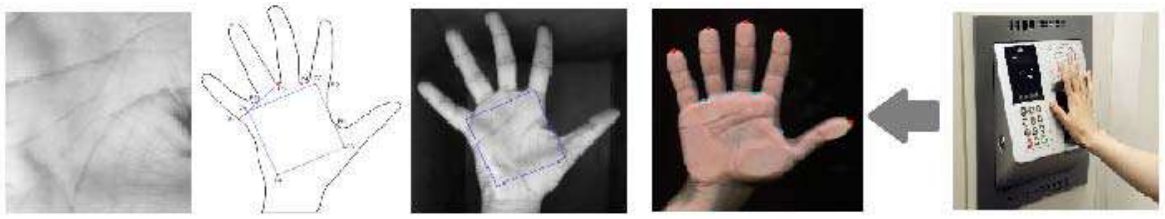


FIGURE 2.5: Palmprint.

❺ **Face:** Face[30] recognition is probably the most common biometric characteristic used by humans to make a personal recognition.Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips, and chin or on the overall analysis of the face image that represents a face as a number of recognized faces (see Figure 2.6). In a face recognition system, it is hard to match face images taken from two different views and under different illumination conditions. Moreover, the face of an individual can be changed by times. All

this criteria make face recognition system to be uncertain if really the face itself is enough to recognize a person from a large number of identities.

FIGURE 2.6: The Face.

❻ **Iris:**The iris [31] of the eye is the colored annular area that surrounds the pupil (Figure 2.7). Iris patterns are unique. Each iris is distinctive and even the irises of identical twins are different. Also even right and left eye of same person.An iris image is typically captured using a non-contact imaging process. The image is obtained using a device that contains an infrared camera. Iris recognition is a new technology since it did not really develop until the 1980s.The identification error rate using iris technology is believed to be extremely small.Iris recognition technology is being used in various domain such as banks and financial organizations or military and high security area, replacing the cumbersome and time taking, PIN based, and password based systems.

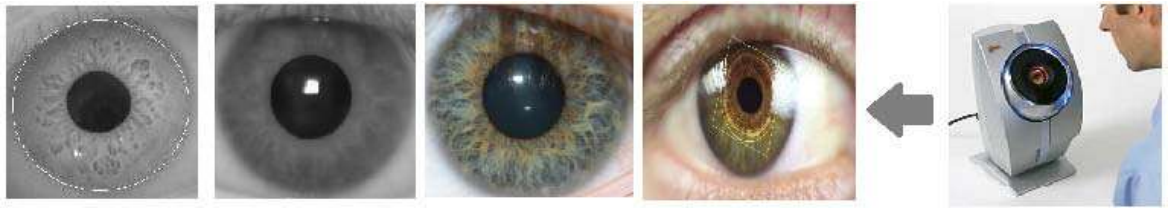


FIGURE 2.7: Iris.

❼ **Retina:**The retinal [32] vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye (Figure 2.8). It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature. Retina image acquisition requires a person to look through a lens at an alignment target. Therefore, it implies cooperation of the subject,entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric.

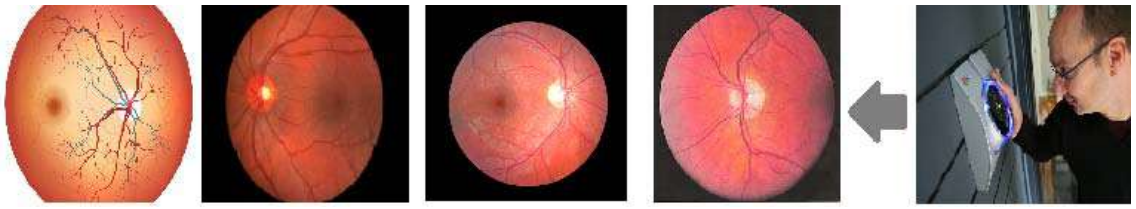


FIGURE 2.8: Retina.

❽ **Ear:**The ear[33] is made up of standard features including the helix, the antihelix, the lobe, and the u-shaped intertragic notch between the ear hole and the lobe. Figure 2.9 shows the locations of the ear anatomical features. The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark location on the ear. No commercial systems are available yet and authentication of individual identity based on ear recognition is still a research topic. Among the popular biometrics, ear biometrics resembles face most. They all make use of facial features and face the same problems, such as illumination, head rotation and occlusion. But it dose have several advantages over face. Ear has a rich and stable structure that is preserved from birth into old age.

FIGURE 2.9: Ear.

2.4.2 Behavioral biometrics

Behavioral biometric trait is a particular characteristics that can be acquired from user actions such as voice, gait, keystroke dynamics or signature. In this section we present a review about some of the commonly used behavioral biometric traits that have been proposed in the literature to design a biometric authentication systems[34]:

❶ **Voice:**Voice [35] recognition or speech recognition is a technology through which sounds, phrases and words voiced by human beings are transformed into electrical signals. Voice is noticed as unique feature of every individual that utilizes different qualities of the voice such as the pitch, time, and intensity used to identify one from other. the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice is also not very distinctive and may not be appropriate for verification or identification purposes. Speaker recognition is most appropriate in phone-based applications such as intelligent personal assistant like siri developed by apple company and cortana of MICROSOFT.(see Figure 2.10).

FIGURE 2.10: Voice.

❷ **Signature:**Signature [36] is defined as the way of person how signs his or her name and it's known to be a characteristic of that individual (Figure 2.11). Signature based recognition system can be operated in two different ways: **Static mode** where users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signature by analyzing its shape. This group is also known as "off-line". the second mode is **Dynamic**, In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Some systems also operate on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as "on-line". Dynamic information usually consists of the following information: spatial coordinate (x(t),y(t)), pressure, azimuth, inclination and pen up/down. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

FIGURE 2.11: Signature.

❸ **Keystroke dynamics:**Keystroke [37] dynamics refers to the process of measuring and assessing humans typing rhythm on digital devices. Such device, to name a few, usually refers to a computer keyboard, mobile phone, or touch screen panel. A form of a digital footprint is created by human interaction with these devices. These signatures are believed to be rich in cognitive qualities, which is fairly unique to each individual and holds huge potential as a personal identifier(see Figure 2.12). Keystroke dynamic features are based on time durations between the keystrokes. Some variants of identity authentication use features based on inter-key delays as well as dwell times-how long a person holds down a key. So no special hardware is required for keystroke analysis, just the usual computer keyboard. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

FIGURE 2.12: Keystroke dynamics

❹ **Gait:** Gait [38] is one of the newer technologies and is yet to be researched in more detail. Basically, gait refers to 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 (Figure 2.13). Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric. Since video-sequence is used to measure several different movements this method is computationally expensive. Gait may not stay invariant especially over a large period of time, due to large fluctuations of body weight, major shift in the body weight (e.g., waddling gait during pregnancy, major injuries involving joints or brain (e.g., cerebellar lesions in Parkinson disease), or due to inebriety (e.g., drunken gait). This technology is currently used in hospitals to determine medical issues. Athletes use gait technology to optimize and improve their performance.

FIGURE 2.13: Gait.

2.4.3 Biological biometrics

Another category that is the study of biological traits.This is a biometric characteristic that is primarily based on an individual's anatomy or detailed physiology. It includes features such as odor, blood, saliva, hair, DNA, facial thermography and shape of the hand veins, etc.

❶ **DNA analysis:** DNA (Deoxyribo Nucleic Acid)[39] is the ultimate unique code for persons individuality except for the fact that identical twins have the identical DNA pattern. DNA is the part of a cell that contains genetic information (chemical structure) unique for each person that is used in a form of identification. DNA of a person can be located throughout his/her entire body. DNA is present in a number of bodily materials such as blood, saliva, hair, teeth, mucus and semen.

The use of DNA in crime investigation has grown in recent years. It helped law enforcement in a great way to identify the criminals and solve difficult crimes.(see Figure 2.14).

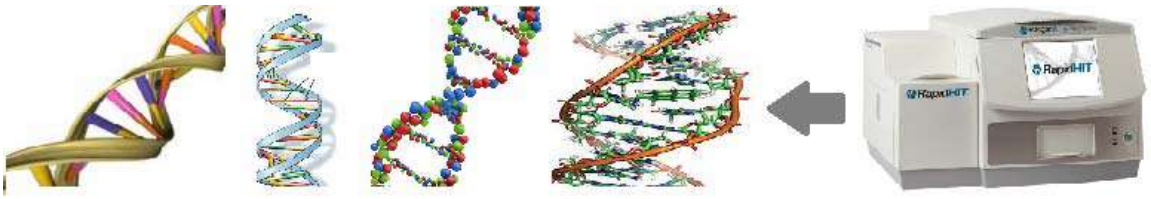


FIGURE 2.14: DNA.

❷ **Hand Vein:** Hand Vein[40] based recognition system is a system for identification using a person's unique vein patterns(Figure 2.15) .Veins as a biometrics tool involve the measurement of the blood vessels on the back of palmprint or a single finger of hand.The technology works by identifying the subcutaneous (beneath the skin) vein patterns in an individual's hand. When a user's hand is placed on a scanner, a near-infrared light maps the location of the veins. The red blood cells present in the veins absorb the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white. The current uses of vein technologies can be found in various applications such as Security systems, logical control, healthcare, banking and financial services. An example is in the Bank of Tokyo-Mitsubishi in Japan, the palm vein biometrics system is already being used. Vein biometrics are also used in the testing of major military installations.

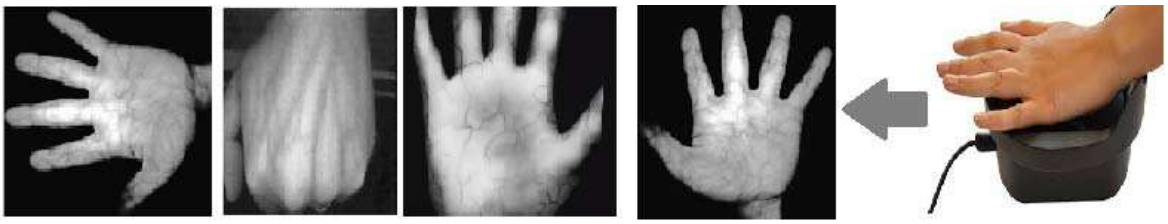


FIGURE 2.15: Hand Vein.

❷ **Facial Thermography:** Biometrics Facial thermography[41] detects heat patterns created by the branching of blood vessels and emitted from the skin. These patterns, called thermograms, are highly distinctive. Even identical twins have different thermograms. Developed in the mid-1990s, thermography works much like facial recognition, except that an infrared camera is used to capture the images. , Infrared systems work accurately even in dim light or total darkness.(see Figure 2.16)

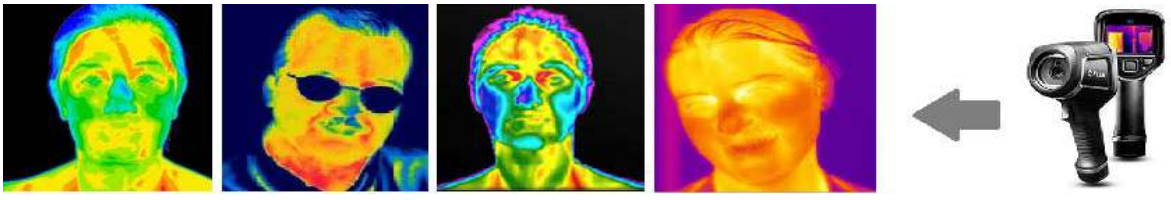


FIGURE 2.16: Facial Thermography.

2.4.4 Comparative Study Of different Biometric Techniques

As it is mentioned previously, There are different biometric traits could be used in authentication system which relies on the application context. Each trait could be used in certain context but others not. hereafter, we give the advantages and the disadvantages of most used biometric techniques in market which can help to choose the appropriate used traits as summarized in Table 2.3 :

TABLE 2.3: Advantage and Disadvantage of Biometric Techniques

Method	Advantages	Disadvantages
Finger Print	• High Reliability • Highly Distinctive • Proven Accuracy	• Injury can affect • Dry skin can cause difficulties • Poor environment
Hand Geometry	• Small Template • Unaffected by skin condition	• Injury can affect • Size of Scanner • Low Distinctiveness
Face	• Efficient Process • High Acceptance	• Face change over time • Can be manipulated by surgery • Cannot be distinguish between twins
Iris	• Uniqueness, Robust • Highly Distinctive	• Complex Processor and high cost • Poor environment
Voice	• High level of user acceptance • Low training requirement	• Voice and language change over time • Easy to manipulate • Low Accuracy • Flu or Throat infection
Signature	• High level of user acceptance • Low training requirement	• Unstable over time • Changes over time • Low distinctiveness
DNA	• High distinctiveness • unchanged over time	• high cost • Low level of user acceptance

2.5 Biometric System Conception

2.5.1 Enrollment, verification and identification

before talking about the biometric system, the first question that is posed is what is a or what does biometric system mean?.A biometric system is a technological system that exploit information about a person biometric traits to either identify or verify that person. Looking at biometric systems in a more general way will reveal certain things all biometric-based authentication systems have in common. In general such systems work in two phases[34](see Figure 2.17):

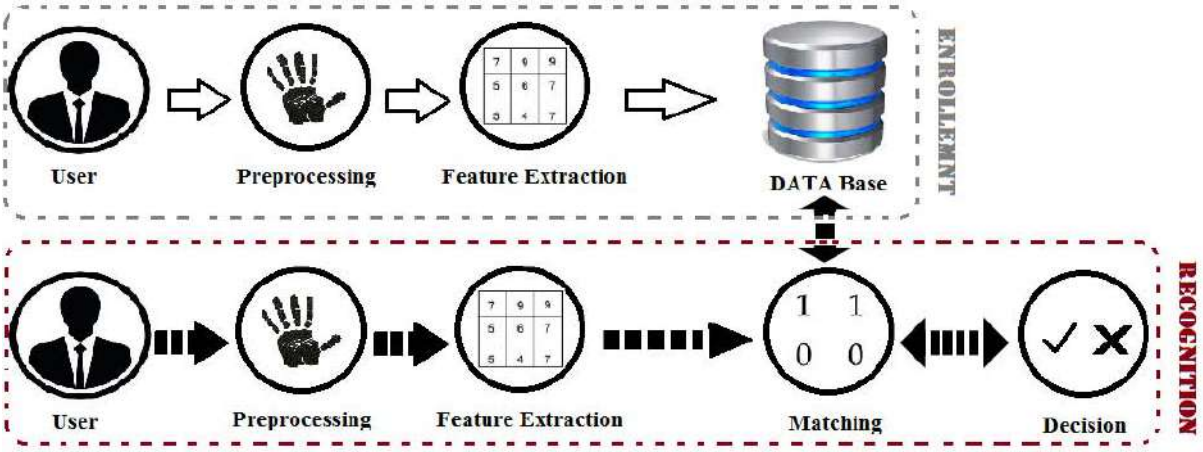


FIGURE 2.17: Biometric System Structure.

❒ **Enrollment:** In this mode biometric user data is acquired. This is mostly done with some types of biometric scanner. After that, the gathered information is stored in a central database where it is labeled with a user identity(e.g.name, identification number) to facilitate recognition[42, 43].

❒ **Recognition:** Again biometric user data is acquired first and used by the system to either *verify* the users claimed identity or to *identify* who the user is.

❶ **Verification mode:** In verification mode, which is one-to-one $(1:1)$ matching process, the system verifies the claimed identity by comparing it with the stored one. If the matching score of the claimed identity greater than a predefined threshold $\alpha \in (0,1)$, then the claimed identity is accepted as genuine, otherwise, the claimed identity is rejected as imposter. So, authentication process could operate based on verification mode and could be implemented as a binary classification problem. The decision rule is calculated and based on the following formula[44]:

$$S(u_i) = \begin{cases} Genuine & \text{if } S(u_i) > \alpha \\ imposter & \text{otherwise.} \end{cases} \tag{2.1}$$

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

❷ **Identification mode:** In identification mode, which is one-to-many $(1 : N)$ matching process, the system recognizes the presented biometric sample by comparing it with all stored templates (i.e., a template for each user), where the matching stage estimates the user identity based on the highest matching score and a designated threshold (i.e., there is multiple matching scores will be generated, one for each user, in which the highest score will be selected).
let us consider V_U the biometric features extracted by the system when a user U is in front of it.So, identification involves determining the identity of $I_i, i \in [0, 1, 2, ..., N]$ where $I_1, I_2, ..., I_N$ are user identities previously enrolled in the system, and I_0 indicates an unknown identity. The identification function f can be defined by[11]:

$$f(V_U) = \begin{cases} I_k & \text{if } Max_{1 \leqslant k \leqslant N} S(V_U, M_k) > \alpha \\ I_0 & \text{otherwise.} \end{cases} \tag{2.2}$$

where M_k is the biometric model corresponding to the identity I_k; S is similarity function, α is the decision threshold.
Such biometric identification system can work into two modes of identifications: *open-set* and *closed-set* identification.
■ ***Open-set* identification:**it is unknown whether the person presented to the biometric system for recognition has enrolled in the system or not. Therefore, in this case, the system needs to decide whether to reject or recognize him as one of the enrolled person.
■ ***closed-set* identification:** any person presented to the biometric system for recognition is known to be enrolled in the system; thus, no rejection is needed in principle unless the quality of the input biometric trait is too low to process.

2.5.2 Biometric system architecture

The basic biometric system architecture consist of a four main stages to recognize persons from their biometric traits which include a Data acquisition followed by Region Of Interest (ROI) extraction. After ROI extraction, features are extracted using the feature extraction algorithms. Then matching is done on the basis of the extracted features. The person is then accepted or rejected[44].
❶ **Data acquisition stage:** in this module a sensor collects the raw biometric data and converts the information to a digital format. The quality of the data captured typically depends on the intuitiveness of the interface and the characteristics of the sensor itself. The sensor can be a camera, a fingerprint reader, a microphone, etc.).

❷ **Feature Extraction stage:** This module is responsible for extracting feature values of a biometric trait by applying the feature extraction algorithm. As an example, if hand geometry would be used as a biometric sample then feature values would include width of fingers at various locations, width of the palm, thickness of the palm, length of fingers etc.The outcome of this stage is a biometric template which contains only the discriminatory information necessary for recognizing the person. Typically, a biometric template is unique for each persons and relatively invariants.
The obtained biometric template is then stored in the system database module, which is used by the biometric system to store the biometric templates of the enrolled users.
❸ **Matcher stage:** In this stage a matching algorithm compares the new biometric template (the query) to one or more templates kept in data storage and creates a "match score". The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.
❹ **Decision stage:** The users identity is either established or a claimed identity is accepted or rejected.This is done based on the results of the matching modules. This can either be automated or human-assisted.

2.5.3 *On-line* and *Off-line* Biometric system

In addition to the feature selection process, the image acquisition method is another factor to consider. Generally speaking, biometric recognition systems are classified into two main categories: *on-line recognition* and *off-line recognition* [18].
■ ***off-line recognition:*** An off-line biometric system processes the images (biometric modalities) captured previously. Such as images obtained from fingertips anchored digitally by a digital scanner. These approaches can provide high resolution images and are suitable for methods that require fine resolution images to extract lines. However, these methods are not suitable for online security systems since two steps are required: anchor fingers to get modality images on papers and then scan them to get digital images.
■ ***On-line recognition:*** In this system, a specific capture device for each modality (as an example a CCD digital camera (*Charged Coupled Device*)) to capture the modality images, is used. The acquired digital images are processed in real time. For example, the *on-line signature* is digitized directly by a device that makes it possible to sample the signals at a fixed frequency, when you sign. As a result, the acquisition of an *on-line signature* requires a specific sensor. A digital tablet or a touch screen can be enough for this task.

2.6 Multimodal Biometric Systems

Biometric recognition systems which use a single biometric trait of the individual for identification and verification are called unimodal systems. when the ones that can use or are capable of using a combination of two or more biometric traits are called multimodal biometric systems. Despite having many inherent advantages, the large scale deployment of biometric identification systems have been hampered due to various reasons. Theoretically, unimodal biometric identification might seem very proficient but in reality there are numerous challenges when enrolling large populations using just a unimodal biometric. Unimodal biometric system have some limitations over recognition like noise in sensed data, intra-class variation,non-universality, distinctiveness and spoof attacks. Therefore, unimodal biometric system is less secure and less reliable and this is the reason that unimodal biometric systems are become less acceptable where high security required [45]. In this section, we will discuss the limitations of unimodal biometric systems and how these limitations are overcome by the use of multimodal biometric systems.

2.6.1 Unimodal Biometric System limitations

Biometric systems that operate using any single biometric characteristic have the following limitations [26, 46] :

- **Noise in the captured data:** The captured biometric trait might be distorted due to imperfect acquisition conditions. This limitation can be seen in applications which use facial recognition. The quality of the captured facial images might get affected by illumination conditions and facial expressions. Another example could be in fingerprint recognition where a scanner is unable to read dirty fingerprints clearly and leads to false database matches. An enrolled user might be incorrectly rejected whereas an impostor might be falsely accepted.

- **Intra-class variations:** The biometric data acquired from an individual during the phase of recognition may be largely different from the data that was used to generate the template during enrollment. This can affect the matching process significantly. This variation is typically caused due to incorrect interaction with the sensor, or when sensor characteristics are changed during the identification/verification phase.

- **Non-universality:** it might not be compatible with certain groups of population. Fingerprint images might not be properly captured for the elderly and young children because of faded fingerprints or underdeveloped fingerprint ridges. Though the biometric traits are expected to exist among every individual in a given population, there

could be some exceptions when an individual is unable to provide a particular biometric. For example, iris images might not be acquired if the subject has a pathological eye condition.

- **Distinctiveness:** within a large population, unimodal biometrics is prone to inter-class similarities. Facial recognition may not work correctly for identical twins as the camera might not be able to distinguish between the two subjects leading to inaccurate matching.
- **Spoofing attacks:** An imposter may make different attempts to spoof the biometric trait of a legitimate user in order to circumvent the security of the system. Unimodal biometric systems are quite vulnerable to spoof attacks where the data can be imitated or forged. For example, fingerprint recognition systems can be easily spoofed using rubber fingerprints.

some types of unimodal biometric system limitations are illustrated in Figure 2.18.

FIGURE 2.18: Some Unimodal Biometric System limitations.

2.6.2 Biometric Multi-modality

As biometrics attracts much attention from many areas, the demand of high accuracy and reliability is also increasing. Although various biometric systems have been developed and improved, there are still limitations which have to be overcome to meet stringent performance requirements from many applications. Nowadays, most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication. These systems are vulnerable to variety of problems as treated in subsection (2.6.1). Those limitations imposed by the unimodal system can be overcome by the integration of multimodal based identification system. Multimodal biometrics refers to the use of a combination of two or more biometric traits in a recognition system. As an example, a system that uses the combination of two modalities such as finger knuckle-print and hand geometry or the use of two representations of the same modality can be considered as a multimodal biometric system. Multimodal biometrics provides supplementary information among different modalities in order to increase the recognition performance in terms of accuracy and reliability. Multimodal biometric systems can alleviate many of the limitations of biometric systems because the different biometrics sources usually compensate for the inherent limitations of the other sources[47].

2.6.3 Data Fusion principal

Data fusion is a technique used to process information from multiple sources[48] . It consists of combining data from several sources in order to obtain a better decision than that obtained from each of the sources considered separately[49]. The used systems utilize various techniques from various fields such as signal processing, artificial intelligence, pattern recognition, classification, etc. In general, data fusion is an integration operation of several data in order to extract a new information which will be more representative of all the data. Currently, data fusion is becoming increasingly important in many areas. It can effectively help scientists to extract the more relevant and accurate information. Data fusion was first considered to improve the answers quality to the problems raised by the military but today it greatly affects areas such as: remote sensing, weather forecasting, multimodal biometrics, medical application and robotics.

It is obvious that the integration of the Data fusion in the conception of biometric system will increase the efficiency and accuracy. These improvements put us in front of several challenges.Successful pursuit of these biometric challenges will generate significant advances and improvements. Hence, the challenges in designing a biometric multimodal systems are :

1. The sensors used for acquiring the data should show consistency in performance under variety of operational environment. The sensor should be fast in collecting quality images from a distance and should have low cost with no failures to enroll.

2. The information obtained from different biometric sources can be combined at four different levels such as sensor level, feature level, score level and decision level (see subsection 2.6.5). Therefore, selecting the best level of fusion will have the direct impact on performance and cost involved in developing a system.

3. There are numbers of techniques available for data fusion in biometric multimodal system; the multiple source of information is available. so, it is challenging to find the optimal solution for the application provided.

2.6.4 Multimodal Biometric Sources

Multimodal biometrics does not only refer to the use of two or more separate biometric sensors. So, we shall answer this question to determine the sources of multimodal biometric. 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 (see Figure 2.19). In general, there are five types of multimodal biometric systems, in the first four scenarios

described below, information fusion is accomplished using a single trait, while in the fifth scenario multiple traits are used[50, 51].

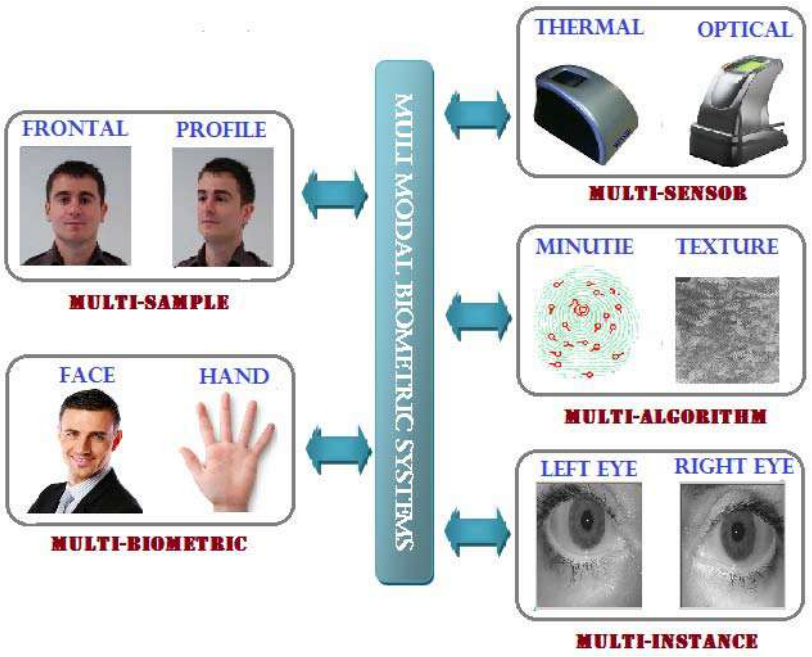


FIGURE 2.19: Some Unimodal Biometric System limitations.

1. **Multi-sensor systems:** These systems employ multiple sensors to capture a single biometric trait of an individual in order to extract diverse information from captured images.A face system, for example, a multiple 2D camera can be used, also, an infrared sensor may be deployed along with a visible-light sensor to acquire the subsurface information of a person's face. Another example of multi sensor system is those systems that exploit a multi/hyper spectral camera to acquire images of the iris, face or palmprint. In the case of the fingerprint, an optical sensor and a thermal sensor may be used to acquire the fingerprint.

2. **Multi-algorithm systems:**In this integration scenario, multi-algorithm systems apply different feature extraction algorithms on a single biometric trait. For example, a texture-based algorithm and a minutiae-based algorithm can operate on the same fingerprint image in order to extract diverse feature sets that can improve the performance of the system.These systems do not necessitate the deployment of new sensors and, hence, are cost-effective compared to other types of multi biometric systems. On the other hand, the introduction of new feature extraction and matching modules can increase the computational complexity of these systems.

3. **Multi-instance systems:** In these systems (also referred as a multi-unit in the literature) a multiple instances of the same individual body trait are deployed. For example,

the left and right index fingers, or the left and right irises of an individual, may be used to verify a person identity. Multi-instance systems are especially beneficial for users whose biometric traits cannot be reliably captured due to inherent problems. For example, a single finger may not be a sufficient discriminator for a person having dry skin. However, the integration of evidence across multiple fingers may serve a good discriminator in this case.

4. **Multi-sample systems:** Multi-sample systems leverage multiple samples of a same biometric characteristic for enrollment/recognition of individuals using a single sensor in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait. For example, a multi-sample face recognition system may require left and right profiles of face along with frontal profile. In another example, a multi-sample fingerprint recognition system can use multiple impression of the same finger.

5. **Multi-biometric systems:** Multi-biometric systems establish identity based on the evidence of multiple biometric traits. For example, a person may have to present his/her fingerprints as well as iris scan for personal identification on a multi-biometric system that uses data from both the biometric identifiers. The cost of deploying these systems is substantially more due to the requirement of new sensors. Consequently, the development of appropriate user interfaces. The number of traits used in a specific application will also be restricted by practical considerations such as the cost of deployment, enrollment time, expected error rate, user habituation issues, etc.

2.6.5 Fusion levels

The problem of consolidation of information presented by multiple biometric sources or cues from any of the types mentioned above is known as information fusion. The information fusion in a biometric system can be carried out at different levels of the biometric system[52]: at sensor level, at feature level, at matching (score) level or at decision level. These levels can be broadly classified as (i) fusion prior to matching, and (ii)fusion after matching.
Figure 2.20 indicates the various levels of fusion that are possible in the context of a biometric system.

❶ **Fusion at sensor level:** The fusion at this level [53] is defined as the process of combining the relevant information from a set of images, into a single image, where in the resultant fused image obtained will have more complete information of all the input images in a single image itself. Processing of the multiple samples images can be done with one algorithm or a combination of algorithms such as Principal Component Analysis (PCA), Discrete Wavelet Transform (DWT) or pyramidal decomposition like (Laplacian pyramid, Contrast pyramid

and Gradiant pyramid,...etc) .

❷ **Fusion at Feature level:** The fusion at this level[54] refers to the combination of deferent feature vectors obtained either with different sensors or by applying different feature extraction algorithms to the same raw data. If the features are homogeneous, the final fused vector can be computed as a weighted sum of individual features. If the features are non-homogeneous, they are concatenated to form a final feature vector.

❸ **Fusion at Matching (score) level:** Each biometric matcher output a set of possible scores along with the confidence score for each match, can be fused at matching score level[55]. Score Level refers to the combination of matching scores provided by the different systems.The score level fusion rules are divided into two main sets: fixed rules (AND, OR, majority, maximum, minimum, sum, product and arithmetic rules) and learned rules (weighted sum, weighted product and support vector machine,...etc).

❹ **Fusion at Decision level:** in this scenario of fusion, each biometric subsystem completes autonomously the processes of feature extraction, matching, and recognition. Information fusion at decision level [56] can take place when each unimodal biometric decides on the best match for the input given to it. Decision strategies are usually of Boolean functions viz., majority voting, AND rule, OR rule etc.

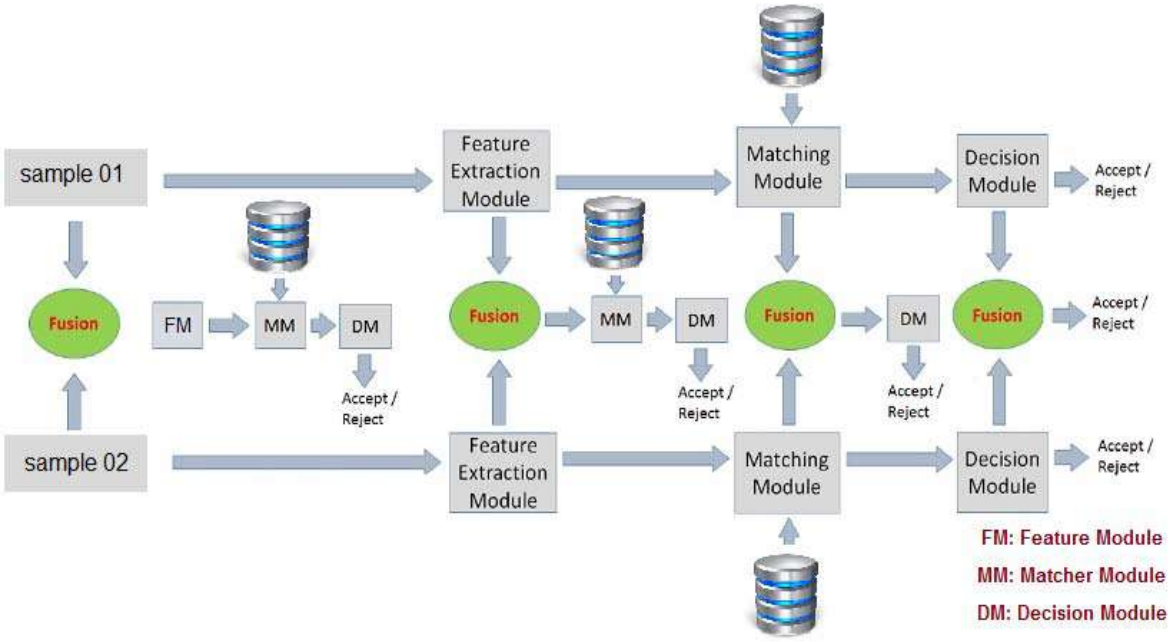


FIGURE 2.20: Multi-modal biometric system fusion levels.

2.7 Biometric System Evaluation

Assessing the performance of a biometric system is a fundamental task in the conception of the biometric verification/identification system. This section discusses methodologies for testing a biometric system and reviews various performance statistics and charts that are involved in visualizing. As it is mentioned previously,there are two types of biometric applications, namely *verification*, and *identification*. It is useful to distinguish between them here as they will have an impact on the choice of performance evaluation.

2.7.1 Error Rate Metrics

In general,there are several metrics used in the context of biometric system conception and evaluation,some of them are used in the verification application and the others are used in the identification one(*open-set / closed-set*), hereafter we give the most common metrics used[11, 18, 57, 58] :

- **False Match Rate (FMR):** an empirical estimate of the probability (the percentage of times) at which the system incorrectly declares that a biometric sample belongs to the claimed identity when the sample actually belongs to a different subject (impostor).
- **False Non-Match Rate (FNMR):** an empirical estimate of the probability at which the system incorrectly rejects a claimed identity when the sample actually belongs to the subject (genuine user).
- **False Acceptance Rate (FAR):** is the probability of cases for which a biometric system fallaciously authorizes an unauthorized person. It happens when a biometric system, solution or application inaccurately matches a biometric input with a stored template, fallaciously returning a match and granting access to an unauthorized person.
- **False Rejection Rate (FRR):** it can be defined as the contrary case of the FAR, it is the probability of cases for which a biometric system fallaciously denies access to an authorized person. It happens when a biometric system, solution or application fail to match the biometric input with a stored template, fallaciously returning a no-match and denying access to an authorized person. The False Rejection Rate (FRR) is one of the important metrics along with FAR and commonly used for assessing the performance of a biometric system,
- **Equal Error Rate (EER):** The rate at which FAR(FMR) is equal to FRR(FNMR).

FAR and **FMR** are often used interchangeably in the literature, so as **FNMR** and **FRR**. However, their subtle difference is that **FAR** and **FRR** are system-level errors which include samples failed to be acquired or compared.

Figure 2.21 shows the theoretical distribution of likelihood ratios of genuine users and impostors. The two metrics rates, FAR and FRR, are linked. They depend on a decision threshold which must be adjusted according to the targeted characteristic of the high or low security biometric system. Indeed, when the decision threshold is low, the false acceptance rate (FAR) will increase. In this case, the biometric system will accept impostors. On the contrary, when the decision threshold is high, the false rejection rate (FRR) will increase. The biometric system will then be robust to impostors but will reject genuine users.

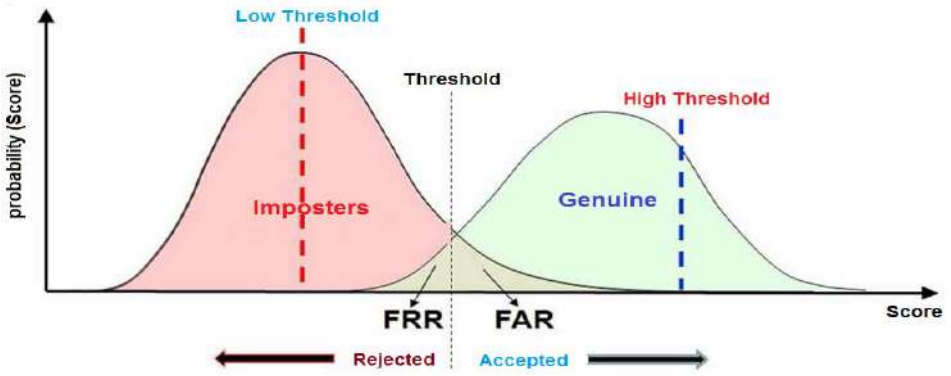


FIGURE 2.21: Distributions of genuine users scores and impostor scores

- **Genuine Accept Rate(GAR):**it is defined as a percentage of genuine users accepted by the system. It is given by $GAR = 1 - FRR$.
- **Rank One Recognition (ROR):** This rate is defined as the percentage of persons recognized by the biometric system based on a variable which is called rank. the ROR rate is calculated when $rank = 1$.
- **Rank of Perfect Recognition (RPR):** this rate is defined as at which rank the identification rate attempts 100%. One can say that when RPR increases, the corresponding identification rate is linked to a lower security level.

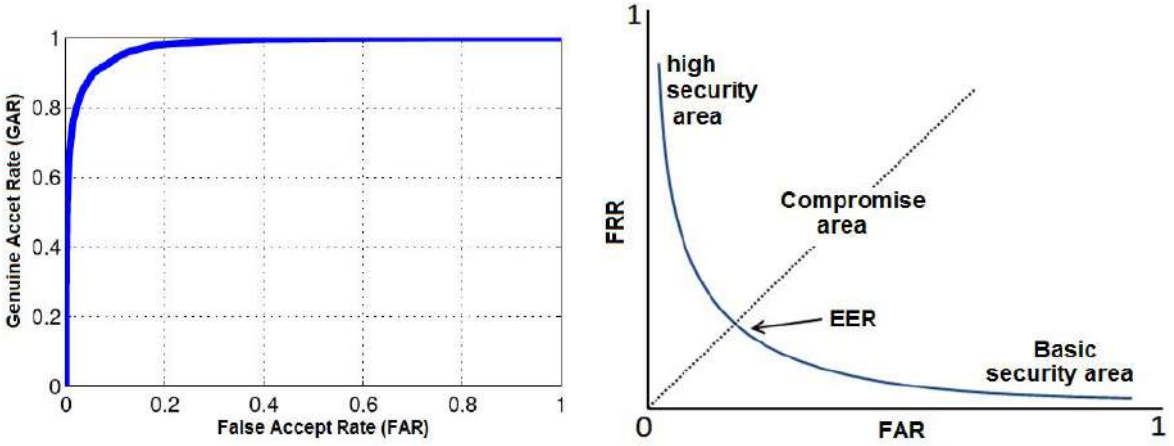
It is important to note that the performance evaluation metrics, mentioned previously, can be applied in both biometric system tasks. For the *verification* and the *open-set* identification mode, the FAR(FMR), FRR(FNMR) are often used. Generally, for the *closed-set*, the ROR and the RPR metrics are used.

2.7.2 Curves of Performance

The performance of a biometric system for different parameters (decision threshold) is graphically illustrated using specific curves. The logarithmic scale is sometimes used to make them clearer and more readable, especially in the case of comparison between biometric systems that have similar performance. A a results, we find:

- **Receiver Operating Characteristic (ROC):** One of the standard method for expressing the technical performance of a biometric system in a specific application(generally in *verification* and *open-set* tasks) is the Receiver Operating Characteristic (ROC) curve. The ROC curve is A graphical representation giving a relationship between FAR (FMR) and FRR(FNMR) (alternatively GAR against FAR). An illustration of the ROC curve is given in Figure 2.22.

- **Cumulative match characteristic curve (CMC) :** A CMC curve is a graphical representation used to evaluate the performance of a biometric identification system under *closed-set* mode. A CMC curve plot the identification rate against the rank. An example of this curve is given in Figure 2.23.



(*a*) (*b*)

FIGURE 2.22: Receiver Operating Characteristic (ROC): (*a*) GAR against FAR when the decision threshold varies, (*b*) FRR Variation according to the FAR when the decision threshold varies

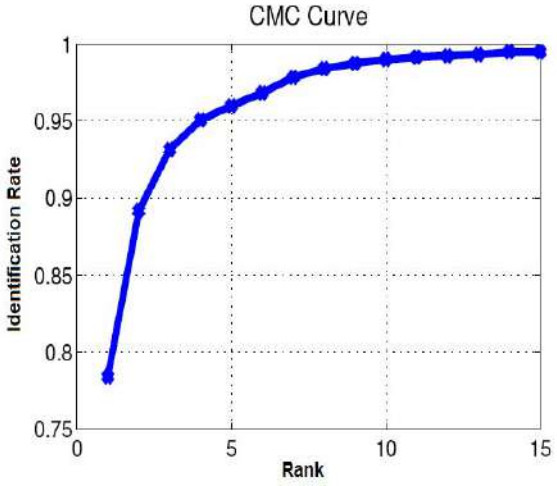


FIGURE 2.23: Cumulative match characteristic curve (CMC).

2.8 Conclusion

This second chapter has offered an overview to biometrics with the intention to introduce briefly the science and its related technology. To that end, the fundamental concepts of biometrics and its principles have been described. This description also covers the taxonomy of the existing biometric modalities and the most relevant properties of the different biometric characteristics. Furthermore, this chapter has explained the basis of a general biometric system, including their components and the most significant biometric functions: enrollment, verification and identification. After analyzing the deferent limitations of the unimodal system, the notions of multimodal biometric and its deferent concepts(sources and levels of fusion) were introduced. Finally, Metrics and charts which needed for the evaluation of biometric performance are presented.
The next chapter namely “Information Security: From cryptography to Bio-cryptography” will focus on the combination of biometric technologies with cryptography system in terms of strategies, conception and performance evaluation.

Chapter 3

Information Security: From cryptography to Bio-cryptography

3.1 Introduction

GENERALLY , there are several methods and techniques used to ensure the information security, one of the most known means are the cryptographic techniques . In cryptography, the general idea is to transform the information during a phase called encryption, before being stored or transmitted, based on a secret key. This secret key is required in order to retrieve the information from the transformed data during decryption. These secret keys are generally too long for a user to remember. Therefore, they should be stored somewhere. The drawback of cryptography lies in the fact that these keys are not strongly linked to the user identity. In order to strengthen the link between the user identity and his cryptographic keys, biometrics is combined with cryptography.

This chapter is motivated by very recent advances in the field of biometric template protection or biometric crypto-system, and its aim is to contribute to the studies of the interaction between biometrics and cryptography, presenting at the first section, a brief introduction to cryptography followed by a presentation of the various vulnerabilities of the biometric system in Section 2. Section 3 introduces the different categorizations of biometric-Crypto system for template protection schemes and presents some remarks to be discussed. Finally, in the last section, a comprehensive conclusion is given.

3.2 Cryptography: Encryption & Decryption

As it is mentioned previously, in order to secure the information during transmission or storage, the cryptography is deployed. Cryptography or Cryptology comes from the combination of the two Greek words : cryptography = " kryptós" + " graphein", Kryptós meaning hidden or secret and graphein meaning writing. Cryptography involves two phases: encryption and decryption. In *Encryption*, the data, denoted as *plaintext*, is transformed into illegible gibberish, denoted as *ciphertext*, with the help of an encryption key. The *Decryption* process is the reverse of *Encryption*, i.e., obtaining the *plaintext* from the *ciphertext*. The pair of algorithms that creates the *Encryption* and the *Decryption* is denoted as *cipher* [59]. The basic idea of cryptography is shown in Fig 3.1.

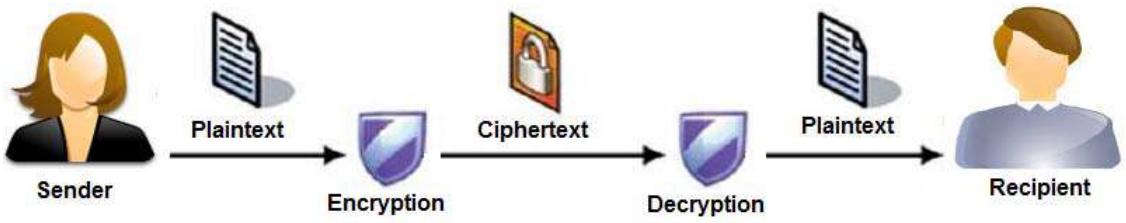


FIGURE 3.1: Basic idea of cryptography.

As a result, one can say that the cryptography is the science of keeping information secret. Recently, the advent of computer-aided information exchange has greatly increased demands upon the field, requiring it to mature quickly and develop flexible yet robust practices. These practices address the following important objectives within cryptography:

1. **Confidentiality:** Information is made unreadable to unauthorized persons or processes. This is, in part, achievable by encrypting data
2. **Authenticity:** Access to stored data is controlled by verifying potential readers.
3. **Integrity:** Information is prevented from being changed during transmission or on storage.

3.3 Symmetric and Asymmetric Encryption

Safeguarding information has become an indispensable measure in today's security world. Encryption is one important method which protects discreet information being transferred or stored. The Encryption techniques can be employed in two ways, namely Symmetric Encryption and Asymmetric Encryption.

3.3.1 Symmetric Encryption

This type of encryption techniques is also called conventional cryptography method. In symmetric encryption system both phases encryption and decryption involves the use of one single key. To illustrate the functionality of this encryption mode, let us first introduce Alice and Bob. Alice has a sensitive document and she wants to share it with Bob, she uses an encryption program to protect her document with a chosen a password or a pass-phrase. After that, she sends the encrypted document to Bob via emails . However, bob can not open this document because he does not know the password or pass-phrase which Alice uses to encrypt the document, in other words, he does not have the key to open the lock. So, Alice must share her secret key with Bob in order to unlock the document. This is a brief description of how the symmetric encryption techniques work [60]. Figure 3.2 shows a diagram of symmetric cryptographic system.

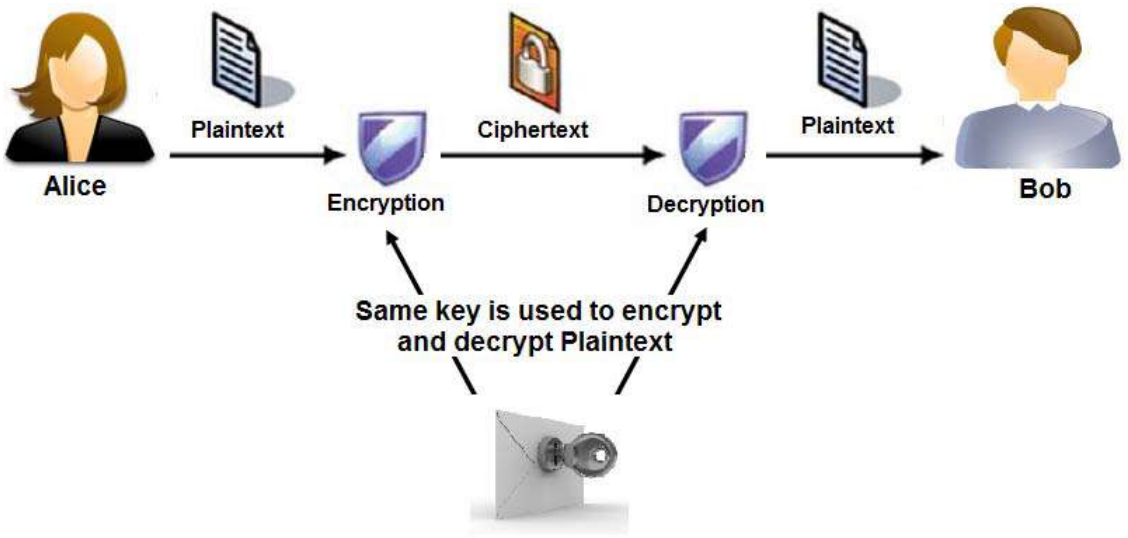


FIGURE 3.2: Basic idea of symmetric cryptography.

the symmetric-key encryption is categorized by the fact that they are fast and suitable for real-time applications. Moreover, the security provided by these systems is high as long as the key used for encryption/decryption is secret. However, those systems require additional key management techniques.

One of the main disadvantage of the symmetric-key encryption is that the same key is used for both encryption and decryption. Some cryptanalytic attacks can take place easily . Therefore, the encryption/decryption key needs to be frequently renewed.

Examples of symmetric key cryptography systems include the Data Encryption Standard (DES),Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Rivest Cipher 4(RC4) and etc..[61].

3.3.2 Asymmetric Encryption

Asymmetric encryption is also known as Public key encryption, in this scenario of encryption two encryption key are used: public and private key. these two key are relatively mathematically related. The Public key, as the name suggests, is available to everyone who wishes to send a message. On the other hand, the private key is kept at a secure place by the owner of the public key[62]. To understand how the public key cryptography works, let us introduce this example, the public key cryptography is comparable to the mailbox on the street. The mailbox is exposed to anyone who knows it's location. We can say that the location of the mailbox is completely public, anyone who knows the address can go to the mailbox and drops the letter. However, only the owner of the mailbox has a key to open it up and read the messages. Now, let us go back to technical details, when using asymmetric encryption , both Alice and Bob have to generate a key pairs on their computers. A popular and secure way for doing this is by using the Rivest-Shamir-Adleman (RSA) algorithm[63], this algorithm will generate a public and private key which are mathematically linked to each other.Public keys can be used to encrypt the data and only the owner of the private key can decrypt it. It is also known that those two pair of keys cannot be derived from each other. Figure illustrate how Alice and Bob use Asymmetric encryption.

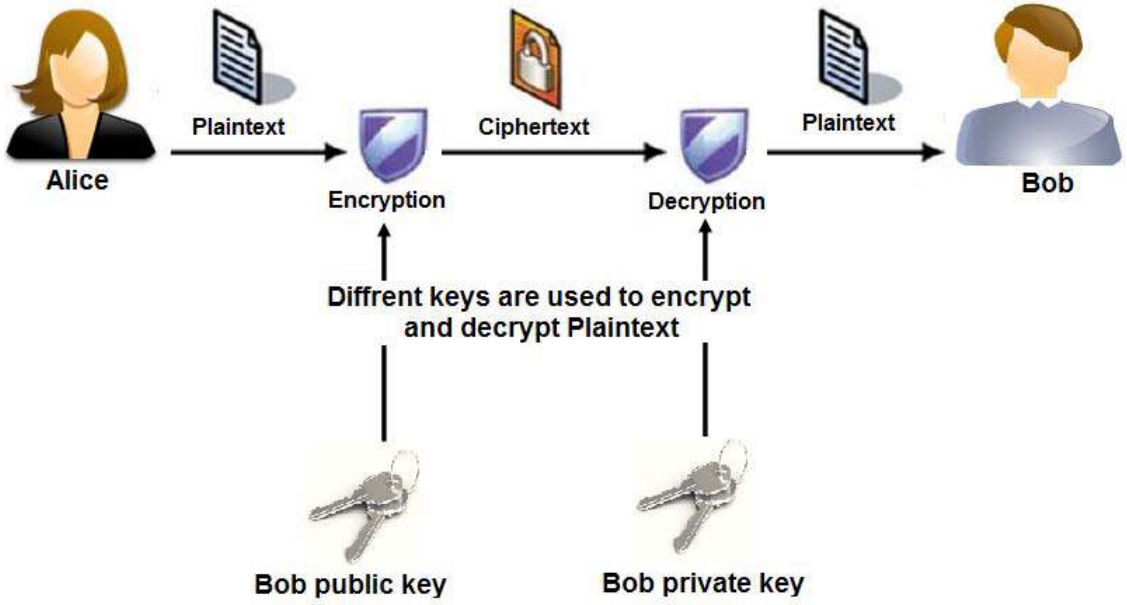


FIGURE 3.3: Basic idea of Asymmetric (public key) cryptography.

In this figure, there are two contacts: Alice and Bob. Alice wants to send a message to Bob in a secure way. Bob has a public-private key pair. He sends the public key to Alice openly. Then Alice encrypts the message with this public key and sends the ciphertext to Bob. The message can be recovered from this ciphertext only with the help of the corresponding private key. Since Bob is the only one having access to this key, he is the only one who can recover the plaintext.

Compared to the symmetric encryption techniques, asymmetric encryption techniques are categorized by the fact that they are too slow for practical purpose and computationally expensive. On the other hand, the advantage of these public key encryption techniques is that there is no need of secure key sharing but only requiring a mathematical operation to compute the relation between public and private keys.

As an example of public-key cryptosystems, the RSA (Rivest, Shamir,Adleman) algorithm [62], the Diffi-Hellman key exchange protocol [64], elliptic curve cryptography [65],etc.

3.4 Problems related to Cryptography

According to what is mentioned in the previous section and the Kerckhoffs' principle, the strength of cryptosystem whatever symmetric or public key encryption is s dependent on the secrecy of the secret or private key, respectively[66]. In addition, for security reasons, the cryptographic keys are required to be long. For example, the possible lengths of keys required in the AES are 128, 192, or 256 bits. For public-key cryptographic systems such as RSA, the key lengths are even higher (e.g., 512, 1024, or 2048 bits). Because of the large size of a cryptographically strong key, it would clearly not be feasible to require the user to remember and enter the key each time when required. However, a user cannot remember such long keys and therefore, the keys need to be stored somewhere such as computer or smart card.

the keeper of the secret cryptographic keys must be a legitimate user and should be kept in secure manner from the attackers. Traditionally, two authentication mechanism are deployed, knowledge based (e.g., passwords) or possession based (e.g., token, smart card, etc.).These authenticators are assigned to the user identity and do not necessarily indicate the presence of the person to whom they belong. Therefore, they can be easily stolen by an attacker, and in this situation, the system cannot distinguish between the attacker and a legitimate user.

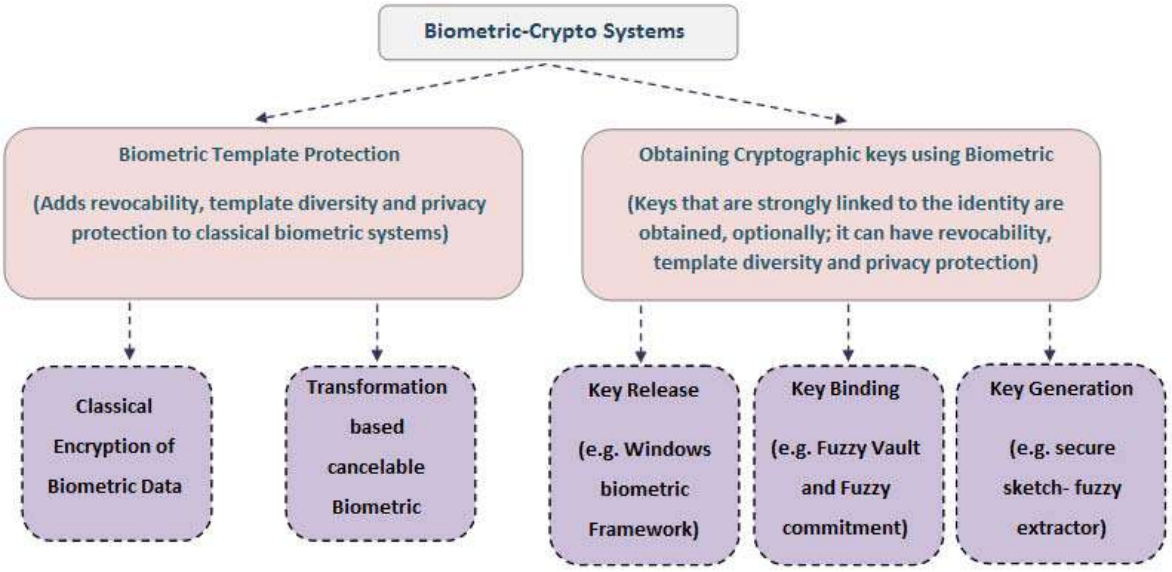


FIGURE 3.4: Categorization of Biometric template protection schemes.

3.5 Biometric-Crypto systems: An Introduction

Starting from the description of the problems related to cryptography and biometric in the last sections. Clearly, both of these techniques (biometric and cryptography) need improvements. Firstly, when identity matters, biometric authentication techniques establish itself as a powerful means for doing that. Also, biometric authentication gives a better protection against repudiation (for example in traditional authentication technique, a user can willfully share his credentials and later claim that they were stolen. Thus, such a system can be easily cheated). On the other hand,Cryptography, which is great in providing security, privacy, and anonymity.The common verification mechanisms used in cryptography are based on the traditional mechanism(passwords and/or tokens) which are vulnerable due to the weak link between the person's identity and the associated cryptographic keys.

One of the obtained solutions that were founded to overcome the drawback of biometric and cryptography is to combine between them. The systems that combine between cryptography and biometric are denoted as *biometric-crypto systems* . With the help of these systems, revocability, privacy, and template diversity can be induced in biometric systems. Also, biometrics-based cryptographic keys, denoted as *crypto-bio keys*, which are strongly linked to the user identity, can be obtained [59].

There are many difficulties that faced the combination between biometric and cryptography, one of the biggest difficulties is that cryptography is precise whereas biometric data contain variability. Since , the cryptography keys are binary and need to be unique at each time, the biometric data can be considered as a random variable, it means it contains some

variations in each measurement. For that raison the biometric data cannot be used directly as cryptographic keys, leading to the need to develop specific techniques for designing the *biometric-crypto systems*.

Literally, we can consider that the field of biometric-crypto systems is relatively new (it started in late 1990's). There are several works which deal with this research field, but it lacks a uniform classification of the various techniques found in literature. The majority of researchers call this research field as *Template protection* and classify these systems as feature transformation and biometric-crypto systems [67, 68]. Unfortunately, the prevailing belief is that the aims of the biometric-crypto system are only the template, In fact,many systems classified as biometric-crypto systems were originally designed for obtaining cryptographic keys which are strongly linked to the person's identity protection.

At this context, and according to the literature review and based on their application and functionality, one can classify the biometric-crypto systems into two main categories:*(a)* protection of biometric data and *(b)* obtaining cryptographic keys with biometrics.

In the first category, the main purpose of the techniques of this category is to be deployed to protect the biometric data such as encryption, hashing, transformation, etc., whereas the second category technique deals with obtaining the cryptography key (denoted as Bio-crypto keys) from the raw biometric data. In general, there are three ways to integrate biometrics with cryptography in order to obtain the Bio-crypto keys namely i) key release, ii) key binding, and iii) key generation [69]. A schematic diagram showing this classification of biometric-crypto systems is shown in Fig.3.4.

At this end, the remaining elements of this chapter will focus on the study and the categorization of the different existing biometric-crypto systems schemes especially on the scheme that obtains the cryptographic keys using biometric (the second classes of biometric-crypto system)

Widespread use of biometric-based authentication implies the need to secure biometric template data. Literally, various template protection schemes have been introduced to prevent biometric forgery and identity thefts. Next, we will try to give an overview about the existing biometric template schemes especially those used in the field of Biometric-crypto system.

Before talking about the classification of the biometric-crypto system based template protections schemes. An ideal protection scheme should possess the following four properties [69]:

1. **Diversity:** The secure template must not allow cross-matching across databases, thereby ensuring the user's privacy.

2. **Revocability:** It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

3. **Security:** It must be impossible or computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

4. **Performance :** the recognition performance should not degrade significantly with the introduction of a template protection scheme, with respect to the performance of a non protected system.

Obtaining cryptographic keys with biometric category aims to combine biometric with cryptography in order to increase the security in a cryptographic framework. Moreover, the biometric Data is used to obtain the cryptographic key. In this case, biometric-Crypto systems are classified as : *(a)* key release, *(b)* key generation, and *(c)* key Binding depending on how the secure sketch is obtained. These classes are described in following subsections.

3.5.1 Key Release based on Biometric

The simplest way to integrate biometric systems in a cryptographic framework is to store cryptographic keys securely and release them only after successful biometric recognition. Hence, classical biometric user's authentication is included in this configuration which gives the authentication result and based on which the key (or parameters to generate the key) is released. Therefor,the characteristics of the biometric key release system design are: *i)* it requires access to biometric templates for biometric matching and *ii)* user authentication and key release are completely decoupled. A schematic diagram of this configuration is shown in Fig.3.5. It is noted that the way of storing the biometric templates in this category is the same as the way used in classical biometric system.

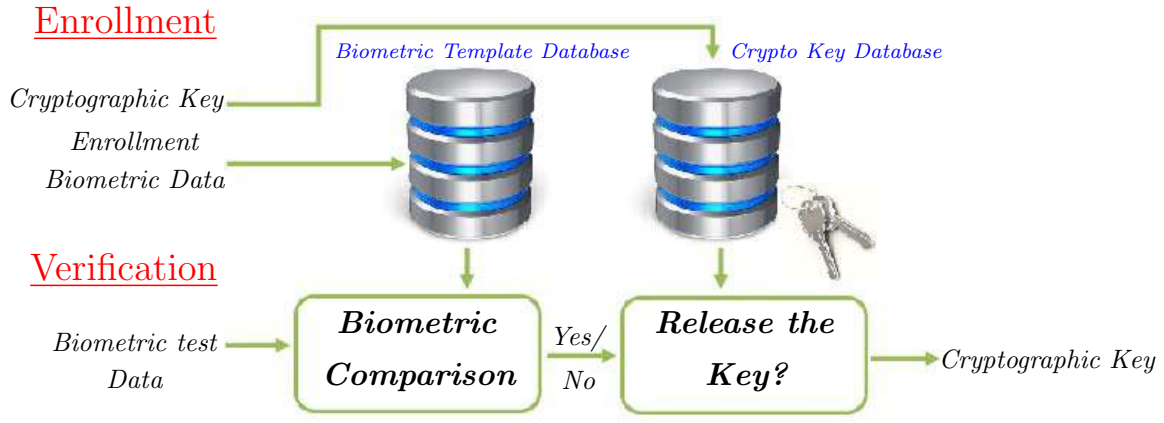


FIGURE 3.5: Key Release based on biometrics [extracted from [59]].

The advantages and the drawbacks of this configuration are as fellows: the main advantage in this configuration is its simplicity, no specific algorithm to integrate biometric and cryptography is needed. On the other hand, the biggest drawback of this configuration is the manner of storing the biometric template. The used method is the same used as the classical biometric system and thus the system inherits all the drawbacks of the biometric system such as non-revocability, non-template diversity, and no privacy protection. One can employ transformation based cancelable biometric system instead of classical biometric system to address those drawbacks in this configuration [59].

An example of an application of this configuration is the use of the Windows Biometric Framework [70] included in the Microsoft Windows starting from the version 7. The Windows biometric framework allows users to login to their windows accounts with their biometric data (currently fingerprints).

Also, another example of the key release based biometric is that the one founded in [71], where some secret parameters are released upon successful biometric verification. The released parameters are required to obtain the cryptographic keys.

3.5.2 Cryptographic Key Binding using Biometrics

According to the literature research, this type of configuration of Biometric-Crypto system is the most used approach. Also, this configuration is sometimes referred to as Biometric key regeneration [59, 68]. In the cryptographic key binding scheme, the key is the secret and the secret is hidden in a cryptographic construct with a biometric feature of the genuine user. The basic idea is that a randomly generated key is combined with the biometric data using cryptographic techniques and that key is later retrieved from the combined data at the time of verification. The stored information is known as *Helper Data*. In key binding schemes, the *Helper Data* does not reveal much information about the cryptographic key or the biometric template, i.e., it is computationally hard to decode the key or the template without any knowledge of the user's biometric data. More often than not, the helper data is an association of an error correcting code (selected using the key) and the biometric template.When a biometric query differs from the template within certain error tolerance, the associated codeword with a similar amount of error can be recovered and can be decoded to obtain the exact codeword and hence, recover the embedded key yielding to an important advantage of this configuration is that this approach is tolerant to intra-user variations in biometric data and this tolerance is determined by the error correcting capability of the associated codeword [68]. A schematic diagram of this approach is shown in Fig. 3.6.

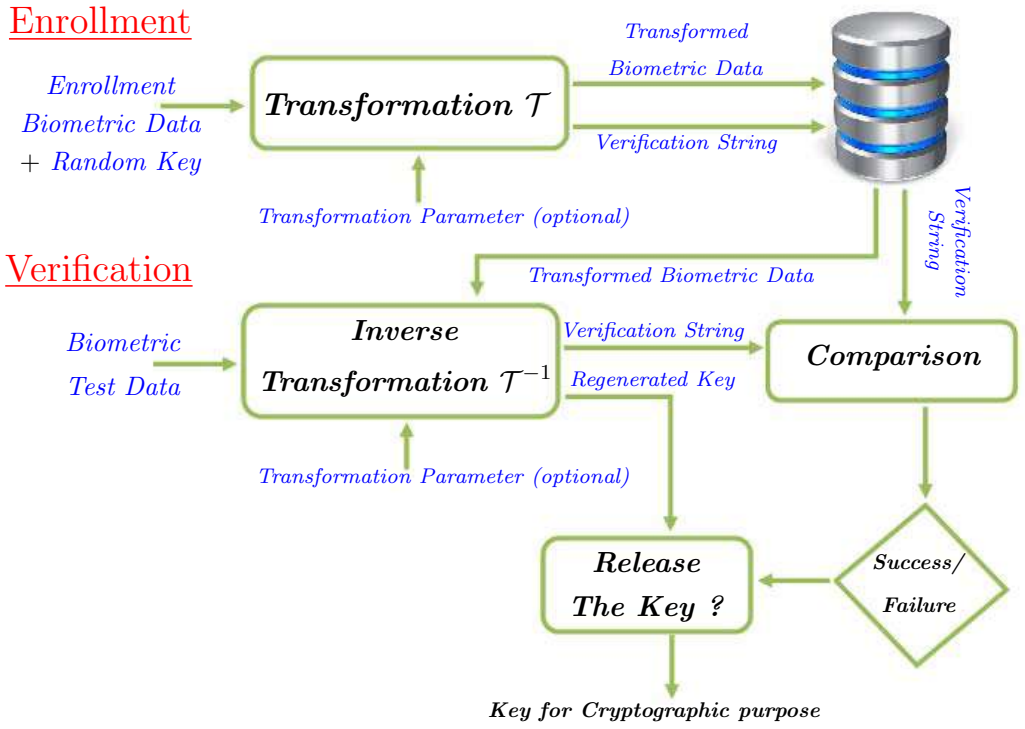


FIGURE 3.6: Cryptographic key Binding using biometrics[extracted from [59]].

Fuzzy commitment scheme [72] and the Fuzzy vault scheme [73] proposed by Juels are the well-known example of the key binding approach and they can be considered the most popular approaches for biometric template protection implementations. these two approach are the basis of our research to construct a Biometric-Crypto system and template protection schemes. What comes next is the discussion of the main theory of two schemes based key binding approach.

3.5.2.1 Fuzzy Vault schemes

The fuzzy vault scheme and the fuzzy commitment scheme are related. Both work by binding a secret key to the template that one wants to protect. The fuzzy vault framework can be considered a well known example of biometric-crypto system which is designed to secure biometric features that are represented as an unordered set [73].

To understand how the fuzzy vault schemes work, let X denotes a biometric template with r elements. The user selects a key K either randomly or by encoding a secret password. The secret key is then encoded in the form of a polynomial P of degree n and evaluates the polynomial P on all the elements in X. The points lying on P are hidden among a large number (denoted by s) of random chaff points that do not lie on P and the union of genuine and chaff point sets constitute the helper data or vault V . It is clear that in the absence of

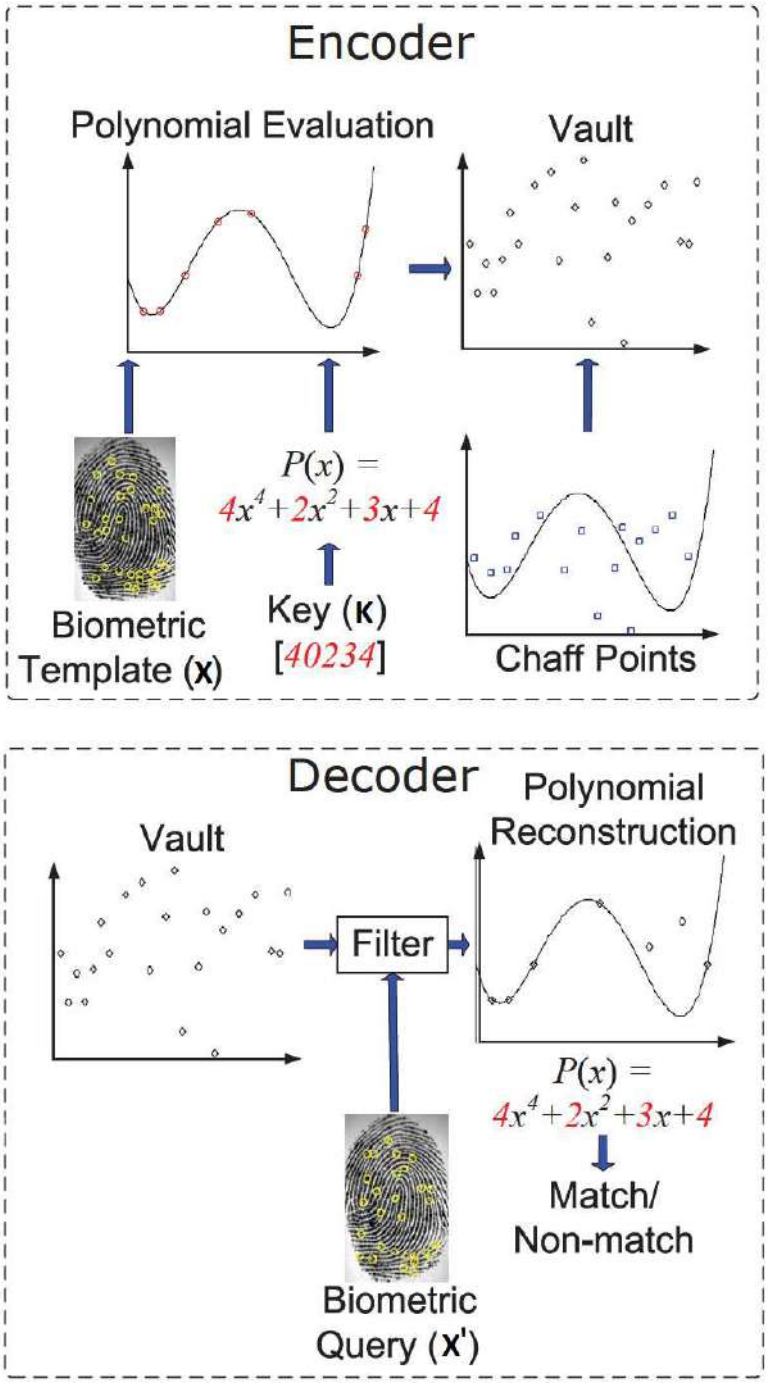


FIGURE 3.7: Typical fingerprint Fuzzy vault Encoding and Decoding.

user's biometric data, it is computationally hard to identify the genuine points in V , and hence the template is secure.

During authentication, the user provides a biometric query denoted by X'. If X' overlaps substantially with X, the user can identify many points in V that lie on the polynomial. If the number of discrepancies between X and X' is less than $(r-n)/2$, to reconstruct P, the Reed-Solomon decoding can be applied and the authentication is successful. On the other

hand, if X and X' do not have sufficient overlap, it is infeasible to reconstruct P and the authentication is unsuccessful[74].

The fingerprint minutiae biometric template protection is the popular application based fuzzy vault template protection. After this, schematic diagram (Figure 3.7) illustrating encoding and decoding of a typical fingerprint fuzzy vault.

The fuzzy vault scheme was also implemented for Face , palmprint, iris and signature modalities. it is proved that this scheme is robust against intra class variations in biometric data. However, one of the biggest limitations on this algorithm is the difficulty to generate chaff point that is indistinguishable from genuine points. Subsequently, the limitations of a fuzzy vault scheme as listed by [75]:

- Difficulty in revoking a compromised vault which is also prone to cross-matching of biometric templates across databases.
- Easy for an attacker to stage attacks after statistically analyzing points in vault.
- It is possible for an attacker to substitute his biometric features with that of the targeted biometric features thus beating vault authentication.
- The other threat is that, if the original template of the genuine user is temporarily exposed, the attacker can glean the template during this exposure.

In the next section, instead of using a polynomial representation and chaff points as in fuzzy vault scheme. It is proposed to another type of encoding like the one used in the fuzzy commitment scheme. So, in the following step, we will discuss how fuzzy commitment based key binding is working.

3.5.2.2 Fuzzy Commitment scheme

Fuzzy commitment scheme was proposed by Juels and Wattenberg in 1999 [72]. It is a key binding based biometric-crypto system that can be used to secure biometric traits represented in the form of binary vectors (e.g. iris codes). This schemes is categorized as a simple and elegant mechanism to couple the non-exactness of biometrics with well-known techniques from cryptography. The scheme makes use of error-correcting codes. It is the simplest, yet the most studied among all Biometric-crypto system schemes and is considered the most suitable for biometrics as it has a template in the form of an ordered string or binary feature vector.

The functioning of the biometric-crypto system under the fuzzy commitment schemes is described as fellow [76]:

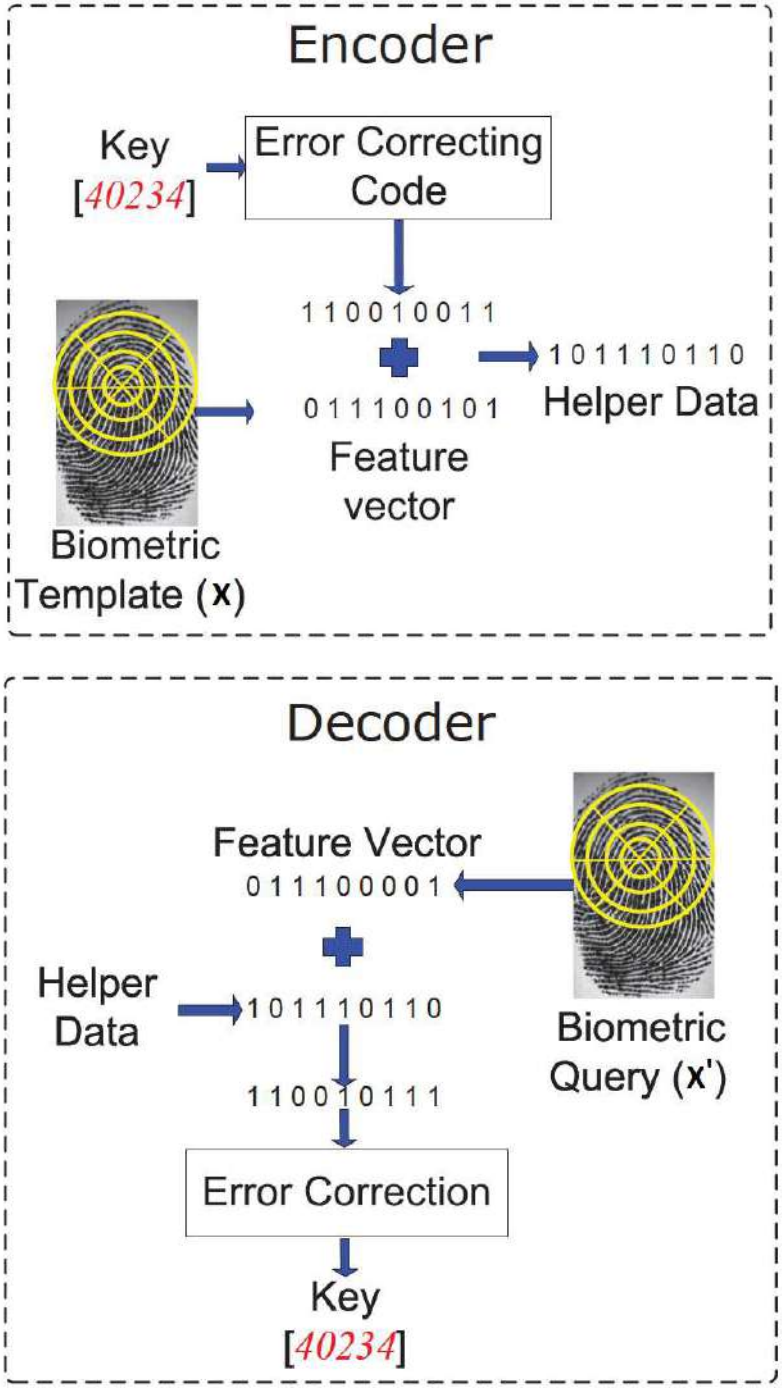


FIGURE 3.8: Typical fingerprint Fuzzy commitment Encoding and Decoding.

During the enrollment, we assume that the enrolled biometric template X is an $N - bit$ binary string. The sketch is then extracted from the template as $y_c = c \oplus X$, where the $\oplus$ indicates the XOR operator, The sketch y_c is stored in the database along with $h(K_c)$, where $h(.)$ is a cryptographic hash function.

For the authentication phase, the codeword is obtained from the query biometric X' and

the sketch y_c as follows: $c^* = y_c \oplus X' = c \oplus (X \oplus X')$. The obtained codeword c^* ,which can be considered as corrupted version of the original codeword c, can be decoded to get the key K^*. If both hashing functions $h(K^*)$ and $h(K_c)$ are the same , The authentication is successfully deemed. If the Hamming distance between X and X' is not greater than the error correcting capacity of the code, K^* would be the same as K_c and the matching will be successful.

Like the fuzzy vault schemes, the fingerprint minutiae seems to be the most appropriate application for the fuzzy commitment algorithm. Figure 3.8 shows a schematic diagram illustrating the encoding and decoding of a typical fuzzy commitment scheme.

Table 3.1 presents a direct comparison between the two schemes , the fuzzy vault and the fuzzy commitment scheme.

TABLE 3.1: Comparison of fuzzy commitment and fuzzy vault.

	Fuzzy Vault	Fuzzy Commitment
Representation	Point-set	Binary string
Main advantage	Ability to secure fingerprint minutiae	Compact size of the sketch
Main limitation	Difficult to generate chaff that are indistinguishable from genuine points	Lack of perfect codes for desired code lengths
Parameters	Polynomial degree (k), size of the template set (r), and number of chaff points (q)	Key length L, length of codeword N, and error correcting capacity of the code
Implementations	Fingerprint ([77]), face ([78]), iris ([79]), signature ([80])	Fingerprint ([81]), face ([82]), iris ([83]), signature ([84])

3.5.3 Cryptographic Key Generation from Biometrics

In the two previous subsections,a discussion about two sub classes of biometric-Crypto system (key release and key binding) was performed. It seems that those two sub classes suffer from certain drawbacks which are mentioned previously. From security point of view, a better solution than the one of the key release and key binding is to generate directly a stable cryptographic key from the biometrics. Figure 3.9 shows a schematic diagram of a generic biometrics based key generation system. In some cases, this configuration of Biometric-crypto system does not require the storage of the biometric template but only a verification string

derived from the biometric data (or from the generated key)is stored as shown in Figure 3.9, this is why that class is denoted as template-free biometrics. Similarly, at verification time, a similar verification string is derived from the query biometric and validity of the key is established by comparing the two verification strings.

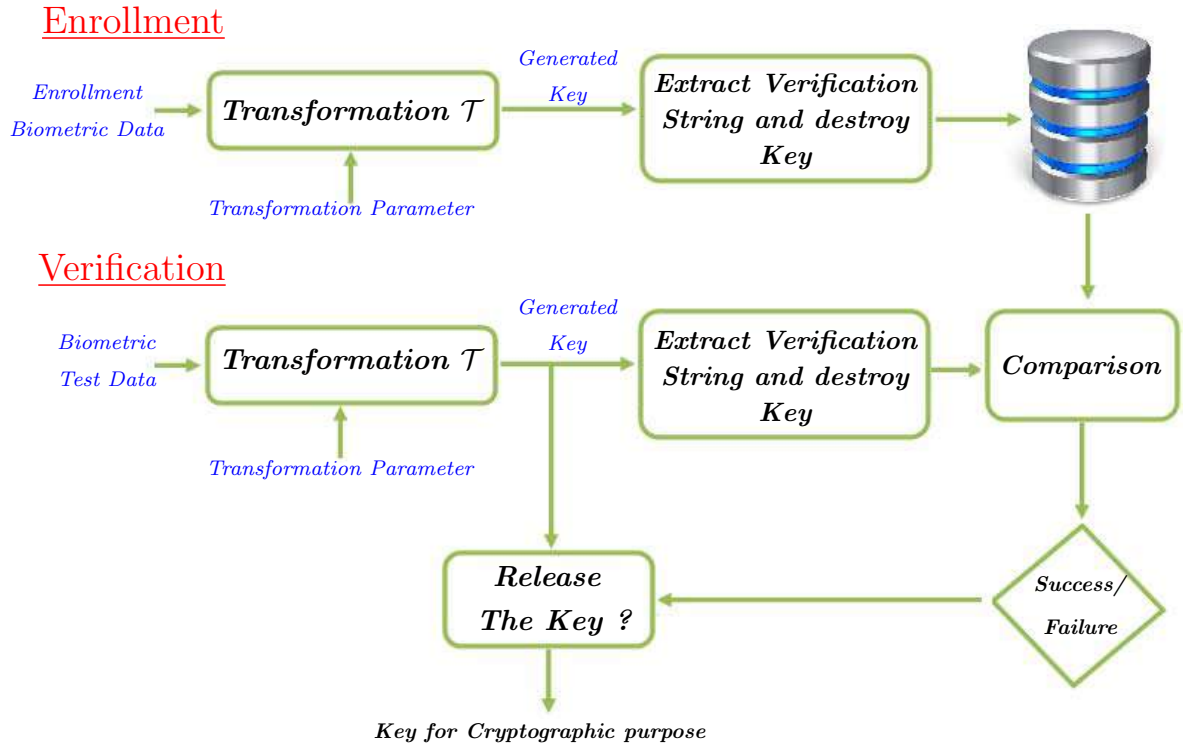


FIGURE 3.9: Cryptographic key generation from biometrics[extracted from [47]].

As an advantage of this approach, the cryptographic key is directly extracted from the biometric data which is an appealing template protection approach and can also be very useful in cryptographic applications. On the other hand, the main drawbacks of this approach are the difficult of generating the cryptographic key with high stability and entropy because of the intra-user variability.

The *secure sketch* and *fuzzy extractor* introduced by Dodis et al. [85] can be considered from the earlies work in this category. This last approach is a cryptographic primitive that generates a cryptographic key from the biometric features [68].

The cryptographic key and the biometric template are completely decoupled in the key release based biometric-crypto system. We cite in Table 3.2 extracted from [76]a direct comparison between the key binding schemes and the key generation based biometric template protection in terms of mode of operation, strengths and weaknesses :

TABLE 3.2: Comparison between key binding and key generation schemes

Approach	Mode of operation	strengths	weaknesses
Key Binding	Secures a biometric data by binding it with secret key. An update of the key requires a re-enrollment in order to generate a new helper data.	❒ A protected data cannot be retrieved without the knowledge of the secret key. ❒ Guarantees user privacy as cryptographic keys are independent of biometric data.	An attacker who knows the secret key can recover original biometric data from protected template.
Key Generation	❒ Generates a key directly from extracted biometric features. ❒ Derives a helper data from a biometric template and generates a key from the helper data and a given biometric sample. The stored helper data is used to update a key that is suspected to have been compromised.	❒ Provides security and privacy by eliminating direct storage of biometric data. ❒ Difficult for attackers to reconstruct original biometric data from key string since biometric data are not retained after enrollment.	❒ Key generation schemes which do not store helper data cannot provide revocable (updateable) keys. ❒ Helper data based key generation schemes which use helper data are vulnerable to attack via record multiplicity

3.5.4 Biometric-crypto system: discussion and chalenges

In the previous section and according to the literature review, we found that the biometric-crypto system based template protection are classified into three main categories which are: key release , key binding or sometimes refereed key locking and the last category is the key generation.We believe that as yet there is no “best” approach for template protection. The application scenario and requirements play a major role in the selection of a template protection scheme. For instance, in a biometric verification application such as a bank ATM, a simple algorithm such as salting scheme based on the user’s PIN may be sufficient to secure the biometric template if we assume that both the transformed template and the user’s PIN will not be compromised simultaneously. On the other hand, in an airport watch-list application, non-invertible transformation is a more suitable approach because it provides both template security and revocability without relying on any other input from the user. Biometric-crypto systems are more appropriate in match-on-card applications because such systems typically release a key to the associated application in order to indicate a successful match.

The other major factors that influence the choice of a template protection scheme are the selected biometric trait, its feature representation, and the extent of intra user variations. Design of a template protection scheme depends on the specific type of biometric features used.

3.5.5 Security analysis of biometric-Crypto Systems

In the last section, the Biometric-Crypto system is revealed to solve the problems related to both biometric and cryptography. So, the biometric-crypto systems are supposed to increase the security, and therefore, it is required to carry out theoretical as well as experimental security analysis of such systems. On this regard, when we talk about the security analysis of those systems, we must take into consideration that the conception of the Biometric-Crypto system mustn't decrease the biometric system based identification performance, this is on one hand. On the other hand, the constructed system must also robust on each kind of attacker based key retrieval. Hence, two security scenarios are considered: stolen biometric: when the biometric data for all the users are compromised; and stolen key: when the secret keys of all the users are compromised. As that one of our main research ,during the realization of this thesis, is the conception of the Biometric-Crypto system . An analysis of such metrics rates is required. Those metrics include FRR(GAR),FAR and EER or the ROR and RPR for the closed-set identification based applications as well as a security analysis depending on the secrecy of cryptographic keys. This will be performed by calculating a genuine key retrieval rate and the impostor based key retrieval rate.

3.6 Conclusion

In this chapter, an emerging field denoted as Biometric template protection is presented and discussed. Before starting to detail the different approaches of biometric template protection schemes, basic concepts of Cryptography were addressed. In addition, this chapter includes a counting of the various attacks that can occur and threats the performance of the biometric system. Numerous approaches and systems were proposed in the literature in order to protect the biometric template . A systems called as Biometric-Crypto system are the well known means in this field. Biometric-Crypto system combine biometrics with cryptography in order to remove the artifacts present in the two techniques.

A classification review of such Biometric-Crypto systems is presented in this chapter. The review is presented so that the systems are classified according to their purpose and their basic working methodology. Clear distinction is made between the various classes along with their representative schematic diagrams.

Chapter 4

Biometric feature selection

4.1 Introduction

As previously mentioned in Chapter 2, one can define *Biometric authentication* as the process of establishing the identity of an individual using measurements of some collection of his/her biological or behavioral characteristics. Generally, when we concept a biometric authentication system we take into consideration three important constraints which are the augmentation of the accuracy rate and the reducing of computational time and the feature vector size. An ideal biometric system is the one that can achieve all of those constraints. unfortunately, the feature vector size can be augmented in order to ameliorate the accuracy rate which leads to a system database with large memory and heavy system in calculation (heavy time processing). However, in order to concept a biometric system that takes into consideration the three mentioned constraints above,a number of questions arise during the conception. Some of them could be: which type of biometric modalities shall we use?, which features descriptors is appropriate to use in the feature extraction phase?, which type of classifiers is the better to distinguish between the biometric system users?. Also, one can request which biometric modalities images representations (gray scale images, color images, multi/hyper spectral images) is better to describe the user identity.

The key task to achieve a robust biometric based identification/verification Depends on the choice of the features extraction techniques as well as the used features to distinguish between users such as principal lines features, textural or shape features. However, this chapter introduces an overview concerning the constructed biometric identification system during the realization of this thesis. We focus our study in this chapter on the performed features tasks descriptors which resulted in proposing a new variants of the well known features descriptor Local Binary Pattern(LBP). The new features descriptor is called 3D Local Binary Pattern (3DLBP) which will be a generalized version of the original LBP and

can be applicable to the color or multi/hyper spectral images . Furthermore, a discussion concerning the used features descriptors that are used to extract the lines, texture or the shape features will be performed in this chapter.

4.2 Feature Extraction Task

The second phase of the conception of the biometric system is the features extraction stage. So, feature extraction is an essential tasks in any pattern recognition application since a more accurate classification results are directly depend on the choice of the feature extraction techniques. However, the distinctiveness and unevenness of the extracted features used to differentiate between different system user's.

4.2.1 Objective

It is known that the aim of the biometric system conception is to construct a robust system that had the ability to distinguish between user's with high degree of accuracy. The feature extraction module is the key process to achieve that. The feature extraction module processes acquired the raw data and extracts only the salient information to form a new representation of the data. Ideally, this new representation should be unique for each person. Practically, this task is not easy to achieve with exact precision [86]. This is mainly due to the choice of extracted characteristics that must be representative of the identity of the person to be recognized. This choice is important because it conditions all the methodology implemented for the recognition.Finally, assuming that these characteristics are known, it is often difficult to define a set of rules to exploit them. Many types of features can be used to represent and identify the modality image. Various techniques have already been proposed for extracting different biometric characteristics. Although these techniques have performed well, various changes happen in the present images , however, a major challenge for recognition systems need to be robust to these changes.

4.2.2 Biometric features types

Features are an inevitable part of machine learning. The more informative features we have, the greater accuracy we get. Therefore, for any classification or recognition algorithm, it is particularly essential to extract the right set of features. Feature extraction algorithms have many applications in computer vision and object detection area. The most important step in image classification is that of defining a set of meaningful features to describe the pictorial

information from the image blocks. Once these features are extracted, categorization can be executed using any classification technique.

There are mainly three kinds of features approach currently used for biometric authentication : line based approach, texture based approach and shape (or appearance) based approach.

4.2.2.1 Lines based approaches

Each biometric traits is characterized by a special set of features which can be useful in many biometric recognition system. The principal lines are one of the essential features that characterize the user's identity and can be found in many biometric traits such as palmprint, Finger knuckle print and Ear images. Principal lines are the most obvious features in the images and they are very important in detection and recognition. This has led researchers to focus their interest on the extraction of principal lines. The lines are either matched directly or represented as different types for matching.

Literally, there many approach found to extract the lines features of the raw biometric data. one can cite Gabor filter response with binarization [87] or by using filtering operations like in [88]

4.2.2.2 Texture based approach

Biometric modalities images can be regarded as a textural image information, comprising the principal lines and other features information.Biometric traits such as fingerprint, finger-knuckle prints, palmprint, ear and iris are rich in texture. This texture is unique and the feature vector extraction algorithm should correctly represent the texture pattern. Biometric recognition based on texture coding usually involves small feature size, fast matching speed and high accuracy in identification [89].

Numerous features extraction algorithm had been proposed to extract the textural pattern of the raw biometric modality. Hence,one can cite the Binarized Statical Image features (BSIF) descriptor [90]. Moreover, the 2D gabor filter response is a well known descriptor in the field of textural features extraction. Also, we can cite Local Binary Pattern (LBP), discrete cosine transform (DCT), Fast Fourier Transform and ...etc [89].

4.2.2.3 Shape based approach

Shape features based approach, or sometimes referred as appearance-based approach, is an important visual feature and can be considered one of the primitive features for image

content description. The coefficients acquired in the shape are employed as features and a distance metric and some other classifiers are implemented for matching purposes. Therefore, shape descriptors can be divided into two main categories: region-based and contour-based methods. Region-based methods use the whole area of an object for shape description, while contour-based methods use only the information present in the contour of an object. Using shape feature extraction techniques provide a powerful representation, low computational cost, ease of implementation and reliable splitting, and are extensively used in various areas such as face,palmprint and Ear recognition.

The 2D-PCA is one of the most commonly used techniques applied to extract shape feature vectors. Also, we can find the Histogram of Oriented Gradient (HOG) features [91], the Fisher Discriminant Analysis (FDA), independent component analysis (ICA) and linear discriminant analysis (LDA)[92].

4.3 Properties of Biometric Features

In the last section we had seen that the biometric features can be classified into three categories. It is clear that the choice of the appropriate features plays an important role in the biometric based recognition application. After processing the biometric sample and extracting the features, we have to store (and maintain) the newly obtained template. Choosing proper discriminating characteristic for the categorization of records in large databases can improve identification/verification tasks later on. Basically, There are 4 possibilities where to store the template: in a card, in the central database on a server, on a workstation or directly in an authentication terminal. The choice of storage method is depend on type biometric system task identification or verification or even information security application. Let us ask these questions: are there any requirements or obligations imposed by the task of the biometric system?, if we are in the phase of an information security system such as biometric-crypto system, what are the obligations that we must respect during the realization of those system. Hereafter we will discuss the obligations imposed by the biometric system and even by the information security system.

4.3.1 Biometric system obligations

We all know that the biometric system can work into two modes: identification and verification. Generally, the first two template storage approaches are the most used during the biometric system conception(i.e a card or in the central database).Probably, all the biometric system based verification applications are a card based storage applications such as the identifying card. Those applications require that the stored feature vector mustn't be with

a greater size because of the limited memory size in the card. A feature vector with smallest size leads as to a speed verification process in time processing. For that the used features as well as the feature descriptor must give a feature vector with a reduced size.On the other hand, for the identification mode, the problem of the feature vector size is not raised because all the templates are usually stored in a central database. However, the research main aim in the biometric identification problems is to increase the system accuracy even with a feature vector with greater size.

4.3.2 Information security obligations

We had seen that the information during transmission/storage must be kept in secure manner from an adversary. Biometric-crypto system are a well known means to secure the secret information by combining cryptography along as with biometric features to overcome the shortcoming comes from biometric and cryptography separately. Biometric-crypto system are mainly classified into three categories : key release, key binding and key generation. For the key release based approach, the cryptographic key must be released only for genuine user's because the drawbacks of the biometric system doesn't solved in this approach . To achieve that, a discriminative biometric features must be used with an appropriate feature descriptor that had th ability to extract those features. For the key binding based approach, the cryptographic key and the biometric template are coupled using such algorithm. Hence, the used algorithm to bind the cryptographic key into the biometric template must be able to recover both of key and template with high level of accuracy and precision. Finally, the key generation based approach extract directly the cryptographic key for the raw biometric data. However, in order to implement an algorithm based key generation approach, we must take into consideration that the extracted key must be the same for all images of the same user's and totally different from the extracted key of an impostor user's.

4.4 Person identity authentication using biometric features

How do we know if the person in front of the system is not an adversary? How do we know a person is who they say they are? As the online world evolves, the need for verifiable and trusted identities increases. While initially, a fake identity might generally be a benign occurrence on online forums, now a fake identity can result in major loss of secret information, funds or be at the core of financial crimes.

4.4.1 Objective

Building the necessary trust system requires an identity check to confirm that the person actually exists. Biometric based identity authentication becomes a powerful means of establishing and confirming the user's identity. The robustness and the precision of the biometric system are related especially to used biometric modalities as well as the used features to distinguish between persons. So, our objective is to construct a biometric-based identification system based on an appropriate discriminative feature. As the biometric features can be classified into three approaches (lines, texture, and shape based approach), we are intended to use some chosen feature descriptors in order to extract the principal lines, texture or the shape features where the aims are to achieve an identity authentication with a high level of accuracy and precision.

4.4.2 Feature Extraction Techniques

In this section, we are going to talk about the used feature vector descriptor that is used to extract an appropriate feature. the choice of those feature descriptors is depending on their performances in the biometric feature extraction task. For this reason, a Gabor filter response with a binarization thresholding is chosen to extract the principal line of the biometric while the Binarized Statical Image Feature (BSIF) is chosen to extract the textural information and the Histogram of Oriented Gradient (HOG) for extracting the shape features of the biometric images.

4.4.2.1 Line based approach: Gabor filter response overview

Gabor filter, Gabor filter bank, Gabor transform and Gabor wavelet are widely applied to image processing, computer vision and pattern recognition. Thus, For applications requiring orientation analysis, Gabor functions produce a very useful wavelet decomposition [93]. Gabor filters can be used to extract components corresponding to different scales and orientations from images. Hence, the circular Gabor filter can represented by the following general form [94]:

$$h(x,y) = \frac{1}{2\pi\sigma^2} e^{-\{(x^2+y^2)/2\sigma^2\}} e^{2\pi i\mu(x\cos\theta + y\sin\theta)} \tag{4.1}$$

Where $i = \sqrt{-1}$, μ is the frequency of the sinusoidal signal, θ controls the orientation of the function, and σ is the standard deviation of the Gaussian envelope. The Gabor filter application requires an empirical choice of filter parameters (θ, μ, σ). These empirical parameters are very difficult to determine and this is one of the drawbacks of approaches based on this filter.

❑ **Feature vector generation:** Most biometric systems do not directly compare the acquired raw data (image, sound, ... etc.). Instead, different mathematical methods are used to reduce the raw data, but with preservation of the essential information that makes it possible to characterize two images. The Gabor filter representation of an image I is the convolution of this image with the Gabor filter, defined by:

$$I_G(x,y) = h(x,y) * I(x,y) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} h(m,n)I(x-m,y-n) \tag{4.2}$$

where $*$ denotes discrete convolution. As the Gabor filter has a complex formula, it is important to use the information given by the real part and those given by the imaginary part of the Gabor coefficients [95]. At this context, the results $Re\{I_G\}$, and $Im\{I_G\}$ of a pair of a real and an imaginary filter are combined in order to produce three vectors {combined Real-Imaginary (V_{RI}), PHase response (V_{PH}) and AMplitude response (V_{AM})} as fellow :

$$V_{RI} = [\ Re\{I_G\} \quad Im\{I_G\}\ ] \tag{4.3}$$

$$V_{PH} = \arctan\left[\ \frac{Im\{I_G\}}{Re\{I_G\}}\ \right]. \tag{4.4}$$

$$V_{AM} = \sqrt{Re\{I_G\}^2 + Im\{I_G\}^2} \tag{4.5}$$

These vectors should be binarized by a proper threshold value in order to generate the different feature vectors. It is important to find the proper threshold value in order to separate the lines from input image. Thus,V_{RI} and V_{PH} are binarized by the threshold value equal to 0 and V_{AM} by the threshold equal to $mean(V_{AM})$. Finally, the feature vectors are obtained by:

$$\mathcal{F}_X(i,j) = \begin{cases} 1 & \text{if } V_X(i,j) \geq T_X \\ 0 & \text{otherwise.} \end{cases} \tag{4.6}$$

where $\left\{\ RI, \quad PH, \quad AM\ \right\}$. Figure 4.1 shows an example of feature extraction using Gabor filter response applied on EAR images.

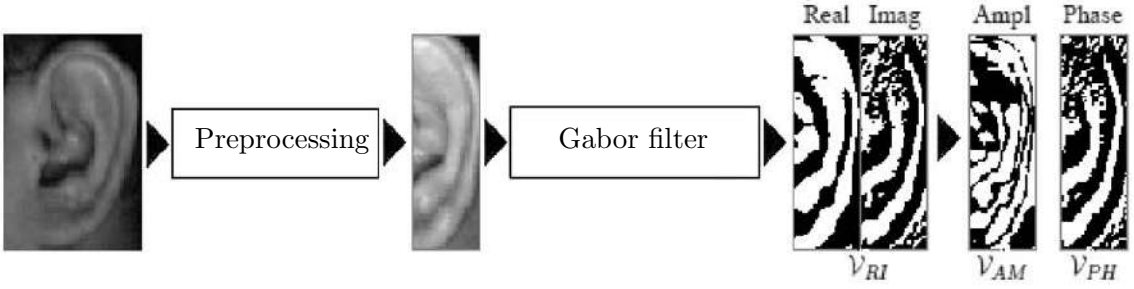


FIGURE 4.1: Block diagram of the feature extraction process based on Gabor filter responses using EAR images.

4.4.2.2 Texture based approach : Binarized Statical Image features (BSIF) overview

This method computes the binary code for each pixel by linearly projecting local image patches into a subspace, whose basis vectors are learnt from natural images via independent component analysis, and by binarizing the coordinates in this basis via thresholding. The length of the binary code string is determined by the number of basis vectors. However, the image regions can be conveniently represented by histograms of pixels' binary codes [90].

Given an image patch X of size $l \times l$ pixels and a linear filter W_i with a same size, the filter response s_i is obtained by:

$$s_i = \sum_{u,v} W_i(u,v)X(u,v) = w_i^T x \tag{4.7}$$

If we have n linear filters W_i, we may stack them into a matrix W and compute all responses at ones:

$$s = Wx \tag{4.8}$$

By giving a random sample of natural image patches, we determine the filter W_i so that the elements s_i of s are as independent as possible when considered as random variables. The binary code string b, which corresponds to image patch x, is obtained by binarizing each element s_i of s as follows :

$$b_i = \begin{cases} 1 & \text{if } s_i > 0 \\ 0 & \text{otherwise.} \end{cases} \tag{4.9}$$

where b_i is the i^{th} element of b. In this manner one may compute a *n-bit* binary code string b for each pixel and thereafter the image region can be represented by histograms of pixel's binary code.

The input image is divided into n sub-blocks where $n = 1; 2; 3; 4; ....$,then the BSIF feature extraction methods are applied to each sub-block, this method is called multi block BSIF (MB-BSIF).Moreover, based on the BSIF method, instead of using single MB-BSIF division, one can use Multi Level Binarized Statical Image features (ML-BSIF). The main idea of ML-BSIF is to extract features from different MB-BSIF divisions and then combine them. In other words, extracting features from the whole image, then dividing the image into 2×2 sub-blocks and extracting the features from each sub-block and so on until we reach the intended level. The final result of ML-BSIF is $1^2 + 2^2 + ... + n^2$ histograms. We combine these histograms to get the feature vector.

Note that the ML-BSIF will be used later in Chapter 5 combined with a *Bits-Plan* technique to generate a binary template. This template is an essential step to construct a fuzzy commitment based key binding Biometric-Crypto system.

4.4.2.3 Shape based approach: Histogram of Oriented Gradient (HOG) overview

Histogram of Oriented Gradient HOG is a dense feature extraction method for images. Dense means that it extracts features for all locations in the image (or a region of interest in the image). The (HOG) feature descriptor was firstly proposed by Dalal and Triggs [91]. The HOG descriptor has become popular for the recognition of different types of objects.

To understand how the HOG descriptor work , we give hereafter, a brief explanation on HOG features and its extractions steps:

The HOG descriptor intuitively tries to capture the shape of structures in the region by capturing information about gradients. It does so by dividing the image into small (usually 8×8 pixels) cells and blocks of 4×4 cells. Each cell has a fixed number of gradient orientation bins. Each pixel in the cell votes for a gradient orientation bin with a vote proportional to the gradient magnitude at that pixel.

To reduce aliasing, the pixels votes are bi-linearly interpolated. This interpolation happens in both the orientation as a position. This statement is important - it means that a pixel will not only vote for its orientation bin, but also for the to neighboring orientation bins (e.g. if the gradient orientation at a pixel is 45 degrees, it will vote with a weight of 0.5 for the 35 to 45 degree bin and a weight of 0.5 for the 45 to 55 degree bin). Similarly, it will vote for these two orientation bins not only in its cell, but also in the 4 neighboring cells of its cell. The weights here are decided by the distance of the pixel from the cell centers.

Histograms are also normalized based on their energy (regularized L_2 norm) across blocks. Since the blocks have a step size of 1 cell, a cell will be part of 4 blocks. This defines four differently normalized versions of the cell's histogram. These 4 histograms are concatenated to get the descriptor for the cell. Typically, the elements of histograms are also capped at some value.

4.4.3 Proposed Feature Extraction Technique

It is well known that the application of the previously discussed feature descriptor requires that the input images must be in gray scale representation. there are more than the gray scale for the image to be represented such as color or multi/hyperspectral representation (images with several bands). The application of feature descriptor such as LBP, BSIF or HOG descriptor on those representations require to be applicate in each band separately and the global feature vector is a concatenation of all vector extracted from each bands. Moreover, this scenario of feature vector generation leads as to greater feature vector in size with an augmentation in computational time.

4.4.3.1 Objective

Generally, when we concept a biometric based authentication system, we take into consideration three constraints which are the augmentation of the accuracy rate, the reducing of computational time and the feature vector size. As mentioned above, the application of the such descriptor like original LBP descriptor on color image or multi/hyper-spectral image aims to separately extract the features for each color or spectral image, which shows, as a result, the increase of the extracted features size (information concatenation) and the increase of time processing. Our objective is to handle these problems by proposing a new feature descriptor, this new descriptor is a generalized version of LBP descriptor and which extends its application to the color or Multi/Hyper-spectral image representation.

Before talking about the theory of the new feature descriptor, we must give an overview concerning the theory of the original LBP.

4.4.3.2 Original Local Binary Pattern (LBP) overview

The Local Binary Pattern (LBP) Descriptor was firstly introduced by *Ojala et al.* [96], it is especially developed for face recognition [97]. The LBP operator labels the pixels of an image by thresholding the 3×3 neighborhood of each pixel with the center value and considering the result as a binary number. Then the histogram of the labels can be used as a texture descriptor. An illustration of the basic LBP operator is shown in Figure 4.2.

The LBP concept is very simple, it proposes to assign a binary code to a pixel according to its neighborhood. This code, describing the local texture of a region, is calculated by thresholding a neighborhood with the gray level of the central pixel. In order to generate a binary pattern, all neighbors will then take a value "1" if their value is greater than or equal to the current pixel and "0" otherwise(see Figure 4.2). The pixels of this binary pattern are then converted to decimal by multiplying its values with weights and then summed up in order to generate the LBP code of the current pixel.

To calculate the LBP code in a neighborhood of P pixels, we simply count the occurrences of gray levels g_p that are greater or equal to the central value g_c

$$\mathrm{LBP}(x_c, y_c) = \sum_{p=0}^{P} U(g_i - g_c) \cdot 2^p \tag{4.10}$$

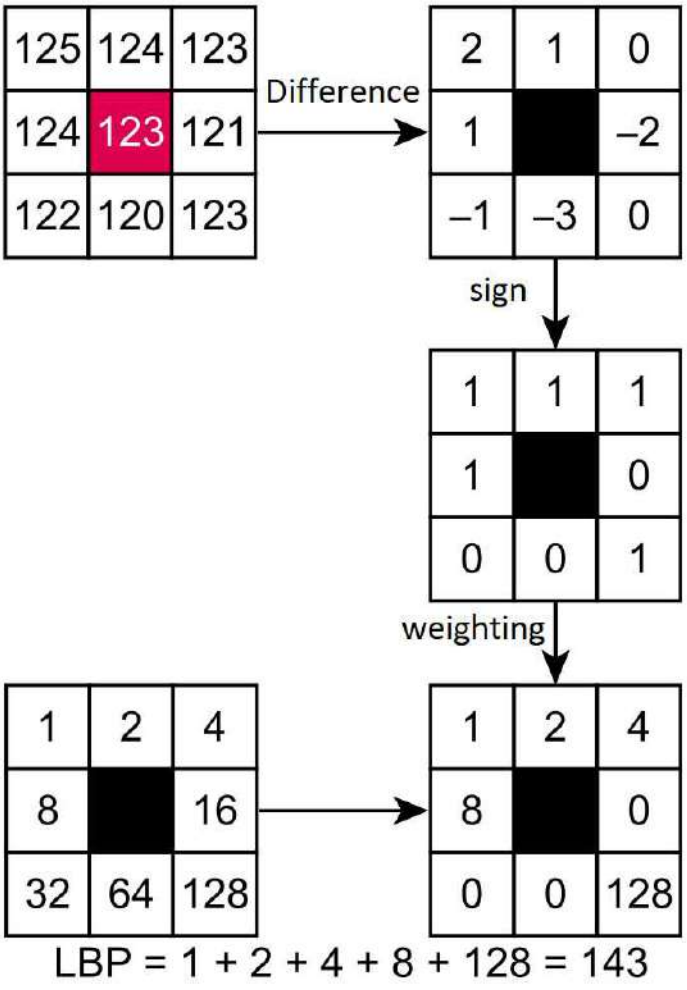


FIGURE 4.2: Basic idea of the basic LBP operator.

where x_c and y_c are the central pixel coordinates, and g_i and g_c are respectively the gray levels of the neighboring pixel and the central pixel. The function $u(x)$ is defined as follows:

$$u(x) = \begin{cases} 1, & \text{if} \quad x \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{4.11}$$

Logically, in any image classification or image recognition system, increasing the number of spectral bands in the image representation (for example three spectral bands in color images instead one spectral band in gray-scale image) involve an increase in the time processing necessary for extract their salient features as in the case of the LBP descriptor. Of course, it is very nice to find a feature extraction techniques that exploit jointly all informations in the different spectral bands with almost same time processing as for a single band.

At this context, we are motivated to propose a technique that exploits all the texture information from a color or Multi/Hyperspectral images. One of the main challenges from the

use of color or multi/hyperspectral images is to find or to develop an appropriate descriptor that exploits all the information extracted from all image spectral bands in a way that we obtain a feature vector with reduced size and can be classified in a possible shortest time with highest accuracy. So, as it is mentioned above, the major inconveniences of the applications of LBP descriptor and its variants on color image are the increase of the extracted features size as well as the times processing. In order to overcomes these limitations, we propose a new LBP descriptor that uses 3D representation of the information contained in the image. The proposed descriptor is called 3D Local Binary Pattern (3DLBP).

In order to prove the efficiency of the proposed feature descriptor, we give, hereafter, a literature review on the application of the original LBP on the color or Multi/Hyperspectral images. Note that, although the number of the papers, which discuss LBP descriptor, in literature is very high, very few papers use LBP descriptor especially for color images. In the recent years, various methods based on LBP features have been proposed for color images representation. In all these methods, the overall feature vector is constructed by concatenating the LBP feature vectors extracted from each color/multispectral band or by combining the LBP by an other approach [98].

A simple feature descriptor based on LBP technique for object and scene image classification is proposed by *banerji et al.* in [99]. In their method, the LBP descriptor is applied to each color band of the color image in order to generate three new representations.

In addition, to make the LBP feature useful on color image, another solution was proposed jointly by [100, 101]. In their proposition, an additional feature (discriminate color information), namely Color Histogram Feature (CHF), is added to strengthen the features of discrimination. It is also noted that the LBP is applied on color image bands separately.

Moreover, another method for LBP based color image, called multichannel decoded local binary pattern, is proposed by [102]. Thus, in this method, color image is described with a multichannel decoded LBPs where an adder and decoder-based two schemes for the combination of the LBPs from more than one band is proposed.

In the fellowing section, we will discuss the theoretical and mathematical aspects of our new proposed 3DLBP.

4.4.3.3 3D Local Binary Pattern (3DLBP)

Our 3DLBP descriptor extract texture patterns for a color or multi/hyperspectral images similar to the way that LBP operator extract texture for grayscale images. Thus, our proposed method extract directly the feature vector from the entire image (using all spectral bands) instead one band at each time (separately). This methodology allows to reduce the

feature vector size and to decrease the time processing. One of the main interests of the proposed method is that the application is not limited only to the color image (image only with visible bands RGB). So, its application can be also extended to the multi/hyperspectral images, which give different information from a variety of spectral bands and can improve the performance of the system because each spectral band highlights specific features of the image.

The LBP descriptor consists of transforming a neighborhood of 3x3 pixels to a binary string using the intensity of the pixel in consideration as a threshold. Such a bit string is converted to decimal value. Finally, a histogram is generated taking into account all occurrences of the obtained decimal values [103]. Our proposal is to generalize LBP for applying it on a multi-band image. The idea is to consider all pixel intensities through the bands as a vector, instead of considering them individually. This is the same for the neighborhood that becomes a vicinity matrix that has dimension of 3 by the number of bands. The following mathematical description of 3DLBP, will detail more our idea.

Let us consider $T = t(g_c^i, g_0^i, g_1^i, \cdots, g_P^i)$, the local neighborhood of an image, as the joint distribution of the pixel levels of images, where g_c^i corresponds to the center pixel of the band i and g_p^i $(p = 0, \cdots, P)$ correspond to $(P + 1)$ neighboring pixels. The 3DLBP descriptor that characterizes the 3D image texture around a given pixel position (x_c, y_c) is defined as:

$$\text{3DLBP}(x_c, y_c) = \sum_{p=0}^{P} S(d) \cdot 2^p \tag{4.12}$$

where $s(d) = 1$ if $d \geq 0$, otherwise $s(d) = 0$, $P + 1$ is the total number of pixels in the local neighborhood and

$$d = dist(V_p, V_c) = \sum_{p=0}^{P} \sum_{i=0}^{N} (g_p^i - g_c^i) \tag{4.13}$$

where $V_p = [g_p^0, g_p^1, \cdots, g_p^N]$, $V_c = [g_c^0, g_c^1, \cdots, g_c^N]$ and N denote the number of the image bands. The 3DLBP descriptor is a histogram $h(j)$ calculated as follow:

$$h(j) = \sum_{x,y} \psi(\text{3DLBP}(x_c, y_c) = j) \tag{4.14}$$

where $j \in [0, 2^{P+1} - 1]$ and

$$\psi(\tau) = \begin{cases} 1, & \text{when } \tau \text{ is true} \\ 0, & \text{otherwise} \end{cases} \tag{4.15}$$

We note that in 3DLBP, the bands number is variable. So, if we have only one band, 3DLBP becomes LBP.

4.5 Conclusion

The evaluation and selection of useful biometric features can improve the accuracy and reduce the complexity of classifier. We had seen that the biometric features are mainly classified into three categories: lines , texture and shape features. Therefore , in the feature extraction stage, an appropriate feature descriptor is used to extract the appropriate features. For that , and according to its powerful discriminability between persons, this chapter include a discussion of some features descriptors performance, one descriptor of each feature categories. Those descriptors are Gabor filter response for extracting the line features, BSIF descriptor for extracting the textural information and finally, the HOG descriptor to extract the shape features. According to limitation of the LBP descriptor, this chapter also include a discussion of our proposal 3D Local Binary pattern (3DLBP) descriptor for extracting the textural information of color or Multi/Hyperspectral images.

In the next chapter (Chapter 5) the proposed biometric system performance evaluation will be performed using the proposed descriptors as features descriptor with an appropriate classifier.

Chapter 5

Experimental Results and Discussion

5.1 Introduction

A WIDE variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Exploiting biometrics in recognition can be considered a powerful solution to achieve those requirements.Hence, the robustness of the biometric identification is depend on used features descriptors.

In this chapter, the obtained experimental results are divided into two parts: the first part is devoted with the performance and the evaluation of the proposed biometric identification system using the features descriptors that mentioned in the previous chapter and take the PLM , FKP and EAR as an input traits. The remaining of this part is as fellow: next section, a new schemes of Gabor filter response based identification system using EAR images is evaluated. Then, a FKP based identification system is discussed using HOG descriptor and SVM classifier, where the aim of this experiments is to perform a comparative experiments between two fusion levels (Features and score level). After that, a PLM based identification system using the ML-BSIF descriptor is evaluated and discussed. Finally, the last section include our main contribution which is the application of our new feature descriptor 3DLBP on the color or MSP/HSP palmprint images. a series of experiments are carried out to show the efficiency of the proposed descriptors. The second part of experiments will focus on the construction of a key binding based Biometric-Crypto system using a fuzzy commitment schemes and binary feature vector that combine both the BSIF features and the $bit - plane$

decomposition. This part includes a description of the *E-voting* system based biometric-crypto system application and the security analysis of the proposed approach.

before starting to discuss the performance of the proposed biometric identification system, we give in the next section , a description of the used biometric modalities with its choice justification.

5.2 The biometrics modalities used

A biometric modality is nothing but a category of a biometric system depending upon the type of human trait it takes as input. The biometric is largely statistical. The more the data available from sample, the more the system is likely to be unique and reliable. The first question revealed during the conception of the biometric system is which biometric modality shall we used ?.Generally, the application type of biometric system which decides the kind of biometric modalities we shall use and that satisfies the properties is described in subsection 2.4.

Starting from Table 2.2 and based on the availability of a biometric data database and according to the literature research. One can see that the hand related modalities (such as PLM or FKP) and Ear show an interested and high level results in term of Universality, Uniqueness, Permanence, Collectability, Acceptability and Performance (achieve at least 4 stars).Also, it is preferred to choose a biometric modality from different part of the human body for biometric system construction . As an example, when we choose the hand related to biometric modalities such as fingerprint, PLM and FKP. Thus, in case the person lose its hand automatically he will lose the related modalities. So, in the phase of biometric system conception we choose three biometric modalities as an input of the system which are Ear, Palmprint (PLM) and Finger Knuckle Print (FKP) where the purpose is to use it for the evaluation of the proposed biometric identification system. It is noted that the biometric system don't exploit all the image of biometric raw data but only a Region Of Interest (ROI) extracted from the raw data by the means of preprocessing stage is used.

Henceforth we will cite the advantages of the above three mentioned modalities to justify the use of them in the conception of the proposed identification system.

❒ **Ear:** Recently, Ear has attracted an increasing amount of attention. Like any other biometric identifiers, ears are believed to have the desirable properties of universality, uniqueness, permanence and collectability for personal recognition [104]. In addition, there are several motivations for ear biometric [105]. Firstly, the ear data can be captured using conventional cameras. Secondly, the data collection is non-intrusive (i.e., requires no cooperation from the user). Thirdly, ear based access systems are very suitable for several usages. Finally,

ear features are more stable over time and are not susceptible to major changes (see Figure 5.1).

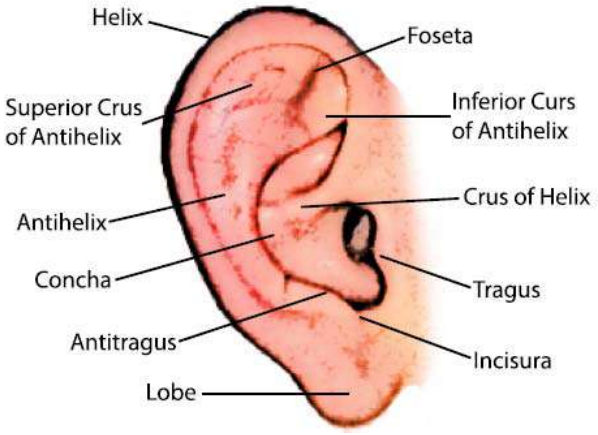


FIGURE 5.1: Ear structure.

❒ **Palmprint (PLM):** The palms of the human hands contain a wide variety of features (e.g., shape, principle lines, wrinkles, ridges, minutiae points, singular points, and texture pattern) that can be used by biometric systems. These features of the human hand are relatively stable and the hand image from which they are extracted can be acquired relatively easily [106]. Therefore, in the past few years, palmprint had attracted so much attention. Moreover, it can easily be combined with other hand biometric modalities to form an acceptable and highly accurate and reliable biometric based personal identification system [107]. Another advantage of the PLM modality is the availability of different database with different representations such as gray level(GL) images, Multi spectral (MSP) or Hyper spectral (HSP) images and three-dimensional (3D) representations as shown in Figure 5.2 .

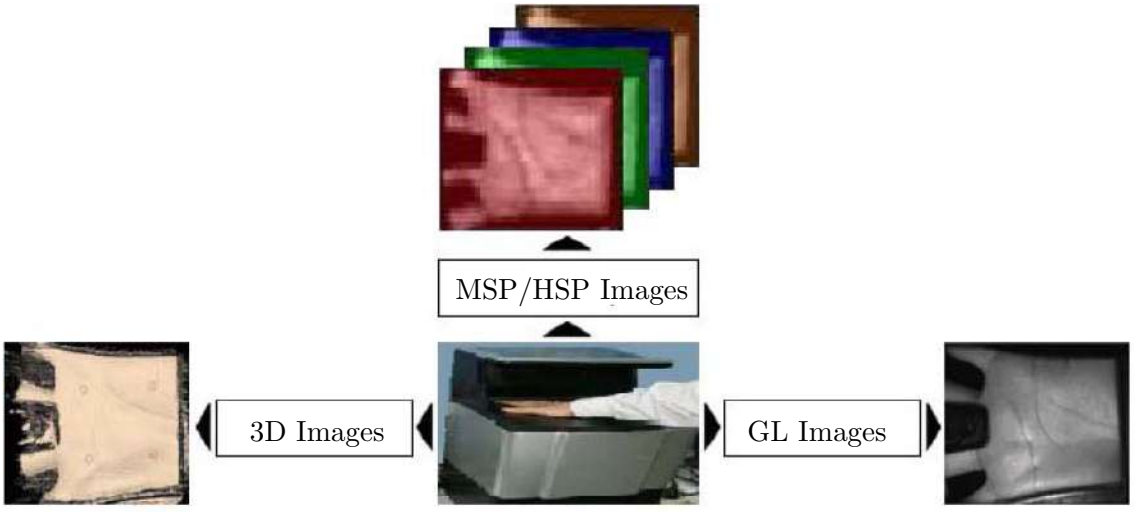


FIGURE 5.2: Representations used for the palmprint.

❒ **Finger Knuckle Print (FKP):** Finger-Knuckle-Print (FKP) is a new hand technology which has attracted an increasing amount of attention [108]. A FKP has several advantages compared to other available features: low-resolution images and low cost capture devices can be used, it is very difficult to fake a FKP modality, and the features like principal lines of the FKP images are stable, etc. It is for these reasons that FKP identification has recently attracted the attention of researchers. As another advantage of FKP biometric, the human hand contains several fingers, this is why an ideal FKP identification system can be based on the fusion of these fingers in order to improve the identification accuracy [109].

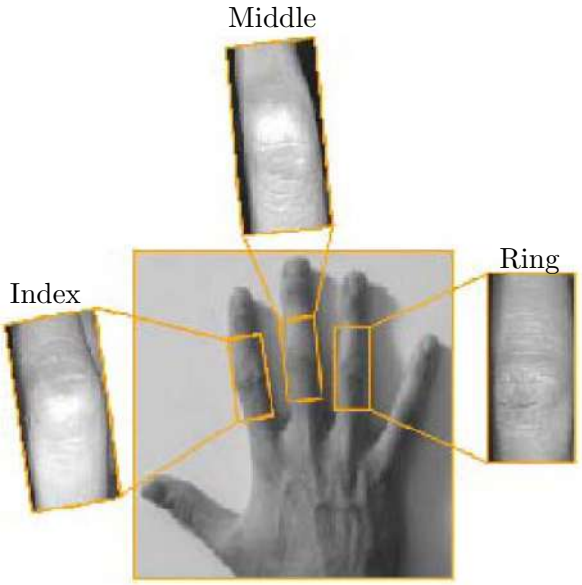


FIGURE 5.3: Finger Knuckle Prints (FKP): Index, Middle and Ring fingers.

5.3 Database Description

In order to validate the proposed schemes, it is necessary to deploy a biometric modalities databases which can be an appropriate tools to evaluate the performance of biometric system before implemented it in real life applications. Hence, a number of database are available to be used for research purpose and experimental test results evaluation. Since we are interested on the use of the PLM, FKP and EAR modalities as an input of the biometric system. The used databases are the PolyU MSP palmprint database , the PolyU FKP database and the IIT delhi EAR database . Those database are described as Fellow:

For the MSP palmprint database, it contains images captured with visible and infrared light. Four palmprints for each person, including R, G, B and NIR band, are collected. 6000 MSP images were collected from 500 persons. These images were collected in two separate sessions. In each session, the person provide 6 images for each palm, so there are 12 images for each person. Therefore, 48 spectrum images of all illumination from 2 palms were collected from

each person. The average time interval between the first and the second sessions was about 9 days.

The Finger- Knuckle-Print database from the Hong Kong Polytechnic University (PolyU) database has 7920 images obtained from 165 persons. This database including 125 males and 40 females. Among them, 143 subjects are $20 \sim 30$ years old and the others are $30 \sim 50$ years old. These images are collected in two separate sessions. In each session, the subject was asked to provide 6 images for each of Left Index Fingers (LIF), Left Middle Fingers (LMF), Right Index Fingers (RIF) and Right Middle Fingers (RMF). Therefore, 48 images from four fingers were collected from each subject.

The IIT Delhi EAR database is a database collected from the students and staff at IIT Delhi, India. All the images are acquired from a distance (touchless) using simple imaging setup and the imaging is performed in the indoor environment. The currently available database is acquired from the 221 different subjects and each subject has at least three ear images. All the subjects in the database are in the age group $14 \sim 58$ years. The resolution of these images is 272 pixels and all these images are available in *jpeg* format.

Part I

Biometric Identification System Test Results

5.4 Introduction

As it is known, a biometric based identification system is generally comport a four main stages including preprocessing, feature extraction, matching and decision stage. In this part of experiment we will focus on the impact of using the proposed feature descriptors (Gabor filter response, BSIF and HOG) as means of extracting the features form the proposed biometric modalities (PLM, FKP and EAR). However, four proposed biometric based identification system will be presented and discussed.

In the first system, we propose the use of EAR modality as an input of the system, for extracting the EAR principal lines, a 2D Gabor filter with thresholding binarization is used. For the matching task, the hamming distance is deployed to compare between two binary vector.

The second proposed system is devoted for extracting the shape feature of the FKP modality using the HOG descriptor as feature extraction technique. The support vector machine is used to perform the classification task.

The third system deals withe the use of BSIF descriptor for extracting the textural information the palmprint modalities where the euclidean distance is deployed between palmprint feature vector.

Finally, in order to decrease the feature vector size and reduce the system time processing. we propose a new feature descriptor called 3DLBP to extract the textural information of the image in variety representations(gray scale, color, MSP or even in HSP representations). a 3DLBP based identification system is evaluated and discussed in order to prove the efficiency of the proposed method.

5.5 General system description

Fig. 5.4 shows a block diagram of one of the proposed personal authentication system based on PLM modality. In the first phase, the Region Of Interest (ROI) for each used modalities is located and extracted. In the second phase, the used biometric modalities features are extracted using an appropriate descriptor. For that, the EAR principal lines are extracted using 2D Gabor filter response(real, imaginary, module and phase parts), the FKP shape are extracted based on the HOG descriptor. The palmprint textural information are released using the BSIF features. Finally, matching of the test image to the templates stored in the database using an appropriate classifiers. For that the Euclidean distance, Hamming distance, Chi-square distance and the SVM classifier are used . Based on this matching score, a decision is taken about whether to accept or reject a user is made.

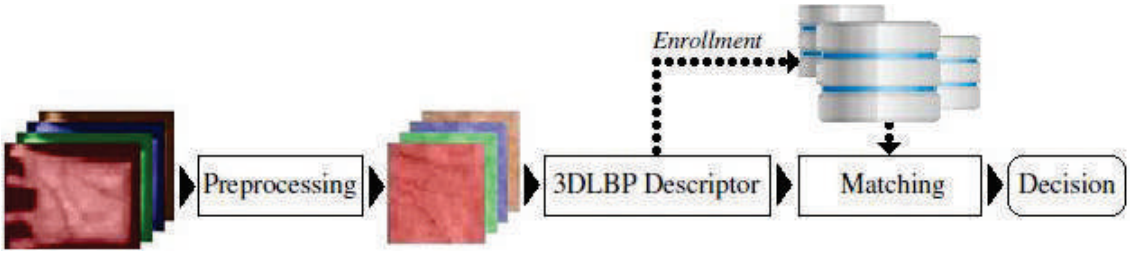


FIGURE 5.4: Block diagram of the person identification system using palmprint images based on 3DLBP descriptor.

5.6 System performance evaluation

In this part we will present and discuss the obtained experimental results,. As it mentioned previously, three different biometric database are used to evaluate the performance of the proposed systems.

Firstly, the IIT delhi EAR database [110], we setup the database with size of 221 persons, each person had at least three images. One image is randomly selected from the available images of each person was used in the enrollment stage in order to create the system database; the remaining images were used for testing. Hence, a 442 genuine comparisons and 48620 impostor comparisons are generated.

Secondly, for experiments based PolyU FKP database [111], three images of each finger were randomly selected for enrollment and the other (nine) were taken as the test set from a database containing 165 person. Thus, there are totally 1485 genuine comparisons and 121770 impostor comparisons are generated.

Finally, we have also used the MSP palmprint database [112] of 300 users captured in four spectral bands (PolyU MSP). For the enrollment phase, three images of each palm were randomly selected. Nine other images of each palm were selected for the test phase of the system. Therefore, we have 2700 comparisons, for applicant identification, and 403650 comparisons, for impostor applicant, to perform.

Now we are moving to present the obtained experimental results of the prosing biometric based identification system

5.6.1 Ear Identification System Using Gabor Filter Responses

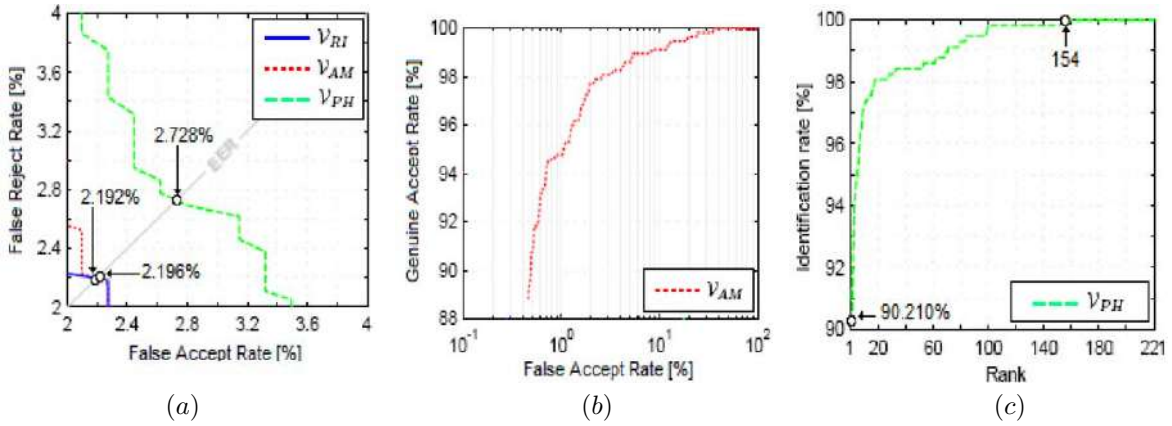
In this section, we propose an efficient online personal identification system based on ear images. In this purpose, the identification algorithm aims to extract, for each ear, a specific set of features. Based on Gabor filter response, three ear features have been used in order

TABLE 5.1: Ear based unimodal open set identification system performance.

DB	V_{RI}		V_{RE}		V_{AM}	
	T_0	EER	T_0	EER	T_0	EER
221 users	0.2352	2.728	0.2617	2.196	0.2624	2.192

TABLE 5.2: Ear based unimodal closed set identification system performance.

DB	V_{RI}		V_{RE}		V_{AM}	
	ROR	RPR	ROR	RPR	ROR	RPR
221 users	87.762	191	90.210	154	88.462	133



(a) (b) (c)

FIGURE 5.5: Results of Ear based unimodal open/closed set identification system. (*a*) The ROC curves with respect to the different feature vectors (*b*) The ROC curve in the case of V_{AM} based open set identification system and (*c*) the CMC curve in the case of V_{AM} based closed set identification system.

to extract different and complementary information: phase V_{PH}, module V_{AM} and a combination of the real and imaginary parts V_{RI}. Using these features, several combinations are tested in the fusion phase in order to achieve an optimal multi-representation system which leads to a better identification accuracy. Since, the feature vector is a binary vector, the hamming distance is used to perform the matching task.

❶ **Unimodal systems test results:** At the first stage, we conducted several experiments to select the best feature vector of the three proposed vectors used (V_{PH}, V_{AM} and V_{RI}). This is carried out by comparing all these vectors and finding the vector that gives the best identification rate (choose the feature vectors such that the Genuine Acceptance Rate (GAR) is maximized). Thus, in the case of open set identification, the Receiver Operating Characteristic (ROC) curves for the three feature vectors are shown in Fig 5.5.(*a*). The experimental results indicate that the V_{AM} perform better than the V_{PH} and V_{RI} vectors in terms of Equal Error Rate (EER). Therefore, the system can achieve a higher accuracy at the VAM vector compared with the other vectors with an EER equal to 2.192% at the threshold To = 0.2624. The ROC curve, which plot the GAR against False Accept Rate (FAR), for the best case (V_{AM} vector) is shown in Fig.5.5.(*b*). Finally, the performance of the open set identification system under all vectors is shown in Table 5.1.

TABLE 5.3: Ear based multimodal open set identification system performance

Combinations	SUM		WHT		MAX		MIN		MUL	
	T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER
$V_{RI} - V_{PH}$	0.2542	2.098	0.2575	2.098	0.2820	2.098	0.2198	2.448	0.0650	2.098
$V_{RI} - V_{AM}$	0.2763	2.083	0.2697	1.193	0.3110	2.331	0.2120	2.098	0.0786	2.098
$V_{AM} - V_{PH}$	0.2732	1.985	0.2854	2.128	0.3256	2.149	0.1852	2.061	0.0322	2.310
$V_{RI} - V_{PH} - V_{AM}$	0.2900	1.981	0.2952	2.028	0.3364	2.249	0.1858	1.761	0.0209	1.759

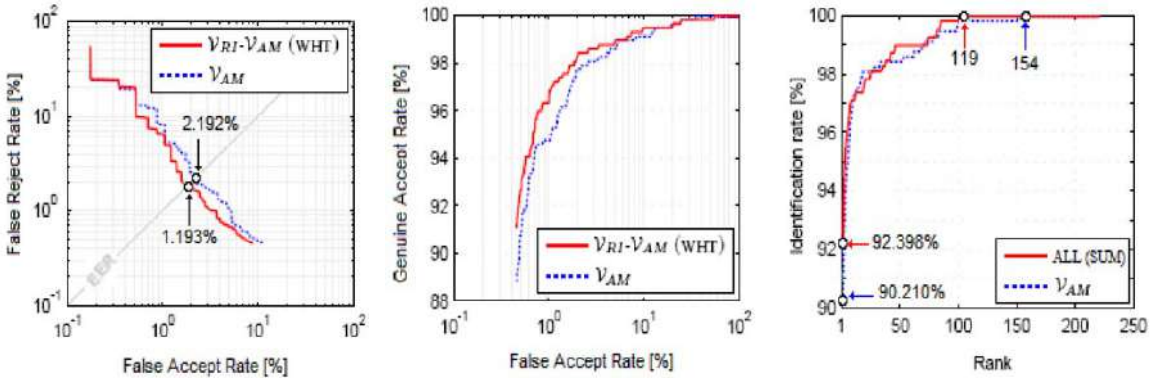
In the case of a *closed set* identification, a series of experiments were carried out to select the best feature vector, this has been done by comparing all feature vectors and finding the vector that gives the best identification rate. Table 5.2 present the experiments results obtained for all vectors. From Table 5.2, the best results of Rank-One Recognition (ROR) produce 90.210% with lowest Rank of Perfect Recognition (RPR) of 154 in the case of V_{PH} vector. The results expressed as a Cumulative Match Curves (CMC) obtained by the proposed scheme, in the case of V_{PH} vector, is plotted in Fig. 5.5.(*c*).

❷ **Multimodal systems test results:** The goal of the fusion process is to improve the unimodal system performance by fusing the information from different feature vectors. The system is then considered as a multimodal system where their inputs are different feature extraction methods (different vectors) for each ear image. Therefore, several multimodal systems are tested in order to choose the best one. In this part of experiment, the fusion is performed at the matching score level were several fusion rules are tested.

In the case of *open set* identification case, the individual scores using the three vectors are combined to generate a single scalar score, which is then used to make the final decision. Table 5.3 provides the performance of the identification system for several combination and fusion rules. From this Table, it is clear that the proposed *open-set* identification system achieves a best performance when using the fusion of $V_{AM} - V_{RI}$ and WHT fusion rule (EER = 1.193% and $T_0 = 0.2697$). Compared with the previous results (V_{AM} based unimodal system), the proposed multimodal identification has achieved better results expressed in terms of the EER ($\simeq$ 54.500% improvement). Fig.5.6.(*a*) shows the comparison test. Finally, graphs showing the ROC curve, plot GAR against FAR, for the open set identification using unimodal and multimodal systems, were generated, see Fig.5.6.(*b*).

We also investigated the closed set identification system performance, thus, a series of experiments were carried out using the ear database to select the best fusion rule that maximizes the ROR rate. Thus, to determine the best fusion rule, Table 5.4 can be established. We can observe that the SUM rule based fusion and the fusion of all feature vectors has the best performance. Thus, the best result of ROR is given as 92.398% with lowest RPR of 119. From this result, the performance of the closed set identification system is significantly improved by using the fusion. Finally, the comparison of the unimodal and multimodal closed set identification system is plotted in Fig.5.6.(*c*).

It is noted that there are other works have been performed in the same field of Ear identification system such as [113].



(a) (b) (c)

FIGURE 5.6: Results of Ear based multimodal open/closed set identification system. (*a*) The ROC curves, FRR against FAR, with respect to the unimodal and multimodal systems, (*b*) The ROC curves, GAR against FAR, with respect to the best case and (*c*) The CMC curves with respect to the unimodal and multimodal system.

TABLE 5.4: Ear based multimodal closed set identification system performance

Combinations	SUM		WHT		MAX		MIN		MUL	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
$V_{RI} - V_{PH}$	91.674	128	91.855	122	91.674	149	90.317	137	90.317	125
$V_{RI} - V_{AM}$	91.493	156	91.493	147	91.312	123	88.869	134	88.869	131
$V_{AM} - V_{PH}$	92.217	102	92.217	102	91.674	116	89.864	102	89.864	102
$V_{RI} - V_{PH} - V_{AM}$	92.398	119	92.036	114	91.674	110	88.597	118	88.597	153

5.6.2 FKP based identification system using HOG features

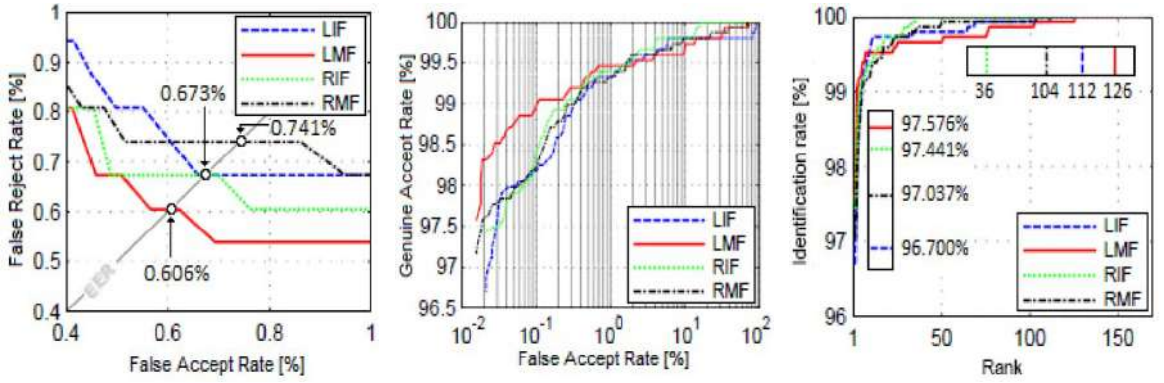
The present experiments section attempts to design an effectively biometric system by using Finger-Knuckle-Print (FKP) traits. In this part of experiments, the feature vector of each segmented FKP is extracted using Histogram of Oriented Gradients (HOG). In addition, a multi-class Support Vector Machine (SVM) based learning algorithm is used to train the system using the extracted features vectors. In addition, for the multimodal biometric identification system, two schemes are used, the first one is based on the fusion at feature level where two or more feature vectors (extracted from two or more fingers) are fused. The second is based on the matching score level where the normalized scores of two or more classifiers (each classifier is based on one finger) are fused.

The identification tests results are divided into two parts. Firstly, we present the performance of the unimodal systems using our proposed method to choose the system (finger) yield the best performance. Also, the tests results in the second part (performance of the multimodal identification systems) was divided into two sub-parts, the first sub-part focalized on the fusion of one or more fingers at feature level whereas the second sub-part discusses the fusion at matching score level.

❶ **Unimodal systems performances:** As mentioned above, the objective of the first part was to evaluate the system performance when we use information from each modality (each finger). For this, the performance of the identification system under the four fingers LIF, LMF, RIF, and RMF is evaluated. Thus, in order to see the performance of the *open-set* identification systems, we usually illustrate, in Table 5.5, the results for all fingers. From this table, it is clear that the LMF finger offers

TABLE 5.5: FKP based unimodal identification test results

MODALITIES	OPEN-SET IDENTIFICATION		CLOSED-SET IDENTIFICATION	
	T_0	EER	ROR	RPR
LIF	0.8903	0.673	96.700	112
LMF	0.8888	0.606	97.576	126
RIF	0.8774	0.673	97.441	36
RMF	0.8811	0.741	97.037	104



(a) (b) (c)

FIGURE 5.7: FKP based unimodal *open/closed-set* identification test results under different fingers. (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*)The CMC curves.

better results in terms of the Equal Error Rate (EER). In this case, the identification system can achieve an EER of 0.606% at a threshold $T_0 = 0.8888$. Also, this table demonstrates the effectiveness of all fingers, the error is in $[0.60 \cdot \cdot 0.75]$. This is justified by the efficiency of the proposed method. We can observe also that the LIF and RIF modalities give some error, they provide 0.673% at a threshold $T_0 = 0.8903$ and $T_0 = 0.8774$ for, respectively, LIF and RIF modalities. Finally, in the case of using RMF modality, EER was 0.741% with $T_0 = 0.8811$. In Fig. 5.7.*(a)*, where the Receiver Operating Characteristic (ROC) curves, we compare the performance of the different unimodal *open-set* identification systems. From this figure, it is clear that the RIF modality is more efficient than the LIF modality when FAR become $\ll$ or $\gg$ at the EER point (in EER point the performance of the RIF and LIF are equal). Also the performance of the RMF modalit becomes very efficient when the FAR $\rightsquigarrow$ 0.000% (in general when $T_0 < 0.8888$). Furthermore, we can observe the performance of the LMF modality at all decision thresholds, T_0, (FAR $\rightsquigarrow$ 0.000% or FRR $\rightsquigarrow$ 0.000%). Finally, the ROC curves (Genuine Acceptance Rate (GAR) against FAR), in Fig. 5.7.*(b)*, provide a more detailed point of view of the performance of proposed unimodal *open-set* identification systems.

Also, at the *closed-set* identification systems tests, we conducted several experiments to determine the best finger modality. This is carried out by comparing the performances of the different unimodal systems varying the fingers modalities. Thus, the results for all fingers are presented in Table 5.5. After analyzing this table we were able to conclude that all the fingers present similar results. However, the Rank-One Recognition (ROR) is between 96.700% and 97.600%. So, the system can achieve higher accuracy at the LMF modality compared with the other fingers modality, it produces a ROR equal to 97.576% with a Rank of Perfect Recognition (RPR) of 126 . Also, the RIF followed by RMF and LIF

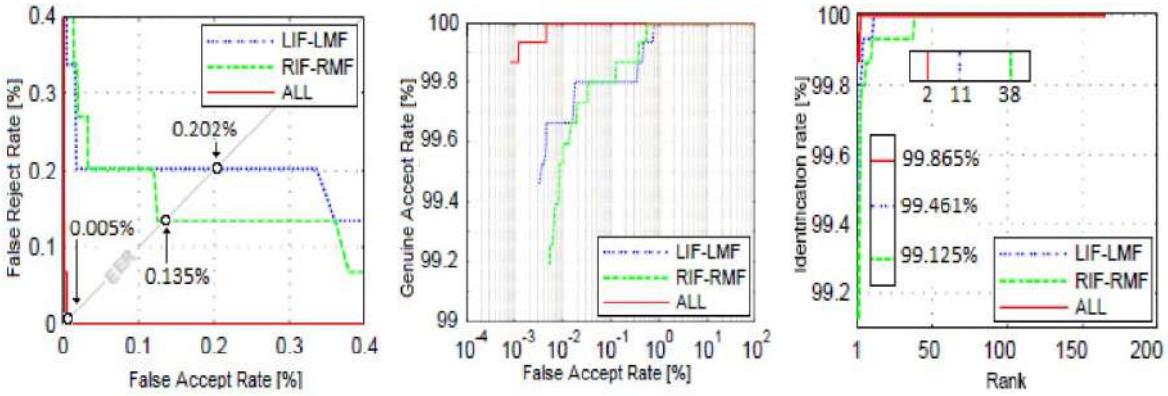
TABLE 5.6: Performance of the FKP based multimodal *Open/Closed-set* identification system (Fusion at Feature Level)

COMBINATION	OPEN-SET IDENTIFICATION		CLOSED-SET IDENTIFICATION	
	T_0	EER	ROR	RPR
LIF-LMF	0.7673	0.202	99.461	11
RIF-RMF	0.7809	0.135	99.125	38
ALL	0.8672	0.005	99.865	2

modalities can produce a best performance, ROR equal to 97.441% (RPR = 36), 97.037% (RPR = 104) and 96.700% (RPR =112), respectively. To summarize the *closed-set* identification experiments, graphs showing the Cumulative Match Characteristics (CMC) curves using all unimodal systems were generated in Fig. 5.7.*(c)*. In conclusion, the obtained identification rates for FKP modalities are equal or even better than those obtained in several previous works in the literatures and make this technology sufficient for several applications.

❷ **Multimodal systems performances:** In this part of experiments, we examine the performance of the multimodal system at two fusion level which are fusion at feature and score levels. So, the purpose of the present part is to examine whether the performance of a biometric identification system can be improved by integrating complementary information which comes primarily from different modalities (different fingers). Another issue that concerns this part is the effect of level fusion (feature level or matching score level) on the performance of biometric identification systems.

❒ **Fusion at feature level:** Fusion at feature level can be applied in the extraction of different feature vectors from the different multi-modalities. On the other hand, concatenating the feature vectors extracted from FKP modalities is an example of a multimodal system. Fusion at the feature level is expected to perform better in comparison with fusion at the other levels. The main reason is that the feature level contains richer information about the raw biometric data. Thus, the data obtained from each biometric modality (LIF, LMF, RIF and RMF) is used to compute a feature vector. The idea of fusion at the feature extraction level is to concatenate the feature vectors of different biometrics (different fingers). The new feature vector has a higher dimensionality and represents a person's identity in a different feature space. It is noted that, there are three different combinations of fingers for the fusion purpose, the two fingers for the same hand (LIF-LMF and RIF-RMF) and the four fingers (LIF-LMF-RIF-RMF for simplified it is noted ALL). In addition, in these experiments, the results obtained for the identification tests are given in terms of EER. Table 5.6 shows the baseline results obtained using the three combinations. These results demonstrate the capability of fusion in reducing the *open/closed-set* identification error rate, particularly that in ALL combination. In the case of *open-set* identification mode, it is observed that the use of fusion process leads to reducing the lowest EER offered by the best unimodal system (EER = 0.606%). However, it is also seen that this capability of fused biometrics is considerably improved through the ALL combination (EER = 0.005% and $T_0 = 0.8672$). The reduction in EER achieved with this combination is in excess of 99%. On the other hand, it is observed that the fusion process, using the rest of the combinations, can reduce, the efficiency of the EER. Thus, an improvement $\simeq$ 67% and 78% can be produced by using, respectively, LIF-LMF (EER = 0.202%, $T_0 = 0.7673$) and RIF-RMF (EER = 0.135%, $T_0 = 0.7809$). The *open-set* identification test, reported in Fig. 5.8.*(a)* and Fig. 5.8.*(b)*, aims at showing the advantage of using the fusion process.



(*a*) (*b*) (*c*)

FIGURE 5.8: FKP based multimodal *open/closed-set* identification test results under the best combinations (fusion at feature level). (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*) The CMC curves.

Similarly, the second mode of identification (*closed-set* identification) was tested for all combinations and the results are reported in Table 5.6 to be compared. However, comparing the errors produced by all combinations, it is clear that using ALL combination improves the system performance; in addition employing the rest of the combinations improves further this error. Almost an improvement $\simeq$ 78%, 64% and 95% can be generated using, respectively, LIF-LMF, RIF-RMF and ALL combinations. In the case of using a LIF-RIF combination, a ROR of 99.461% with RPR = 11 is achieved. Using LMF-RMF combination, ROR was 99.125% with RPR = 38. All Fingers combination improves the result (ROR = 99.865% and RPR = 2) for a database size of 165 persons. Based on the results, it should be noted that, on the contrary to *open-set* identification mode, the LIF-LMF combination become very efficiency than RIF-RMF combination. Finally, Fig. 5.8.(*c*) presents a direct comparison of the effectiveness of All combination with those of the others as CMC plots. As the computational time is minimum, these multimodal identification systems are becoming very suitable for a variety of applications, especially, those involving automatic access control like *e*-banking, physical access control and the withdrawal of money from automatic telling machines (ATMs).

❒ **Fusion at score level:** In the previous sub-part, the effective feature level fusion was discussed. This sub-part examines the investigations into the effectiveness of matching score level fusion in both *open-set* and *closed-set* multimodal biometrics. At the matching score level fusion, it is possible to combine scores obtained from different fingers modalities. The overall score is then sent to the decision module for accepting or rejecting a person. Currently, this appears to be the most useful fusion level because of its good performance and simplicity. In the former approach, a scalar fused score is obtained by normalizing the input matching scores into the same range and then combining such normalized scores. In our work, we use rule-based technique for fusing the scores produced by the different unimodal identification systems. Thus, maximum rule (MAX), minimum rule (MIN), sum rule (SUM), weighted sum rule (WHT) and product rule (MUL) are used.

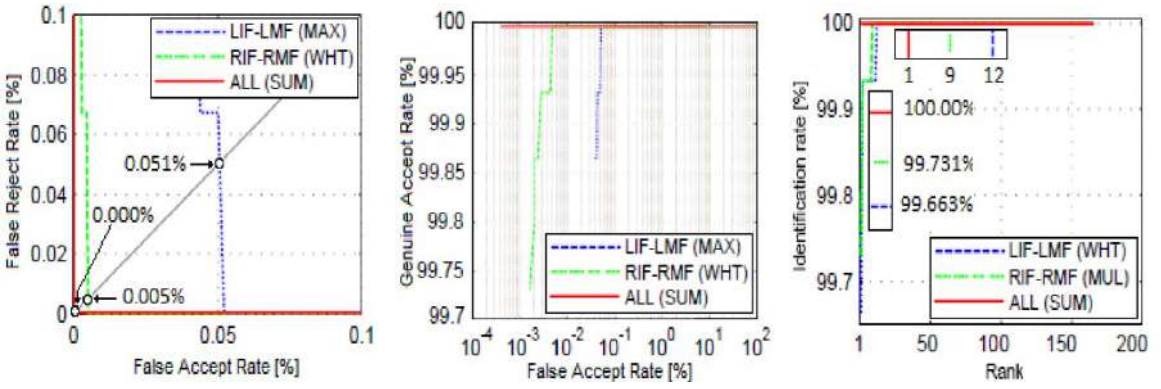
The experiments in this sub-part of the study investigate the effectiveness of the fusion at the matching score level in enhancing the reliability of multimodal identification system when two or more modalities (fingers) are combined. For that, the experimental results for the *open-set* identification

TABLE 5.7: Performance of the FKP based multimodal *Open-set* identification system (Fusion at Matching score Level)

Combinations	SUM		WHT		MIN		MAX		MUL	
	T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER
LIF-LMF	0.7861	0.069	0.7614	0.122	0.7769	0.267	0.9623	0.051	0.6954	0.135
RIF-RMF	0.9003	0.010	0.9272	0.005	0.7940	0.135	0.9947	0.038	0.8555	0.012
ALL	0.9330	0.000	0.9308	0.000	0.8106	0.081	0.9990	0.070	0.9323	0.000

TABLE 5.8: Performance of the FKP based multimodal *Closed-set* identification system (Fusion at Matching score Level)

Combinations	SUM		WHT		MIN		MAX		MUL	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
LIF-LMF	99.596	8	99.663	12	99.327	123	97.172	3	99.596	21
RIF-RMF	99.371	7	97.731	5	99.461	52	97.441	4	99.731	9
ALL	100.00	1	100.00	1	99.529	38	94.882	3	100.00	1



(*a*) (*b*) (*c*)

FIGURE 5.9: FKP based Multimodal *open/closed-set* identification test results under the best combinations (fusion at matching score level). (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*) The CMC curves.

mode, respecting all combinations and fusion rules, are presented, as EER, in Table 5.7. The results in Table 5.7 show that, generally, the use of fusion resulted in better performance than the best individual modalities and the fused biometrics at feature level. Moreover, it is observed that the ALL combination with SUM, WHT and MUL rules successfully reduce the EER to zero for the fused biometrics which is, in this case, more efficient than several previous works obtained using FKP biometric. For these combinations, a considerable improvement equal to 100% is obtained. Using the MIN and MAX rules provides 87% and 89% of improvement, respectively. The ROC curves, in Fig. 5.9.(*a*) and Fig. 5.9.(*b*), presents a direct comparison of the performances obtained using fusion based on LIF-LMF and RIF-RMF combinations, using best rules, together with the performance for the ALL combination.

The experimental results for the *closed-set* identification mode are presented in Table 5.8. As the experimental results show in this table, the identification rate (ROR) for the ALL combination, with SUM, WHT and MUL rules, is also greater than the corresponding ones in the feature level. On

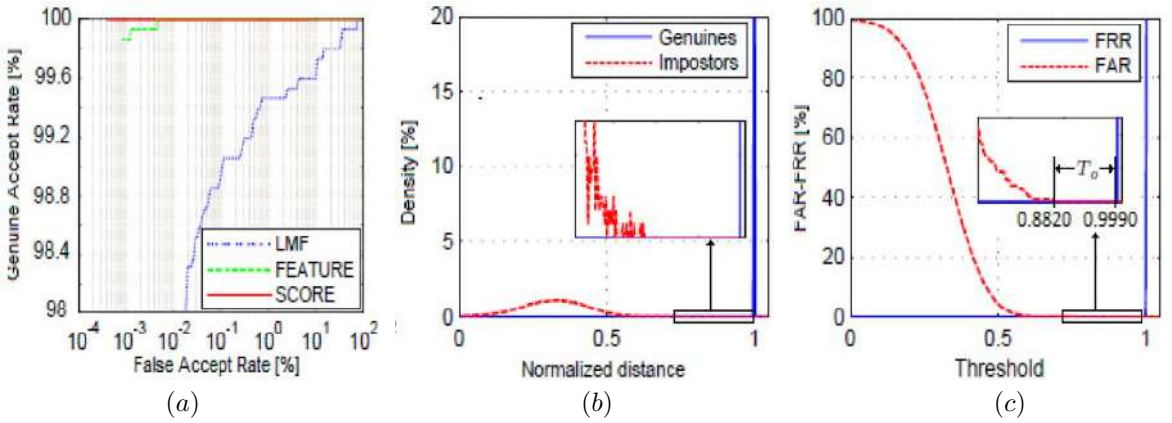


FIGURE 5.10: Performance of the best multimodal identification system.(a) Comparison between the unimodal and multimodal systems, (b) The genuine and impostor scores distribution and (c) The FAR against FRR by varying the decision threshold.

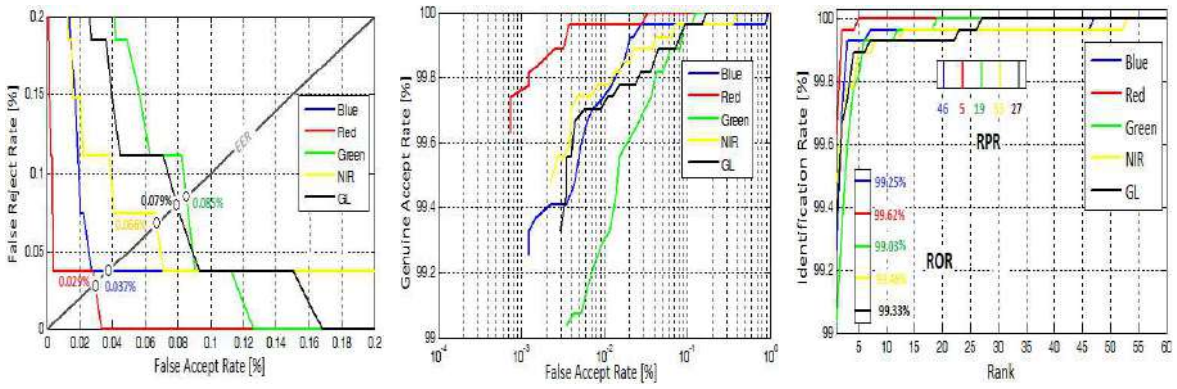
the other hand, although the MAX is provide very efficiency accuracy in the *open-set* identification mode, the accuracy rates for the *closed-set* identification mode are observed to be very poor's. Finally, the curves in 5.9.(c) which plot the CMCs curves for all bests cases, demonstrate the capability of reducing the identification error rates by combining all fingers in the matching score level. Finally, in order to selection the best biometric identification system, with lowest error, a comparative study of the effectiveness of the best unimodal and multimodal identification systems based on the previous experimental results, is made. For that, graphs showing the ROC curves for the *open-set* identification using unimodal and multimodal systems, were generated (see Fig. 5.20.(a)). By the analysis of this plot, it can be observed that the performance of the identification system is significantly improved by using the fusion of all fingers and can give a *zero EER*. To further demonstrate this efficiency, we plot, in Fig. 5.20.(b) and Fig. 5.20.(c), the distribution of the genuine and impostor scores and the relationship between FAR and FRR rate by varying the decision threshold. From Fig. 5.20.(b), it is clear that the two distributions are independent which provide necessary zero error as shown in Fig. 5.20.(c), were the system produce a zero error at a threshold value, T_0, belong the interval $[0.8820 \cdots 0.9990]$. Therefore, the developed multimodal system is expected to give higher accuracy.

Also, another works in same field of FKP identification system were performed during the realization of this work by proposing an efficient FKP based biometric identification such as [114, 115].

5.6.3 Palmprint based identification system

In this section, we propose an efficient online personal identification system based on Multi-Spectral Palmprint images (MSP) using the BSIF descriptor to extract the textural information of the palmprint images while the euclidean distance is used to distinguish between the different persons palms.

❶ **Unimodal systems performances:** the goal of this experiment was to evaluate the proposed system performance when we using information from each band. Thus, in the case of *open-set* identification, the ROC curves for five distinct bands are shown in Fig.5.11.*(a)* where the gray level (GL) representation is created by using the three band (Red, Green and Blue (RGB)). The experimental



(*a*) (*b*) (*c*)

FIGURE 5.11: PLM based unimodal *open/closed-set* identification test results under different fingers. (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*)The CMC curves.

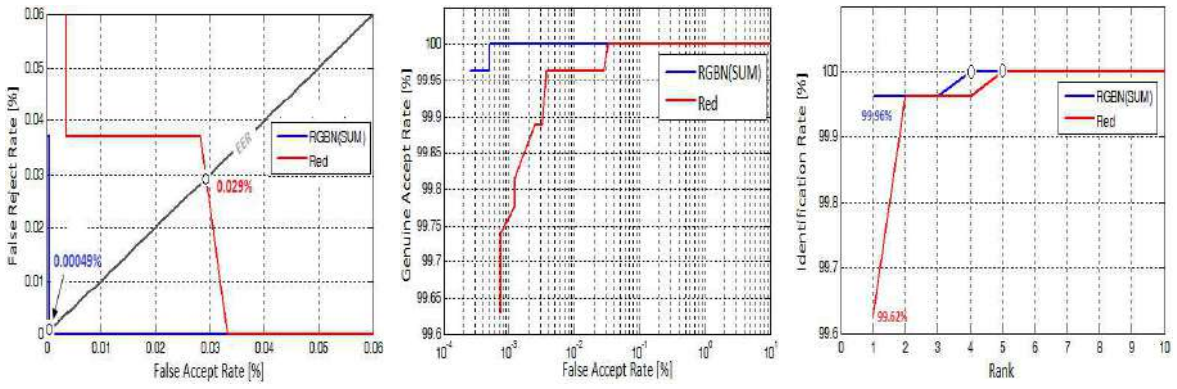
TABLE 5.9: PLM based unimodal identification test results

Bands	OPEN-SET IDENTIFICATION		CLOSED-SET IDENTIFICATION	
	T_0	EER	ROR	RPR
Blue	0.037	0.0534	99.2529	46
Green	0.0851	0.581	99.0370	19
Red	0.0293	0.0546	99.6296	5
NIR	0.0669	0.1026	99.4815	53
GL	0.0795	0.0686	99.3333	27

results indicate that the Red band perform better than the Blue, Gree, NIR band and GL representation in terms of EER. For example, we can see that our proposed system can operate, if only the GL representation is used, the system produce an EER equal to 0.0795% and the corresponding threshold is $T_0 = 0.0686$. In the case of using the Blue band, EER was 0.037% at the $T_0 = 0.0534$. The Green band done an EER equal to 0.0851% at the $T_0 = 0.581$. The use of NIR band gives and EER equal to 0.0669% with $T_0 = 0.1026$. Finally, the use of Red band improves the result (0.0293% at $T_0 = 0.0546$) for a database size equal to 300 persons. Fig. 5.11.*(b)*, provide a more detailed point of view of the performance of proposed palmprint unimodal *open-set* identification systems. Finally, the performance of the *open-set* identification system under different bands is shown in Table 5.9.

In the case of a *closed-set* identification, a series of experiments were carried out to select the best band. This has been done by comparing all bands and finding the band that gives the best identification rate. Table 5.9 present the experiments results obtained for all bands. From Table 2, the best results of Rank-One Recognition (ROR) produce 99.6296% with lowest Rank of Perfect Recognition (RPR) of 5 when the Red band is used. In order to see the performance of the proposed system under this mode of identification Fig.5.11.*(b)* is plotted.

❷ **Multimodal systems performances:** The objective of this section is to investigate the integration of several bands, and to achieve higher performance that may not be possible with unimodal biometric alone. Thus, to find the better of the all fusion rules and all combination (RGB and



(a) (b) (c)

FIGURE 5.12: PLM based unimodal *open/closed-set* identification test results under different fingers. (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*)The CMC curves.

TABLE 5.10: Performance of the PLM based multimodal *Open-set* identification system

Combinations	SUM		WHT		MIN		MAX		MUL	
	T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER
RGB	0.012	0.0004	0.008	0.0007	0.061	0.018	0.02	0.0019	0.008	0.00009
RGBN	0.024	0.0004	0.023	0.0007	0.076	0.017	0.041	0.0.002	0.005	0.0007

TABLE 5.11: Performance of the PLM based multimodal *Closed-set* identification system

Combinations	SUM		WHT		MIN		MAX		MUL	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
RGB	99.963	5	99.963	5	99.851	8	99.925	3	99.963	5
RGBN	99.963	4	99.963	4	99.925	9	99.925	11	99.963	4

RGBN), with the lowest EER, graphs showing the ROC curves was generated (see Fig.5.12.*(a)* and Fig. 5.12.*(b)*).

In the case of RGB combination, only the Red, Green and Blue bands are used. In fact, at such a case the system works as a kind of multimodal system with a single biometric trait but multiple units. Therefore, information presented by different bands is fused to make the system efficient. For the *open-set* identification mode, The obtained results from individual fusion based rules indicate the SUM rule has performed better than other in terms of the EER. For example, if the MIN rule is used, our identification system can achieve an $EER = 0.0189\%$ at the threshold $T_0 = 0.06150.8281$. In the case of using the MAX rule, $EER = 0.0019\%$ at the threshold $T_0 = 0.0208$. Using WHT rule, EER was 0.00073% at the threshold $T_0 = 0.0089$. If MUL rule is used, we have $EER = 0.00097\%$ at the threshold $T_0 = 0.0089$. Finally, a SUM rule improves the result (0.00049% at $T_0 = 0.012$) for a database size equal to 300 persons. Finally, the performance of the open set identification system under different fusion rule is shown in Table 5.10.

For the closed set identification mode, a series of experiments were carried out using the MSP palmprint database to selection the best fusion rule that maximize the ROR rate. Thus, to determine the best fusion rule, Table 5.11 can be established. We can observe that the SUM, MUL and the

WHT based fusion has the best performance. Thus, the best result of ROR is given as 99.963% with lowest RPR of 4. Finally, from this result, the performance of the closed set identification system is improved by using the fusion (see Fig.5.12.*(c)*).

In the case of RGBN combination, all bands are fused. For this, a series of experiments were carried out using the MSP database. for the *open-set* identification. The performance of the proposed identification system is seem to bo like the performance of the system when using the RGB combinations. The system achieve a high performance when using the SUM,WHT and the MUL fusion rule by giving an EER equal to 0.0004% at the thresholding ($T_0 = 0.024$, $T_0 = 0.023$ and $T_0 = 0.005$) respectively. Finally, always Table 5.10 tabulates EER for the RGBN and fusion rules.

In order to see the performance of the closed set identification system, we usually present, in table 5.11, the results for RGBN combinations and fusion rules. This table shows that the SUM,WHT and MUL rule offers better results in terms of the ROR. For example, if MAX rule is used, we have $ROR = 99.925\%$ with $RPR = 11$. In the case of MIN rule, ROR was also 99.925% with $RPR = 9$. Using SUM, WHT or MUL rule, ROR was the same as obtained when using the RGB combination (99.963%) while the RPR value is reduced from 5 to 4. Therefore, the system can achieve higher accuracy at the fusion of the matching score compared with a single matching score.

It is important to note that there another work had been performed in the field of palmprint recognition such as the work in [116, 117].

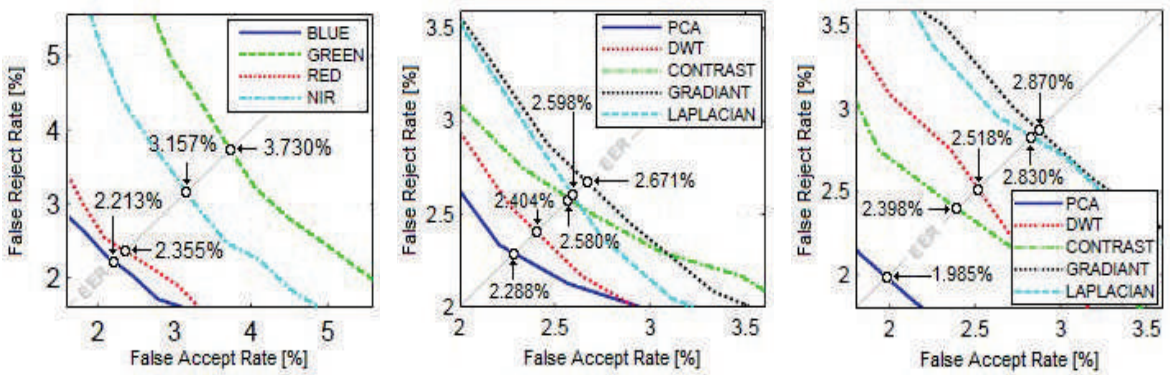
5.7 3D-LBP based Biometric system

In the previous we had perform several experiments in order to concept a biometric based identification system that can extract the principal line , the shape or the textural information of biometric modalities with high level of accuracy, precision and robustness. What it is observed from the conception of those system is that the system require from the biometric input to be in a gray level representation or an image with single band. Using such another representation like color or MSP/HSP, will give the system a much more information that can be useful to distinguish between user's this on one hand. On the other hand, the use of this type of images will increase the system time processing and affect on the system database size. Our proposed 3DLBP descriptor establish its self as a powerful mean in this kind of situations and it will be more adequate for color or MSP/HSP images recognitions and classification problems. Hence, to proof the theoretical part and in order to evaluate the efficiency of the proposed method, we choose to test our method through a multi-spectral palmprint based biometric system which can be considered as an appropriate application example. Another reason to justify the use of palmprint modality is that the FKP and EAR modalities based biometric system application are still a laboratory based application and no real life application using the FKP and the EAR are developed yet. Furthermore, another experiments was performed which treating the impact of our descriptor on image edge detection problem.

In this part of experiments, the biometric identification tests results are divided into two parts. First part presents the performance of the original LBP based palmprint identification algorithm for different spectral bands. For this, experiment was conducted using these bands (BLUE, GREEN,

TABLE 5.12: LBP based unimodal identification test results

SPECTRAL BANDS	*Open-set*		*Closed-set*	
	T_0	EER	ROR	RPR
BLUE	0.049	2.213	79.500	51
GREEN	0.061	3.730	58.458	116
RED	0.051	2.355	71.583	51
NIR	0.059	3.157	64.875	110



(*a*) (*b*) (*c*)

FIGURE 5.13: LBP based *open-set* biometric identification test results.(*a*) Performance comparison between different spectral bands, (*b*) RGB based multimodal *open-set* identification performance and (*c*) RGBN based multimodal *open-set* identification performance.

RED and Near-infrared (NIR) band) to choose the band yield the best performance (minimum Equal Error Rate (EER)). Also, this part contains the performance of the multimodal systems using the fusion, at image level, of some spectral bands. In our work, the fusion in image level is realized using five techniques which are : Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA) and pyramidal analysis such as LAPLACIAN, GRADIANT and CONTRAST techniques. In the second part, we present the performance of our proposed 3DLBP method. In this part, a comparative study was conducted to show the effectiveness of the proposed 3DLBP descriptor.

❶ LBP based identification system test results

The goal of the first experiment was to evaluate the system performance when we using information from each spectral band (unimodal biometric identification system). For the *open-set* identification mode, the ROC curves for four distinct spectral bands are shown in Fig. 5.13.(*a*).The obtained experimental results are given in Table 5.12. The experimental results indicate that the BLUE band performs better than the RED, GREEN and NIR bands in terms of EER. From this figure, we can see that the system can operate, if only the GREEN band is used, at a 3.730% EER and the corresponding threshold is $T_0 = 0.0605$. Using the RED band, EER was 2.355% at the $T_0 = 0.0507$. The NIR band done an EER equal to 3.157% at the $T_0 = 0.0588$. Finally, the use of BLUE band improves the result by an EER = 2.213% at $T_0 = 0.0489$.

In the case of a *closed-set* identification, a series of experiments were also carried out to select the best spectral band. From our obtained results, the best Rank-One Recognition (ROR) produces 79.500% with lowest Rank of Perfect Recognition (RPR) of 51 in the case of BLUE spectral band. The system

TABLE 5.13: Performance of the LBP based multimodal *open/closed-set* identification system (RGB combinations)

PCA		DWT		CONTRAST		GRADIENT		LAPLACIAN	
T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER
0.046	2.288	0.043	2.404	0.047	2.590	0.044	2.671	0.047	2.598
ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
76.042	107	71.417	75	75.125	107	72.833	120	72.375	132

TABLE 5.14: Performance of the LBP based multimodal *open/closed-set* identification system (RGBN combinations)

PCA		DWT		CONTRAST		GRADIENT		LAPLACIAN	
T_o	EER	T_o	EER	T_o	EER	T_o	EER	T_o	EER
0.046	1.985	0.043	2.518	0.046	2.398	0.043	2.870	0.050	2.830
ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
80.250	83	67.958	126	75.958	99	71.833	153	74.00	105

can achieve a ROR of 71.583% for RPR = 51 in the case of using the RED spectral band. If NIR band is used for the identification, the system can achieve a ROR = 64.875% with RPR = 110. Finally, GREEN spectral band gives the poor result with ROR = 58.458% and RPR = 116.

From several works in literature, the system performance could be improved by the integration or fusion of information from each spectral band. This integration can be performed in one of four system levels : image level, feature extraction level, matching score level and decision level. Therefore, the last three levels require the extraction of features of each band separately and then fused, which increase the time processing. Thus, the system is implemented using Matlab 7.5 on a PC embedded by Intel Pentium processor (2.2 GHs) with 2 Go RAM. The average processing time of LBP based identification system for single spectral band, t, is equal to 1.6 seconds for a database contains 300 persons. If the RED-GREEN-BLUE (RGB) bands are used, the system needs almost $3 \times 1.6 = 4.8s$ for identify a person. Another disadvantage of using several LBP descriptors is the greater size of the feature vector. For solve these limitation, the different bands are fused in order to obtain a single image.

Image fusion is the process by which two or more images are combined into a single image. For that, a series of experiments were carried out to selecting the best combination (RGB: fusion of RED, GREEN and BLUE bands or RGBN: fusion of all bands) and fusion techniques (DWT, PCA, LAPLACIAN, GRADIANT or CONTRAST) that minimize the EER. However, in order to see the performance of the *open-set* identification system performance, we usually give, in Fig.5.13.(*b*), the results for all the image fusion techniques in the case of RGB combination. Thus, the result suggests that the PCA technique has performed better than others (EER = 2.288% and $T_0 = 0.0457$). The *open-set* identification system can achieve an EER of 2.404% for $T_0 = 0.0431$ with the DWT technique and it can achieves an EER equal to 2.580% at the decision threshold $T_0 = 0.0470$ for CONTRAST technique. If GRADIENT technique is used for the fusion, our system can achieve an EER = 2.671% with $T_0 = 0.0435$. In the case of using LAPLACIAN technique, EER was 2.598% at $T_0 = 0.0468$. However, it can be concluded that the fusion by PCA technique yields much better biometric identification results compared with one image spectral band.

Similarly, in the case of RGBN combination, always the resulting fused image using PCA technique improves the open-set identification performance (EER = 1.985% at $T_0 = 0.0464$). In this case an improvement about 11% can be achieved. However, in order to see the performance of the *open-set* identification system performance, we usually give, in Fig. 5.13.(*c*), the results for all the image fusion techniques in the case of RGBN combination. The rest of image fusion techniques give ERRs equal to 2.518% ($T_0 = 0.046$), 2.398% ($T_0 = 0.0462$), 2.870% ($T_0 = 0.043$) and 2.830% ($T_0 = 0.0495$) for respectively DWT, CONTRAST, GRADIENT and LAPLACIAN based image fusion techniques, (see Table 5.13 and Table 5.14).

In *closed-set* identification performance, also, Table 5.13 and Table 5.14 illustrate the experimental results for the two combinations (RGB and RGBN). Regarding this tables, it is seen that PCA technique achieves the better results when compared to the rest of image fusion techniques for the two combinations.

❷ 3DLBP based identification system test results

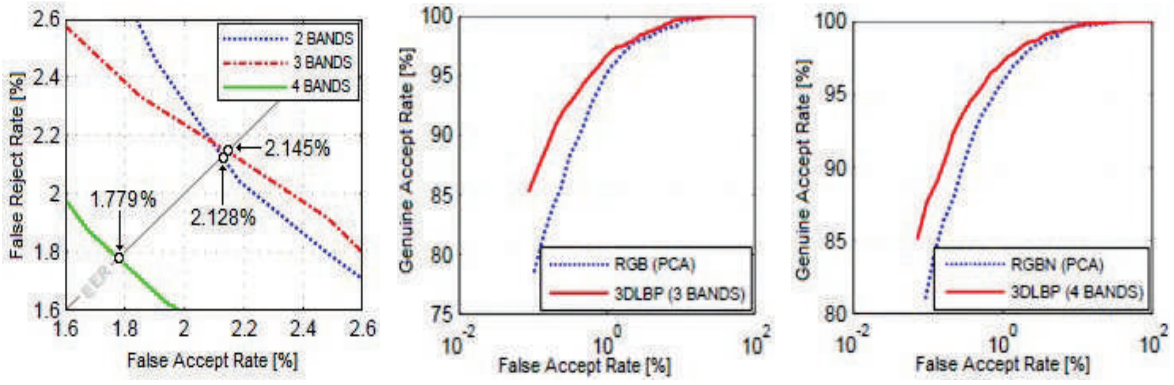
The objective of this section is to investigate the integration of our method as a feature extraction method in the biometric identification system. In our system, different spectral bands were tested to find the combination that optimizes the system accuracy. Thus, to find the best of the all combinations with the lowest EER, Fig. 5.14.(*a*) were generated, for three combinations with, respectively, two, three and four spectral bands. From this figure, it is clear that, combining the spectral band modalities enforces effectively the security of the *open-set* identification system. Furthermore, it may be noted that the system can operate, if only two spectral bands are used, at a 2.128% EER and the corresponding threshold is $T_0 = 0.0504$. In the case of using three spectral bands, EER was 2.145% at the $T_0 = 0.0477$. Finally, the use of four spectral bands improves the result (1.779% at $T_0 = 0.0462$) for a database size equal to 300 persons.

In addition, in *closed-set* identification, the system produces ROR= 73.833% (RPR = 128), 82.625% (RPR = 73) and 82.250% (RPR = 103) identification rate for, respectively, two, three and four spectral bands. To prove the effectiveness of our proposed method, graphs showing the ROC curves for the open-set identification using all best systems for the two combinations (RGB and RGBN), were generated (see Fig. 5.14.(*b*) and Fig. 5.14.(*c*). However, the comparative experimental results show that the identification rate of the *open-set* identification system based on 3DLBP descriptor for 3 and 4 spectral bands is higher than that of the identification rate adopting the LBP descriptor based system. Thus, the multispectral palmprint based biometric system is significantly improved by using the 3DLBP descriptor and can use in several security applications.(see Table 5.15 for more details).

To summarize the experiments, graphs showing the ROC curve and CMC curve for the 3DLBP based *open-set* and *closed-set* identification using the best systems, were generated (see Fig. 5.15.(*a*) and Fig. 5.15.(*b*). Finally, the genuine and impostor distance distributions are plotted in Fig. 5.15.(*c*). The obtained experimental results show that the proposed method performs best, in both *open-set* and *closed-set* identification modes, and is much better than person identification using only single spectral band or multiple spectral bands using image fusion.

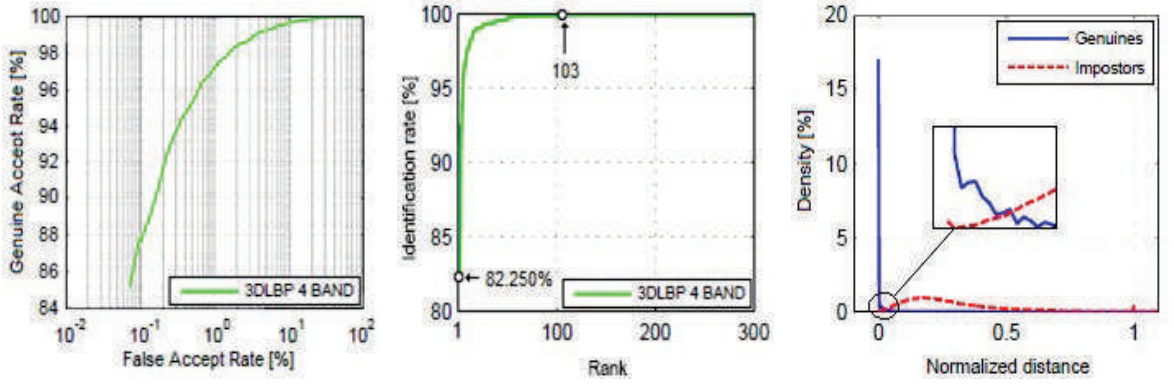
TABLE 5.15: 3DLBP-based identification test results

Combinations	*Open-set*		*Closed-set*	
	T_0	EER	ROR	RPR
2 Spectral Bands (*e.g.* Red-Green (RG))	0.0504	2.128	73.833	128
3 Spectral Bands (*e.g.* Red-Green-Blue (RGB))	0.0477	2.145	82.625	73
4 Spectral Bands (*e.g.* Red-Green-Blue-Near-Infrared (RGBN))	0.0462	1.779	82.250	103



(*a*) (*b*) (*c*)

FIGURE 5.14: 3DLBP based *open-set* biometric identification test results.(*a*) Performance comparison between different combinations, (*b*) Comparison between LBP and 3DLBP descriptor in the case of RGB combination and (*c*) Comparison between LBP and 3DLBP descriptor in the case of RGBN combination.



(*a*) (*b*) (*c*)

FIGURE 5.15: 3DLBP based *open-set/closed-set* biometric identification test results. (*a*) ROC curve for the best case (four bands), (*b*) CMC curve for the best case (four bands) and (*c*) Genuine and impostor distance distribution.

❒ **3DLBP processing time:** As mentioned previously in the last Sections, one of the disadvantages of the application of the original LBP on the color image or multi/hyper spectral images is the increase of the time processing. So, this part of experiments aims to show the efficiency of our proposed method on reducing the processing time. The average processing time of LBP based feature extraction for single spectral band, t, is equal to 1.6 seconds. This time, under our method, for a single band is $1.6s$ because the original LBP is a special case of the 3DLBP when the number of bands is equal to 1. If two bands are used, our descriptor processing time is $t = 1.59s$ instead $2 \times 1.6 = 3.2s$ for the LBP

descriptor. If the three bands (RGB) are used, the LBP based system need almost $3 \times 1.6 = 4.8s$ where our 3DLBP based system processing time is $1.79s$. Finally, using all bands (RGBN), the 3DLBP processing time is less than the LBP processing time ($t_{3DLBP} = 1.61s, t_{LBP} = 4 \times 1.6 = 6.4s$). To resume the experiments Table 5.16 is presented. Finally, it is important to note that we performed our experiments, using Matlab 7.5, on a PC embedded with Intel Celeron processor (2.0 *GHz*), 2 *Go* of memory under Windows 7 operating system.

TABLE 5.16: 3DLBP time processing performance

Combinations	3DLBP	LBP
1 Spectral Bands (*e.g.* Red, Green, Blue, NIR)	1.6s	1.6s
2 Spectral Bands (*e.g.* Red-Green (RG))	1.59s	3.2s
3 Spectral Bands (*e.g.* Red-Green-Blue (RGB))	1.79s	4.8s
4 Spectral Bands (*e.g.* Red-Green-Blue-Near-Infrared (RGBN))	1.61s	6.4s

❒ **3DLBP based Edge Detection Technique:** In the previous section, the effectiveness of the proposed 3DLBP descriptor on multispectral palmprint based identification system was discussed. In this section, we try to use 3DLBP in order to detect the image edges. An edge is simply a change in gray level occurring at one specific location. The greater the change in level the easier the edge is to detect, but in the ideal case, any level change can be seen quite easily. Thus, the edges of an image can be extracted using the edge detection technique.Edge detection is one of the most commonly used operations in image analysis, recognition and classification, and there are several algorithms in the literature for enhancing and detecting the image edges (or image contours). An interpolation of the bit values of each $3DLBP$ code is enough to detect any change and if this code contains an information concerning the image edges. Thus, contrary with $3DLBP$, a threshold T is added to the original form, we call this technique $3DLBP_T$ and it is defined as:

$$3DLBP_T(x_c, y_c) = \sum_{p=0}^{P} s_T(d)2^p \tag{5.1}$$

where $s_T(d) = 1$ if $d \geq T$, otherwise $s_T(d) = 0$. After the $3DLBP_T$ codes are predetermined, the edges of the image can be constructed,however, a $3DLBP_T$ code contains one or two bitwise transitions from 0 to 1 or 1 to 0, e.g. 11111000, 11100011, 00111100 and 00011111, is probably contain an edge. Thus, the image edges is defined as:

$$I_E(x_c, y_c) = \begin{cases} 1, \text{ if } 1 \leq R\left[\text{3DLBP}_T(x_c, y_c)\right] \leq 2 \\ 0, \text{otherwise} \end{cases} \tag{5.2}$$

where I_E represents the edges of image (image contours) and R is a function determining the number of the bitwise transitions in 3DLBP_T codes.

To evaluate the 3DLBP_T based edge detection technique, we use five images (*chess*, *box*, *lena*, *palm* and *retina* image). All of these images are in color format (three spectral bands, $N = 3$) with size equal to 128×128. The first two images (*chess* and *box*) contains straight objects (rectangles and lines), whereas, the second three images (*lena*, *retina* and *palm*) contains curved objects. The

technique is executed for several threshold and the best edges images, for $T = -40,\ -20,\ 0,\ 20,\ 40$, are plotted in Fig. 5.16.

From this figure, the following observations can be made: Firstly, this technique is directly related to the edges form in the image, *e.g.* the edges of straight objects are well detected. Thus, for *chess* and *box* images the $T = -40$ ($3DLBP_{-40}$) outperforms than the others threshold. Secondly, by using this technique, the resulting edges of the two curved images are very acceptable and can be used in several applications. In addition, in the *palm* image and *retina* image, the threshold was 40 instead of -40. Finally, $3DLBP_0$ provide a poor result for all images. As conclusion, these results reveal that $3DLBP_T$ can extract more detailed information and it is very important in several pattern recognition applications.

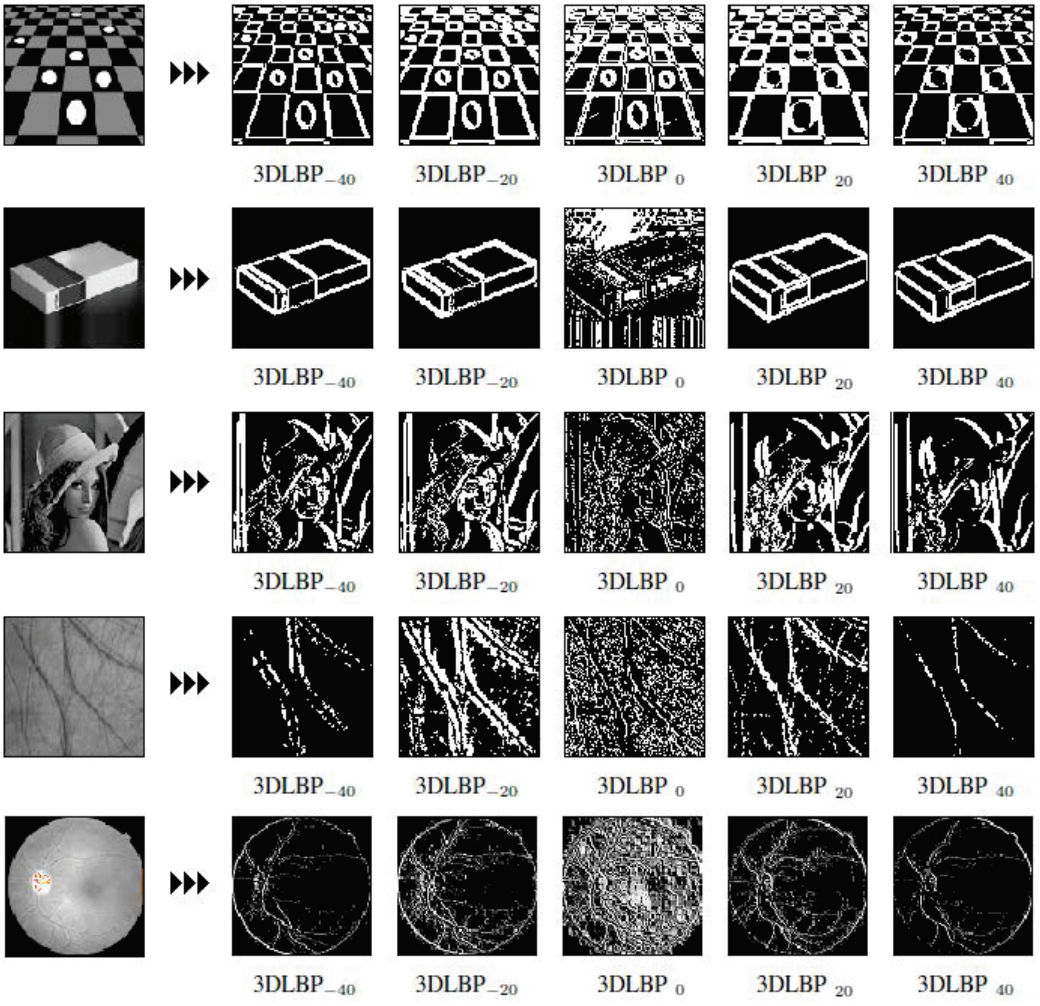


FIGURE 5.16: 3DLBP based Edge features in various images at several thresholds.

5.8 Summary and comparative study

The first part of experiment deals with the conception of biometric based identification system where the purpose was the augment the system performance in term of accuracy, robustness, time processing and database size. To achieve that different biometric identification system were proposed using different biometric traits from the human body.The used biometric modalities include EAR,FKP and PLM traits. those modalities contains distinct features. To extract them we propose the use of four powerful descriptor for extracting the EAR principal lines, the FKP shape and the PLM textural informations. A new variant called 3DLBP of the well known texture descriptor (LBP) is proposed and evaluated to enlarge the application of LBP to be able to extract the textural information of a color or MSP/HSP images where the aims is to reduce the time processing and the database size. To validate the obtained results and the efficiency of the proposed system, one shall compare these results with the existed research works in the field of the EAR, FKP and PLM recognition. Table 5.17 presents a comparative study between the proposed system and the existing state of art.

TABLE 5.17: Performances comparison of our proposed systems with the state-of-the-art

Feature Type		EER	ROR
line approach	[118]	2.0185%	97.73%
	proposed system	1.193%	92.398%
Texture approach	[119]	0.0074%	/
	proposed system	0.0004%	99.963%
shape approach	[120]	0.321%	/
	proposed system	0.000%	100%

it is noted that and due to the huge number of paper that treat the application of the Local Binary Pattern (LBP) on color or MSP/HSP images, no work had been performed , according to our knowledge, that extract directly the information from the color images. For that our proposal descriptor 3DLBP present its self a powerful means for performing this task with a reduction of time processing and database memory size.

Part II

Biometric Crypto-system based E-voting Protocol

5.9 Introduction

Nowadays, the internet becomes very vital for any kind of information exchange. One of the applications which can use internet for information exchange is Online voting (*e-voting*). Indeed, *e-voting* has several advantages like the accessibility for the disabled and elderly; the ease of long-distance voting; the low costs and the greater voter turnout. Thus, the challenges that oppose e-voting application are the concerns of security of transmitted data which are exchanged (chosen candidate) as well as the privacy issues (voter information), which ensure the secrecy of voter information.

In this part of experiments, we propose a secure Biometric-crypto scheme dedicated to online *e-voting* system. The fuzzy commitment concept associated with the palmprint (PLM) modality is the core of our system. In this part of study, to enhance the discriminating capability of the PLM feature vectors, we suggest the use of BSIF descriptor combined with *bit-plane* decomposition method. This choice is justified by the high performances obtained with the use of this descriptor in term of accuracy and high genuine key retrieval rate. Subsequently, the voter's data is encrypted using a random key then this key is binding in the extracted feature vector using the fuzzy commitment scheme. Then, in the central system, a new scheme for the key retrieval is implemented in order to extract this key which used for decrypt the message and then treated.

5.10 *e-voting* system Description

The main objective of this part is to design and develop a secured *e-voting* system. The proposed system uses symmetric cryptographic and multi-factor authentication methods. Thus, in our system (Fig.5.17), voter's authentications are based on a card combined with a PIN code and a biometric trait. The proposed *e-voting* system based on multi-factor authentication is shown in Fig. 5.17. So, in the following sub-sections, we describe in detail each phase of the proposed *e-voting* system.

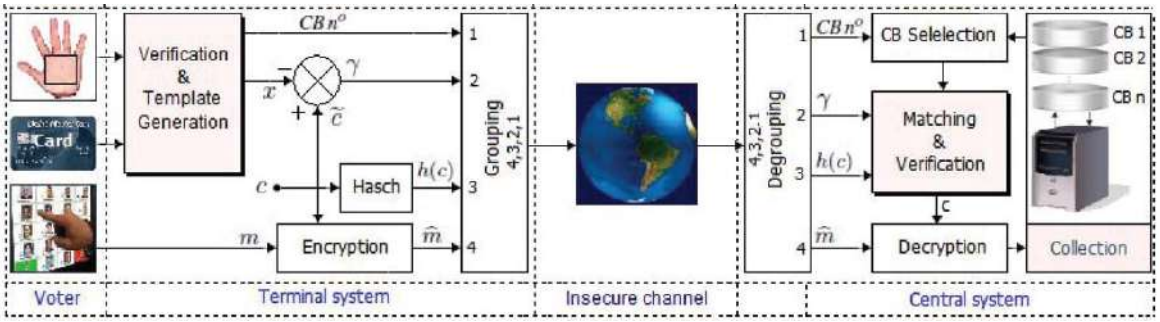


FIGURE 5.17: Proposed online *e-voting* system based on PLM images and a fuzzy commitment based symmetric cryptography.

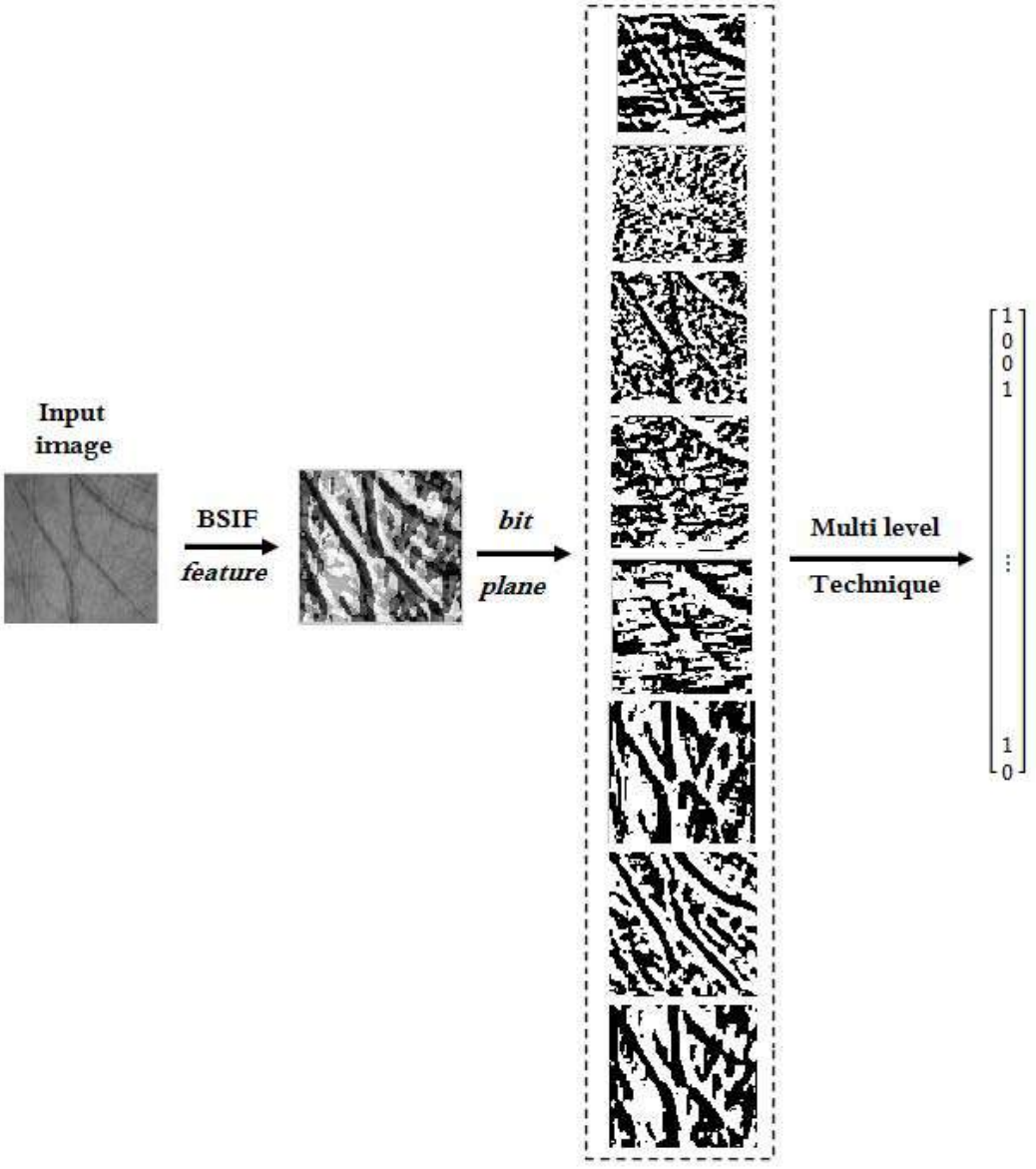


FIGURE 5.18: Framework of the proposed feature extraction method.

5.10.1 Enrollment phase

For each voter, during the enrollment process, the feature vectors (or template) is generated from their PLM biometric modalities and stored for later use (identification process) in a voter's identification server as well as in the voter ID smart-card. In addition, a PIN code is randomly generated and stored in this smart-card. However, the PIN code is used for security purposes and to authenticate the user in the electronic voting device (e.g. PC or smart-phone). Also, a registration number (which is used for selecting the voter sub-database) is generated and stored in both voter's identification server and voter ID smart-card.

In our biometric system, the feature vectors are generated from the PLM ROI sub-images by filtering it with the ML-BSIF descriptor combined with the *bit-plane* decomposition in order to generate a

binary template. The process of obtaining the binary template is described as fellow: at the first stage applying the BSIF feature descriptor on the input PLM ROI images to generate a new representation.When the BSIF features are extracted, the *bit-plane* decomposition is applied to generate eight new binary images (eight images are generated because we choose the number filter in the BSIF code as 8 filters). Finally, the multi-level technique is applied on one chosen of the eight binary images. it is noted that the proposed methodology will be named as **BPBSIF** (Bit Plane Binarized Statical Image Features). Fig 5.18 summarize the process of the proposed methodology.

5.10.2 Sending & data encryption process

In the electronic voting (terminal system), the voter's vote (selected candidate) is sent over the network in an encrypted data format. In this system, two steps can be find:

1. **Verification step:** As the first step of the sending process, verification and template generation are the foundation on which the ID card PIN code is verified, if it is true, the feature extraction technique is applied on the voter PLM modality to generate the template (feature vector) and then to be compared with the stored template in ID card. On the other hand, if the card PIN code or the extracted feature vector does not match with these in the ID card, the voter access is denied(see Figure 5.19).

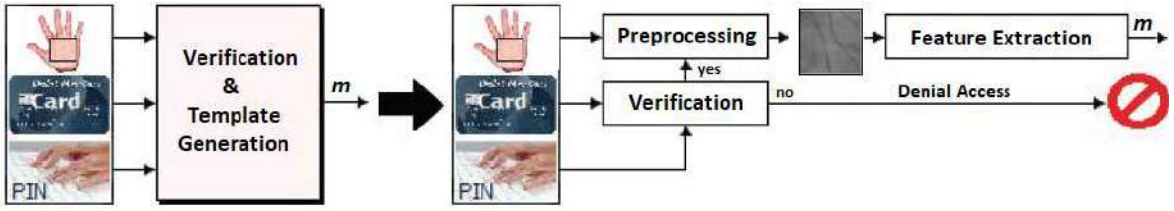


FIGURE 5.19: Flowchart of access verification and template generation process in voter terminal.

2. **Message encryption & Key embedded step:** After the preliminary verification in which the feature vector is extracted, a fuzzy commitment scheme (where an encryption key, c, is protected using the extracted vector, x) is applied. In this case, a combination function (f) is used in order to associate the key c with a person and to compute an offset such as $\gamma = \widetilde{c} \oplus x$. $\widetilde{c}$ is a vector in which several key c is concatenated until the length of the extracted vector $\widetilde{c}$ becomes equal to x. The encrypted message (the fuzzy commitment) is then represented by the pair $(\gamma; h(c))$, where $h(c)$ is a one way hash function. It is worth to notice that neither the biometric feature, nor the associated codeword are publicly transmitted.Finally, the electronic voting system sent: *i)* the voter sub-database, $CB\ n^o$ (stored in smart-card during enrollment), *ii)* the offset γ , *iii)* the hash function $h(c)$ and iv) the encryption voter data ($\widehat{m}$) to the central server for collecting.

5.10.3 Receipting & data decryption process

In the central system, the authentication process is correctly performed if a fresh feature vector reading x_i allows the computation of a binary string $\widetilde{c}_i = x_i \oplus \gamma$ sufficiently close to $\widetilde{c}$ so that the code decodes it to c and the comparison between their hash values succeeds. In this case, the central system can decrypt the voter data ($\widehat{m}$) and send confirmation to him.

1. **Identification & Key retrieval:** In the key retrieval process, the feature vector of the stored voter (x_i) in the system database is XORed with the binary string γ ($\widetilde{c}_i = x_i \oplus \gamma$). Now, the key can be recovered. To achieve that, bits of binary vector $\widetilde{c}$ are mapped into matrix M_x (with size of $\eta_1 \times \eta_2$ where η_1 represents the key length and η_2 is the number of key within $\widetilde{c}$) and the key retrieval is performed by taking the majority vote among M_x. After that, the extracted key is concatenated until the length of $\widetilde{c}$ become equal to the length of the feature vector x_i, then a XORed function is applied on the $\widetilde{c}$ and γ to obtain the template x. Then, the obtained template x is matched with x_i by the Hamming distance to obtain a distance d_o. If d_o is below a predefined security threshold, T_o, the key $\widetilde{c}$ must be verified. Thus, to check whether the retrieving key ($\widetilde{c}$) is identical to the key generated (c) in the central system, the system checks to see whether $h(c) = h(\widetilde{c})$.
2. **Message decryption step:** Our scheme decrypts confidential data (voters data) that has been encrypted using biometric data combined with random numbers (encryption key). As a result, confidential data can be decrypted just with the voters biometric data (stored in central system database); however, the need for a proper and reliable key management mechanism is required in order to confirm that the listed keys actually belong to the given voters. Indeed, the central system uses key recovery algorithm to disassemble the encryption key (c) from the feature vector and then to decrypt transaction data ($\widehat{m}$) and authenticate the voter.

$$m = \mathcal{F}^{-1}(\widehat{m}, c) \tag{5.3}$$

where m is the original voter data, $\widehat{m}$ is the encrypted voter data, c is the key and $\mathcal{F}^{-1}$ denote the decryption function.

5.10.4 Multimodal System

As previously discussed and analyzed, biometric system performance when using single biometric trait produces some errors. For that, in this study, we try to improve their performance by using the data fusion principal. However, in the proposed multimodal system, the two used representations of palmprint, GL and NIR representations, operate independently and their results are combined using score level fusion scheme. Thus, as our main goal is to improve the e-voting system, it is necessary that we evaluate the performance of the identification system based on several key lengths. So, several key binding schemes are proposed using the best fusion rule. Thus, in general, two schemes can be found. In the first one, the same key is bound to the two feature vectors produced by the used biometric modalities (duplicated key in the two palmprint representations GL and NIR). Consequently, in this

case, the entire encryption key is given by:

$$c = \begin{cases} \widetilde{c}_{GL} & \text{if} \quad h(c) = h(\widetilde{c}_{GL}) \\ \widetilde{c}_{NIR} & \text{if} \quad h(c) = h(\widetilde{c}_{NIR}) \\ \widetilde{c}_{GL} \quad or \quad \widetilde{c}_{NIR} & \text{if} \quad h(c) = h(\widetilde{c}_{GL}) = h(\widetilde{c}_{NIR}) \end{cases} \tag{5.4}$$

where the $\widetilde{c}_{GL}$ is the retrieved key from the GL based palmprint representation and the $\widetilde{c}_{NIR}$ is the retrieved key from the NIR representation. Whereas, in the second scheme, each template (for each representation) contains a different key. Thus, in this case, the entire encryption key is given by the concatenated of the two extracted keys, as follow:

$$c = [\widetilde{c}_{GL} \quad , \quad \widetilde{c}_{NIR}] \tag{5.5}$$

It is important to note that, the first scheme is dedicated for the small to medium length key, whereas, the second scheme for the greater length key.

5.11 System performance evaluation

Experiments are performed on the Hong Kong PolyU multi-spectral palmprint database[112]. This dataset can be considered as an example similar to the number of voters in small to medium sized office. In all experimental results, two image representations are used, the first representation (Gray Level-GL), is constructed from the red, green and blue bands, and the second representation is the Near-Infrared (NIR) band. Thus, we randomly select three samples for each representation in order to construct the system database (enrollment phase). The remaining nine samples were used to test the system performance. Accordingly, the aim of this part of experiments is to design a key binding based Biometric-Crypto system using those two previous representation in order to choose which representation is better to be used in the Biometric-crypto system conception.

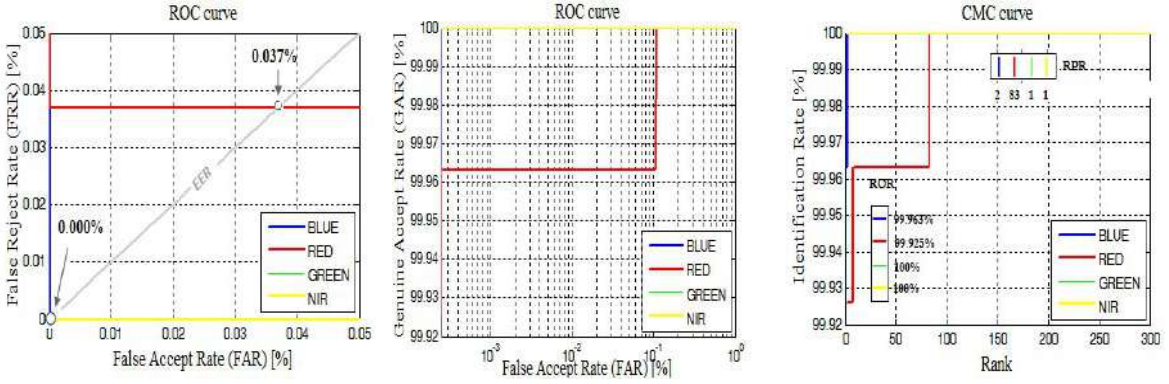
In our work, the set of experiments are divided into three sub-parts. In the first sub-part, we present a comparison study between the unimodal biometric system by applying our proposal approach which combines both the ML-BSIF and the *bit-plane* technique(**BPBSIF**) in order to show the efficiency of the proposed combination as a feature descriptor and also to observe the system performance without key encryption key insertion . The second sub-part focus on the biometric system performance in which the encryption key is embedded. In this sub-part, several key lengths (32 bits to 512 bits by a step of 32 bits , 512 bits to 1024 bits by a step of 64 bits and 1024 to 2032 by a step of 128 bits) were tested. Note that, in these two sub-parts we use unimodal biometric systems. Finally, the last sub-part is devoted for evaluate the performance of the multimodal based *e-voting* systems.

5.11.1 BPBSIF based unimodal system evaluation:

The aim of the first experiment is to evaluate the system performance without key insertion when we use our proposal descriptor (BPBSIF technique). Thus, in our e-voting scheme, before using the proposed biometric system in a biometric-crypto protocol, it must (firstly) evaluated to test the

TABLE 5.18: BPBSIF based unimodal identification test results

SPECTRAL BANDS	*Open-set*		*Closed-set*	
	T_0	EER	ROR	RPR
BLUE	0.12	2×10^{-4}	99.963	2
GREEN	0.093	0.000	100	1
RED	0.3345	0.037	99.925	83
NIR	0.108	0.000	100	1



(*a*) (*b*) (*c*)

FIGURE 5.20: BPBSIF based Unimodal *open/closed-set* identification test results under different bands. (*a*) The ROC curves (FRR against FAR), (*b*) The ROC curves (GAR against FAR) and (*c*)The CMC curves.

efficiency and robustness of the proposed methodology. To evaluate the performance of the proposed unimodal system, Table 5.18 is generated. after an analyzing of this table, it can be observed that the proposed BPBSIF descriptor can be considered as a powerful descriptor for discriminating the user's identity or other pattern recognition application. Thus, for the *open-set* identification mode, all the bands based system performance had an excellent performance , this can be justified by the lowest value of EER which is equal to 0.037 at a threshold $T_0 = 0.3345$ when we use the red modality. On the other hand , the BLUE band give an EER almost equal to zero ($EER = 2 \times 10^{-4}$ at a threshold $T_0 = 0.12$). the best perfomance can be observed when we use the NIR or the Green bands where the system achieve an EER equal to zero.

For the *closed-set* identification mode. also Table 5.18 illustrate the obtained results in this mode. similarly to the *open-set* mode, the use of our proposal methodology give an excellent and remarkable results in term of ROR and RPR . From this table, it can be seen also that the NIR and the Green bands achieve the better results by giving $ROR = 100\%$ and $RPR = 1$. the use of the BLUE band gives $ROR = 99.963\%$ with $RPR = 2$ where the lowest ROR is achieved when we use the RED band($ROR = 99.925$ and $RPR = 83$). To summarize the performance of the proposed unimodal identification system ,Fig.5.20 is plotted.

5.11.2 Biometric-Crypto system security analysis

Generally, the typical practice in a biometric-crypto system is that a key must randomly generated and then binds in the feature vector for the user (voter). Thus, this method always makes the system more secure. For that, several tests (several key sizes) are presented in this sub-section in order to evaluate the key retrieval task as well as the biometric system performance at the receiver end. Basically, at the reception of the transmitted data, the system must identified is this voter is an authorized voter (genuine voter) or not. For that, the system must execute firstly an *open-set* identification task. If the voter is accepted, then a *closed-set* identification is performed in order to authenticate exactly this voter.

❶ Unimodal biometric-Crypto system evaluation

In this sub-part, we examine the performance of the biometric-Crypto system when single representation(GL or NIR) is used. Indeed, the biometric system performance can be affected by the variation of the length of the key, because this key is combined with the biometric template at the terminal users level and retrieved at the receiver end level and then used again to generate the biometric template. For that, a series of tests is performed in order to evaluate the biometric system performance when the key length is varied.The obtained experimental results are shown in Table 5.19 and Table 5.20 under both representation NIR and GL. The experimental results in this two table indicate that, firstly, the integration of the key in feature vector doesn't affects the accuracy of the system and the system get a 100% of ROR with $RPR = 1$. This can be justified by the high discriminability and robustness of the proposed BPBSIF descriptor. By reading in-depth the results obtained in this tables, we observe that the maximum key retrieval rate is equal to 100% for key size $32, 64, 96, 160, 192, 224, 288, 320, 352, 416, 448, 480, 576, 704, 832, 960$bits for both representation, It is also expected that there are another key size where the system can achieve the 100% of key retrieval rate because of the key step used for the evaluation.Hence, for the rest key sizes, and when the GL representation is used, Table 5.19, show that the key retrieval rate is confined between $\left[58.3704\% \quad \cdots \quad 99.9255\%\right]$, the lowest rate of key retrieval is obtained when a key of size $1024bits$ is used whereas the other key sizes key retrieval rate are exceed the 99.50% except the 512 and 1536 key size where the system achieve a key retrieval rate of 97.8185% and 96.8148% respectively.

On the other hand, when the NIR representation is used. The first observation which can be made is that the lowest obtained key retrieval rate when the GL representation is used becomes greater than the GL one at key size of $1024bits$(65.4444%). another observation from the NIR results (see Table 5.20) is that the key retrieval rate at the key size of $512bits$ and $1536bits$ are better than the obtained when using the GL representation(97.5556% and 97.070%). For the other key size and from Table 5.19 and Table 5.20 , it can be seen that the system performance under the NIR representation is almost similar to the system performance when we use the GL representation with a slight superiority of the GL representation compared to the NIR based system performance. In this context, the system achieves the maximal key retrieval rate (100%) at the same key size when we used the GL representation and the other key size retrieval rate are bounded between $\left[99.2963\% \quad \cdots \quad 99.7728\%\right]$. To summarize the genuine key retrieval rate under the two representation in terms of key sizes Fig 5.21. is plotted.

TABLE 5.19: GL based Biometric-Crypto system performance evaluation

Key size	Closed-set identification		Genuine key retrieve	Impostor key retrieve
	ROR	RPR		
32	100	1	100	41.1537
64	100	1	100	12.0674
96	100	1	100	39.9475
128	100	1	99.9255	0.9050
160	100	1	100	38.6109
192	100	1	100	11.3282
224	100	1	100	40.2757
256	100	1	99.7037	0.2770
288	100	1	100	35.6490
320	100	1	100	10.6335
352	100	1	100	34.2549
384	100	1	99.8889	0.7611
416	100	1	100	33.6953
448	100	1	100	11.4099
480	100	1	100	32.5760
512	100	1	97.5185	0.0116
576	100	1	100	9.1096
640	100	1	99.8889	0.6999
704	100	1	100	8.4137
768	100	1	99.5926	0.1992
832	100	1	100	8.2076
896	100	1	99.8889	0.7628
960	100	1	100	7.4936
1024	100	1	58.3704	0.0022
1152	100	1	99.8519	0.5094
1280	100	1	99.5556	0.1717
1408	100	1	99.8519	0.4016
1536	100	1	96.8148	0.0042
1664	100	1	99.8519	0.4125
1792	100	1	99.5926	0.1992
1920	100	1	99.7407	0.3439
2032	100	1	99.7037	0.0691

In the previous sub-part, the biometric-crypto system under the genuine key retrieval rate criteria is analyzed. it is great that the system achieve a 100% of key retrieval rate in certain key sizes. but , on the other hand, another criteria must be taken into consideration which the robustness of the proposed biometric-crypto system against the impostor or the adversary attacks, or in other words, how the impostor is able to reconstruct or to retrieve the cryptographic key. At this end , this part discuss the impostor key retrieval rate under the two representations. it obvious that when the cryptographic key has a small size, the impostor guess easily the key and its capability of retrieve the key is decreased when the key size length increase. Moreover, the impostor key retrieval rate under different key sizes is also cited in Table 5.19 and Table 5.20, by a comparison between the results obtained in those two tables under the two representations, one can note the maximum impostor key

Table 5.20: NIR based Biometric-Crypto system performance evaluation

Key size	Closed-set identification		Genuine key retrieve	Impostor key retrieve
	ROR	RPR		
32	100	1	100	51.9557
64	100	1	100	15.0053
96	100	1	100	50.7717
128	100	1	99.7728	0.7938
160	100	1	100	49.4535
192	100	1	100	14.0146
224	100	1	100	51.0913
256	100	1	99.6296	0.2435
288	100	1	100	46.3582
320	100	1	100	13.1495
352	100	1	100	44.8463
384	100	1	99.7407	0.6570
416	100	1	100	44.2963
448	100	1	100	14.1031
480	100	1	100	42.9521
512	100	1	97.5556	0.0114
576	100	1	100	11.1815
640	100	1	99.7407	0.6062
704	100	1	100	10.2537
768	100	1	99.5185	0.1670
832	100	1	100	10.0389
896	100	1	99.7407	0.6597
960	100	1	100	9.0303
1024	100	1	65.4444	0.0022
1152	100	1	99.7407	0.4387
1280	100	1	99.5185	0.1491
1408	100	1	99.7037	0.3441
1536	100	1	97.0370	0.0067
1664	100	1	99.7037	0.3590
1792	100	1	99.5185	0.1660
1920	100	1	99.7037	0.3020
2032	100	1	99.2963	0.0587

retrieval rate is observed when we use a key size of length $32bits$ where the impostor can achieve a 51.9557% of key retrieval rate under the NIR representation. As for the GL representation the maximum rate,the impostor can achieve a 41.1537% of the key in the same key size. For the rest of key size impostor retrieval rate, one can observe that this rate when we use the GL images is among the interval of $\left[7.4936\% \quad \cdots \quad 41.1537\%\right]$ and among the interval $\left[9.0303\% \quad \cdots \quad 51.9557\%\right]$ under the NIR images for the key size less than $1000bit$ except the key size of rank 128 where the impostor key retrieval rate didn't exceed the 0.9050% when the system is based on GL images and 0.7938% for the NIR images. For the key greater the $1000bits$ the rate become less then 0.51% and balanced between $\left[0.0022\% \quad \cdots \quad 0.5094\%\right]$ under the GL representation and between $\left[0.0022\% \quad \cdots \quad 0.3590\%\right]$ under the NIR representation. To see the performance of the proposed biometric-crypto system against the

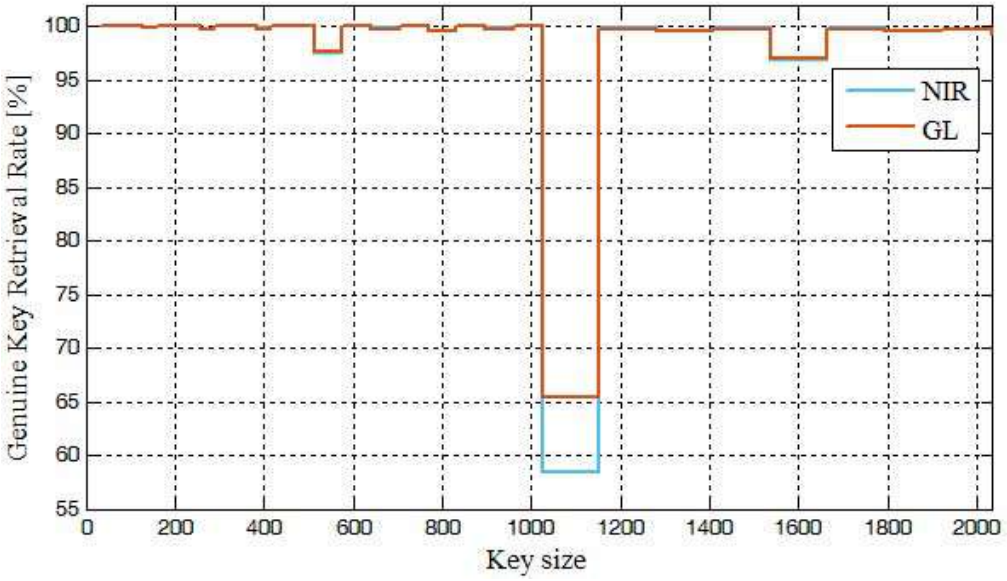


FIGURE 5.21: Biometric-Crypto system genuine key retrieval rate under the two representation GL and NIR with different key sizes .

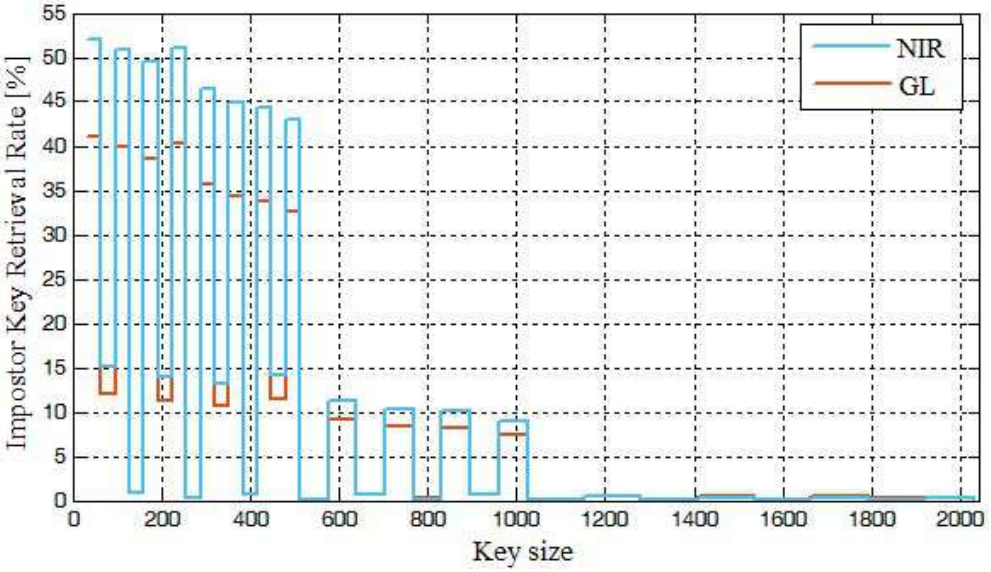


FIGURE 5.22: Biometric-Crypto system impostor key retrieval rate under the two representation GL and NIR with different key sizes .

impostor attack, Fig 5.22 is made.

Generally, biometric systems that use a single modality or single representation for identification are often affected by several practical problems like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait and unacceptable error rates. Multimodal biometric systems overcome some of these problems by consolidating the evidence obtained from different sources. For that, the objective of the next sub-section is to test our system when multi-modality principal is used.

❷ Multimodal biometric-Crypto system evaluation

Previously, we say that the data fusion process can be performed at each level of biometric identification system. Matching at score level is the efficient scheme of fusion due to their simplicity, ease implementation and practical aspects. In this scheme, the individual matching scores from the two subsystems are combined to generate a single scalar score. The aim of this subsection is to investigate whether the system performance could be improved by using the fusion of information from each modality or each representation. However, due to that the unimodal biometric-Crypto system based on our BPBSIF descriptor under the two palmprint representation achieve an $EER = 0.000\%$ for the *Open-set* mode and a $ROR = 100\%$ for the *Closed-set* mode. we didn't interested on the influence of data fusion on the biometric-crypto system accuracy. So, our main aim in this sub-part is to study the affect of data fusion process on the genuine and impostor key retrieval rate.

Traditionally, two fusion schemes can be found : key duplication and key separated. In the first one, the same key is bound to the two templates produced by the two representation. In the second scheme, each template for each representation contains a different key. What is remarked from the evaluation of the unimodal based biometric-Crypto system performance is that the system achieve a lower performance when we use a key in order of $128bits$ whereas the other key length, the system achieve a 100% key retrieval rate. So, to see the effect of data fusion on the key retrieval rate we use a key in order of $128bits$ (128, 256, 384, 512, 640, 768, 896 and 1024 bits). The obtained experimental results are illustrated in Table 5.21 and Table 5.22 for both fusion schemes. For the first scheme evaluation(duplicated key i the two representations), from Table 5.21 a height improvement is remarked in term of genuine key retrieval rate especially in the case of $128bits$ where the system achieve a 100% key retrieval rate . For the other key length, a remarkable improvement is observed when the fusion process is deployed. as example, when we use a key with length of $512bit$ the system achieve a genuine key retrieval rate of 99.2963% (where it was 97.55% in the best case of unimodal system). Also, from this table , another observation is remarked, a great improvement is achieved when we use a key size of $1024bit$, the best genuine key retrieval rate in the unimodal system was 65.4444% (in the case of the use of NIR representation) where the genuine key retrieval rate in the case of using fusion process was 76.7778%. Finally, for the other key sizes the rate is bounded between $\left[99.9259\% \quad \cdots \quad 99.9630\%\right]$. For the impostor key retrieval rate evaluation, it is obvious that this rate will be increased be of the duplication of the key in the two representations, the rate was between $\left[0.0022\% \quad \cdots \quad 0.9050\%\right]$ in he case of unimodal system where in the case of multimodal system, the rate is varies between $\left[0.0022\% \quad \cdots \quad 1.4961\%\right]$. In general, the duplication scheme is dedicated for small key sizes and not preferred for the long key sizes.

For the second scheme where the key is devised in the two representation. the obtained results are shown in Table 5.22. From this table , the first note that appear from the result analysis is that the impostor key retrieval rate is reduced almost to zero where the rate varies between $\left[0.0022\% \quad \cdots \quad 0.0557\%\right]$ which give this schemes a great influence on the system security. For the genuine key retrieval rate evaluation, the global key is the concatenation of the two extracted key. Table 5.22 indicate a great improvement of genuine key retrieval especially in the case of key length of $512btis$ which means a global key with size of $1024bits$ where the rate was 95.7778% (improvement of 46.34% compared with the best case obtained in the unimodal system (65.4444%). Also, for the other key sizes , the rate is improved by the means of fusion process. the more the key is increased,

TABLE 5.21: Biometric-crypto system based multimodal test results evaluation(duplicated Key)

Key size	Closed-set identification		Genuine key retrieve	Impostor key retrieve
	ROR	RPR		
128	100	1	100	1.4961
256	100	1	99.9630	0.4526
384	100	1	99.9630	1.2575
512	100	1	99.2963	0.0111
640	100	1	99.9630	1.1572
768	100	1	99.9259	0.3099
896	100	1	99.9630	1.2598
1024	100	1	76.7778	0.0022

TABLE 5.22: Biometric-crypto system based multimodal test results evaluation(Separated Key)

Key size(×2)	Closed-set identification		Genuine key retrieve	Impostor key retrieve
	ROR	RPR		
128	100	1	99.7037	0.0557
256	100	1	99.4074	0.0067
384	100	1	99.6667	0.0468
512	100	1	95.7778	0.0022
640	100	1	99.6667	0.0401
768	100	1	99.1852	0.0022
896	100	1	99.667	0.0468
1024	100	1	47.6667	0.0022

the more the rate is improved. For example, in case of key size of $256bis$ (a global key of $512bit$) the rate is enhanced from 97.5556% to 99.4074%. As another example, if the key size is $384bits$ (which means $768bits$) the rate is improved from 99.5926% $\rightsquigarrow$ 99.6667%. which justify why this schemes of fusion is preferred when we use a long key sizes for protecting the information.

It is important to note that, regarding the PLM images, it is obvious to find several persons presenting almost the same feature vector due the high inter-class correlation. Thus, if an attacker possesses a feature vector similar to that of the voter, then the attacker could retrieve the embedded key. As a result, it can decrypt the transmitted data in the network. Thus, a very little probability that two voters have a very similar of two PLM image representation GL and NIR, for that, the use of multi-modality scheme with sharing the key in the two modalities allows decreasing the probability that an attacker retrieve the encryption key. This can be justified by the obtained results where the impostor or the attacker key retrieval rate is approximately reduced to 0.000%. To show and prove the utility and the efficiency of using the multimodal process, a comparison between the unimodal and the multimodal biometric-crypto system performance in term of genuine and impostor key retrieval rate is performed and plotted in Fig 5.23.

5.11.2.1 Biometric-Crypto system with greater databases

Generally, the number of voters is much greater, which is systematically increasing the size of the voters database. Thus, the greater size of this database can provide several problems such as increasing

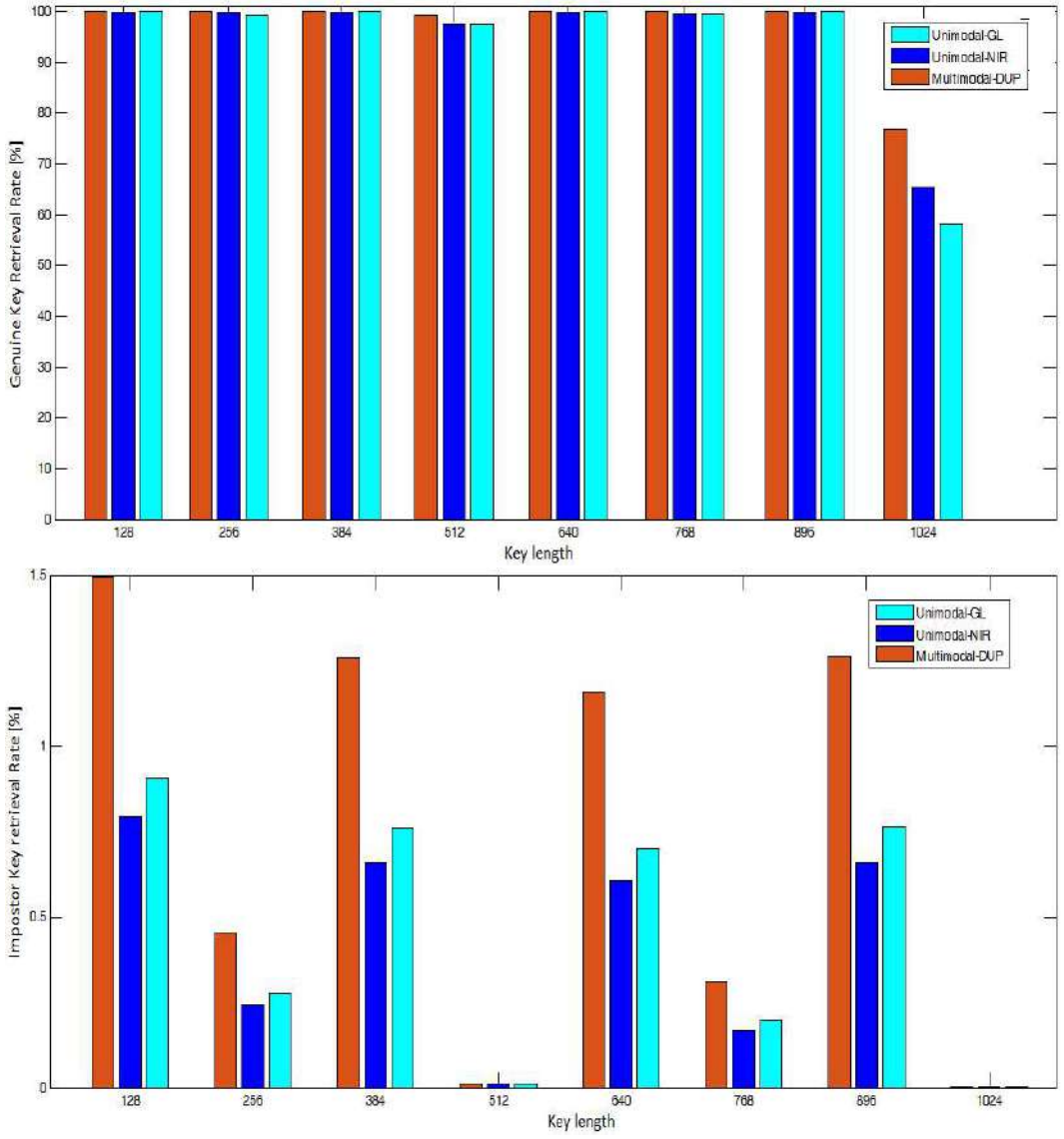


FIGURE 5.23: Unimodal/Multimodal Biometric-Crypto system test results evaluation comparison under different key sizes .

the response time and decreasing the biometric system accuracy. In order to decrease the response time and increase the biometric system accuracy, the system database is segmented into few sub-databases. Thus, our scheme provides effective results when using a database of 300 voters. If each voter has a $16 - bits$ registration number $CB\ n^o$ to select the sub-database, our scheme can works with a database size equal to $300 \times 2^{16} = 19,660,800$ voters($\backsimeq$ 20 million voters).Furthermore, if the registration number is represented on 20-bits, our scheme can works with a database size equal to $300 \times 2^{20} = 314572800$ voters($\backsimeq$ 314.5 million voters).

5.12 Conclusion

The aim of this chapter is devoted for the evaluation of proposed biometric identification system as well as the proposed Biometric-Crypto system performances. For that, the obtained experimental results were devised into two main part. In the first part, three designed approaches were discussed where the aim of this part is to enhance the user's privacy. To achieve that, different biometric identification systems were proposed using different biometric traits which are the EAR, FKP and palmprint modalities. therefore, and as the feature extraction phase is a crucial task in the conception of the identification system, various features extraction descriptors were used in order to extract the discriminant information of the biometric data. Those descriptors include Gabor filter response, HOG, BSIF feature and 3DLBP descriptor, each descriptor is applied on specific biometric identification system using an appropriate biometric modalities and appropriate classifiers. Also, it will be noted that our own 3DLBP application is not limited only to the color image. So, its application can be also extended to the multi/hyper spectral images, which give different information from a variety of spectral bands and can improve the performance of the system in term of accuracy, time processing and database size.

The objective of the study presented in second part is to develop a biometric-crypto system that implements the concepts of fuzzy-commitment scheme combined with palmprint biometrics to enhance the security and privacy of voters information (identity and opinion). In this study, to enhance the discriminating capability of the palmprint feature vector, we use feature extraction method based on combination between two technique namely bit plane technique and the ML-BSIF descriptor. Subsequently, the voter data is encrypted using a random key then this key is binding in palmprint (using two representation GL or NIR) modality of the voter using fuzzy commitment scheme. Then, in the central system, a new scheme for the key retrieval is implemented in order to determine the cryptographic key which used for decrypt the message and then treated. The analysis of the obtained experimental results, using a database of 300 voters, showed that voters can been trust in *e-voting* system which increased by the proposed palmprint based biometric-crypto system scheme.

Chapter 6

Conclusions, Perspectives, and Future Directions

Basically, the aim of the information security process is to ensure the confidentiality, integrity, and availability of information. It essentially provides the necessary protection to information and the supporting processes, systems, and infrastructures from various forms of possible threats and vulnerabilities. Biometrics and cryptography are two techniques which have high potential for providing information security. However, biometric is considered as the well known of establishing the identity of the user's by measuring one of physical/behavioral characteristics. On the other hand, Cryptography techniques are the most used tools in order to secure the information security during transmission or storage. Unfortunately, both of these have certain limitations. Biometrics suffer from non-revocability, non-template diversity, and possibility of privacy compromise. Whereas, the cryptography requires keys, but these keys are not strongly linked to the user's identity. To solve the problems related to biometric and cryptography, an alternative solution is proposed by combining those two techniques. We call such systems, in which biometrics and cryptography are combined, biometric-crypto systems.

The work presented in this thesis has two main folds: the first part is designed to the conception of biometric identification system based on biometric traits where the second part is devoted to the conception of the Biometric-crypto system. So, our main objectives were focused firstly to design robust biometric systems for a reliable user's identification. The second main objective is to concept and construct an encryption/Decryption Biometric-Crypto system (Encryption key generation) using an appropriate biometric modalities. To achieve that, three approaches were proposed and original features extractions techniques from different biometric modalities are used.

First of all, in order to concept a biometric identification system , we have introduced the notion of biometric and biometric technologies in terms of definitions, categorization of biometric modalities and the function of the biometric identification system. We also give an overview of the multimodal system process and its benefits compared to the unimodal system.

Secondly, because the Biometric-Crypto system is an emerging field which started from late 90's, we presented a systematic classification of the biometric-crypto systems found in literature based on

their principal goals and working methodologies. We proposed two major classes: *(1)* protection of biometric data and (2) obtaining biometrics based cryptographic keys. The systems in these two categories were further classified based on their working methodology.

It is well known that the biometric based identification system comport four main stages, the main and the important one is the feature extraction stage. For that, different feature extraction descriptors during the realization of this thesis were proposed. Our proper and main descriptor called 3DLBP has the capability of extracting the distinctive information from the user's traits from different images representation(gray, multi-spectral or hyper-spectral images) . Our 3DLBP benefits don't limited for increasing the the system accuracy but also fo minimizing the computational time and decreasing the system database size. the experimental results was performed on an available multi-spectral palmprint database which is an appropriate application example to show the efficiency of the proposed descriptor. The obtained results had proved the theoretical part in term of the three mentioned benefits. We are also motivated by the conception of different biometric identification system using different features extractions techniques under different biometric modalities. This is why, we propose a FKP and EAR based identification system using the HOG and Gabor filter response respectively. The proposed identification system had shown an important performance in terms of robustness,efficiency,precision and accuracy.

Finally,as it was mentioned, our second main objective was to design a biometric-crypto system. Literally, three ways can be found to integrate biometric with cryptography. So, we direct our research into the Key binding schemes based biometric-crypto system where the Fuzzy commitment scheme is used. The proposed biometric-crypto system is tested through a conception of an *e-application* namely *e-voting* system. In this architecture of biometric-crypto system, a binary template is required. To achieve that, we propose the use of a descriptor named BPBSIF where the ML-BSIF descriptor is combined along with a *bit-plane* technique. The experimental results are performed using the Multi-spectral palmprint database in which two representation of palmprint image (GL and NIR) are generated. The obtained results showed that the insertion of the cryptographic Key didn't affect the biometric based identification system. The performance of the proposed biometric-crypto system was tested through the calculation of the genuine key retrieval rate and impostor key retrieval rate. The results indicate that the system can achieve a 100% of genuine key retrieval rate in certain key size. Also , the system shows a great performance against an attacker or impostor where the greater impostor key retrieval rate didn't exceed the 50% by using the lowest key size($32bit$) and didn't exceed the 0.55% if the key size is greater than $1000bit$. However, the obtained results showed that the introducing of Multimodal based biometric-crypto system ameliorate the unimodal genuine key retrieval rate and reduce the impostor key retrieval rate approximately to zero.

At the end of the conclusion of this work, we intend in future work to use other approaches to extract features of biometric modalities. Also, we intend to use other binary template based feature descriptors. The deep-learning approaches become very popular by the researchers in the recent years . So, we will focus on the design of biometric based identification system using one of the deep-learning approaches such as PCANet(Principal Component Analysis Networ), DCTNet (Discrete Cosine Transform Network) LDANet (Linear Discriminant Analysis Network) or ICANet(Independent Component Analysis Network). Finally, we will redirect our research on the use of biometric-crypto system schemes such as fuzzy vault or designing a key generation based biometric-crypto system.

Appendix A

Region Of Interest (ROI) Extraction

A.1 Image preprocessing

SINCE the obtained biometric modalities images (raw data) are not directly usable by the biometric systems, they must undergo a preprocessing during which a region of interest (ROI) is extracted. The purpose of the preprocessing phase is to configure and modify the image (original biometric modality) so as to prepare it, to the feature extraction.

A ROI is an interesting image region, and can be used as a starting point for many image processing algorithms. As a result, the quality of the used algorithm to detect ROIs often conditions the quality of the entire processing chain result that is to be applied to an image. Also, the fact that the same (or near) ROIs can be detected on two different images but representing the same scene, is an important and generally required property for all ROI detection algorithms. In the biometrics field, the meaning of ROIs depends on the biometric modality type. It can match the eyes areas or areas around the mouth in the facial image, as it can match the iris in the eye image. Thus the extraction method will depend on the biometric modality.

A.2 Palmprint preprocessing

A palm is the hand inner surface between the wrist and the fingers. A palmprint is defined as an imprint on a palm. Therefore, the preprocessing phase, for this modality, is to isolate the palmprint (ROI) from the rest of the hand image obtained by any sensor (e.g. CCD camera). The extraction of ROI is not necessarily ideal, a tolerance of a few pixels in translation is introduced in both directions, vertical and horizontal. The ROI extraction method applied in our system is based on the algorithm described in [121].

Step1 : Noise Reduction

Image smoothing is an important operation, used to attenuate noise that corrupts information, before the binarization step. Indeed, a Gaussian linear low-pass filter makes it possible to reduce this noise due to the noise location in the high frequencies. After passing through a Gaussian low-pass filter of size 3×3 and a standard deviation $\sigma = 1.5$, a smooth image is obtained (see Figure A.1).

FIGURE A.1: Image filtering

Step2 : Binarization

Binarizing an image amounts to segmenting the image into two classes: the background and the object. This latter consists of putting the background in black and the object in white. Several binarization techniques exist, but the thresholding technique is the most popular, due to its ease of implementation and its rapidity. The final thresholding is performed by comparing the filtered image with a threshold T_P. This operation is given by the formula:

$$I_b(i,j) = \begin{cases} 1, & \text{if} \quad I_0(i,j) \geq T_p \\ 0, & \text{otherwise} \end{cases} \tag{A.1}$$

with I_0 is the original image after Gaussian filtering and I_b is the resulting binary image. To generate the T_P threshold, we opted for the Otsu method because of its eficiency. Figure A.2 shows the binarization operation.

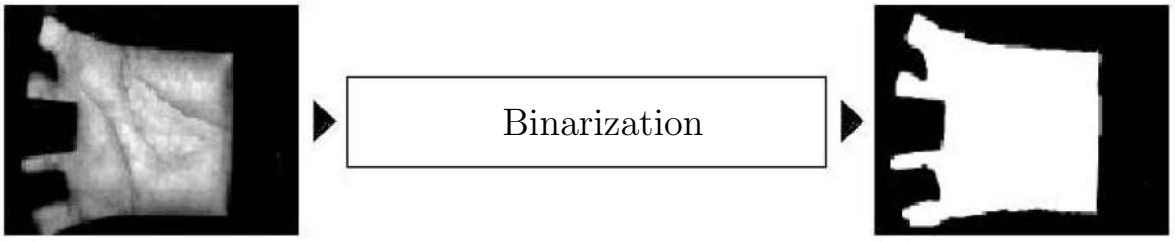


FIGURE A.2: Image binarization

Step3 : Edge Detection

The objective of this step performed using a classic square-tracing algorithm is to determine the hand edge. On binary images, the pixels are either black or white. In order to identify objects in a binary image, we need to locate the white pixels that are connected to each other. In other words, the related or neighboring pixels form an object on a binary image that must be successfully identified. In addition, in a square tiling, the pixel is in contact with 8 pixels. These pixels deny their neighborhood.

This type of connectivity is called Type 8 connectivity (see Figure A.3.(*a*)). In the case where the pixels are only bound by 4 pixels, the connectivity is of type 4 (see Figure A.3.(*b*)).

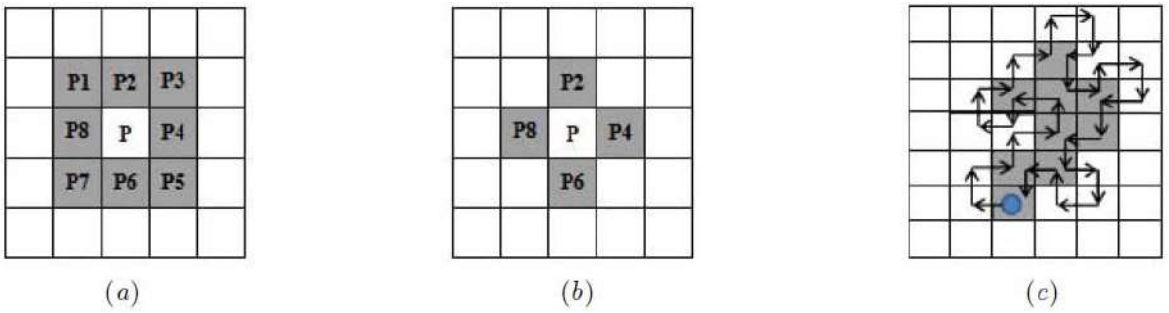


FIGURE A.3: Contour in a binary image. *(a)* type 8 connectivity, *(b)* type 4 connectivity, and *(c)* the algorithm application .

We consider in the image that the hand corresponds to a set of white pixels on a black pixel background. In other words, the pixels that interest us are white one (useful pixels) and the black pixels represent the background. We start from the bottom left of the image and we make columns scan from bottom to top, until we found a white pixel (pixel that interests us). This pixel is stored as the starting pixel. Once the starting pixel is detected, if we are on a useful pixel, then we turn to the left and if we are on a background pixel, we turn right. The algorithm stops once we fall back on the starting pixel. At each white pixel detection, this latter coordinates are stored in order to know the hand edge. The operation of this algorithm is shown in Figure A.3.(*c*). Figure A.4 shows the hand edge after the application of this algorithm.

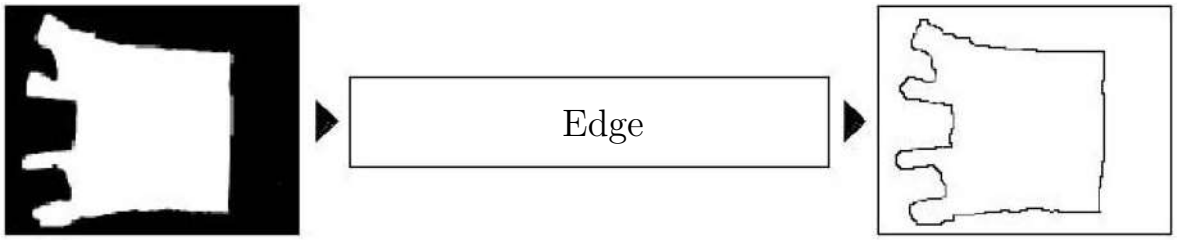


FIGURE A.4: Hand Edge.

◗ Step4 : Key points Detection

The characteristic points, represented by the fingertips and the valleys between the fingers, are calculated with the same edge tracking algorithm. These points coincide with the maxima and minima of the edge point abscissa. In addition, the fingers tips are initialized at the the lowest points abscissa of each finger, and the valleys at the largest points abscissa situated between the fingers. Palm window (ROI) is constructed according to a conventional models (generally square). Its location depends solely on the position of the $F1$ and $F2$ valleys, as well as the width of the palm. Figure A.5 shows the extraction result of the two points ($F1$ and $F2$).

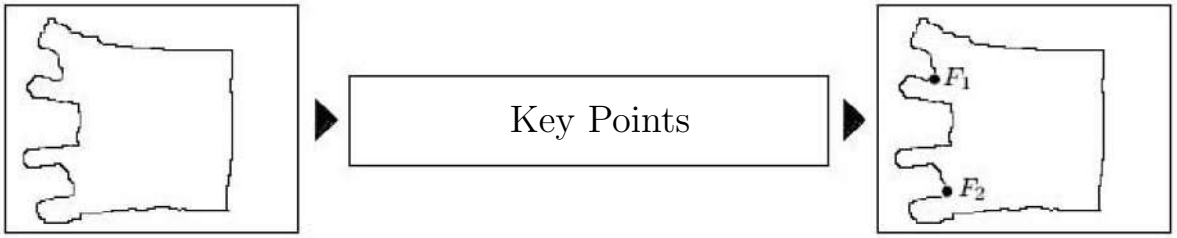


FIGURE A.5: Key Point localization.

Step5 : Image Rotation

With the extraction of these points, there is only one step left for the palm to be normalized: its rotation. The rotation angle was calculated according to the line drawn between the two points $F1$ and $F2$ and the ordinate axis. Once the angle θ is determined, we rotate the image by angle θ, in order to align the $F1$ and $F2$ axis with the ordinate axis of the image (see Figure A.6). In many studies, the rotation takes place before the definition of the window, and this makes it easier to locate the square. In fact, if the rotation is performed on the entire image, the edges of the extraction window are horizontal and vertical, the square (corresponds to the ROI) is therefore easy to locate.

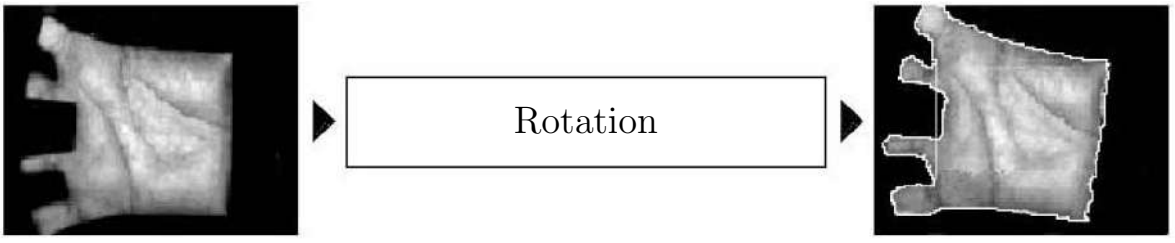


FIGURE A.6: Image Rotation.

Step6 : ROI Localization

The width of the study area (ROI), corresponds to the distance d between the reference segment $\overline{F1F2}$ and the palm square, is fixed at a few pixels (in our work, $d = 20$ pixels). The width of the square, W, is also fixed at a few pixels (in our work, $W = 128$ pixels). These two distances are set so that the ROI is centered on the hand. This (ROI) region is highlighted in the following diagram (see Figure A.7).

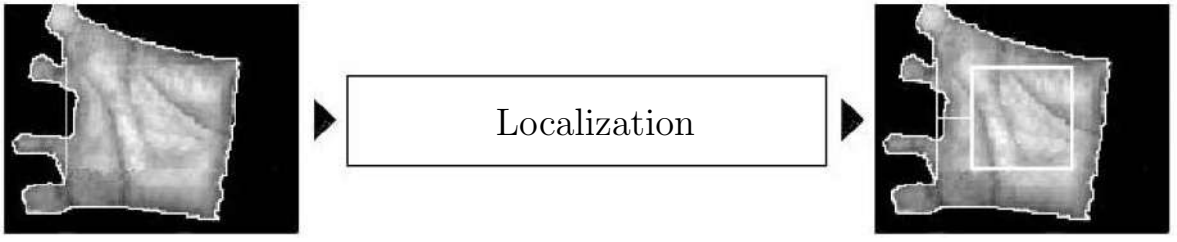


FIGURE A.7: Palmprint ROI localization.

Step7 : ROI Extraction

A square region, which corresponds to the ROI, has a fixed size (128×128 pixels), so that all the regions conform to the same dimension, are then extracted. Figure A.8 shows the obtained result after the ROI extraction operation.

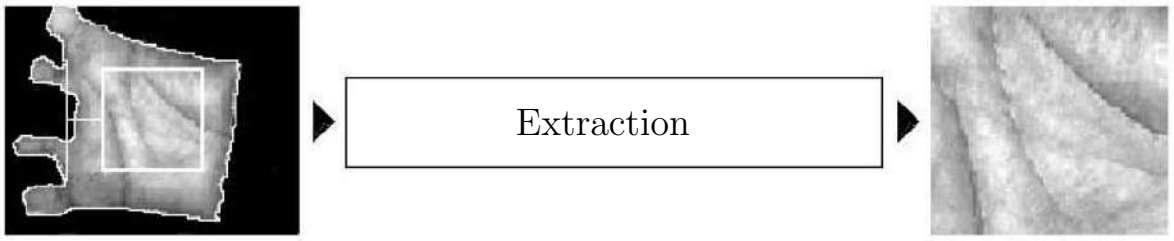


FIGURE A.8: Palmprint ROI Extraction.

A.3 Finger-Knuckle Print (FKP) ROI Extraction

The Finger-Knuckle print has also a unique features to each individual. It is invariable over time, easy to collect, digitize and store. After establishing the coordinate system, the central part (ROI) is segmented. In order to extract the region of interest (ROI) that contains the textures around the knuckle, we use the algorithm described in [122]. This operation aims to eliminate the background (image size reduction) and to have more accurate results.

Step1 : Filtering and Sub-sampling

The size of each image in the database is 768×576 pixels with a resolution of $400dpi$. It is not necessary to use this resolution for feature extraction (low resolution may well represent principal and secondary lines around the knuckle). Therefore, the finger image undergoes a filtering operation followed by a sub-sampling operation. The filtering operation purpose is to reduce the noise in the image. A low-pass filter (Gaussian filter) can be applied to reduce this noise and improve the original image quality. The sub-sampling operation allows to reduce the image resolution to $150dpi$. The advantage of this operation is to significantly reduce the computing cost by reducing the data amount. We note I_D the resulting image. The result of this step is shown in Figure A.9.

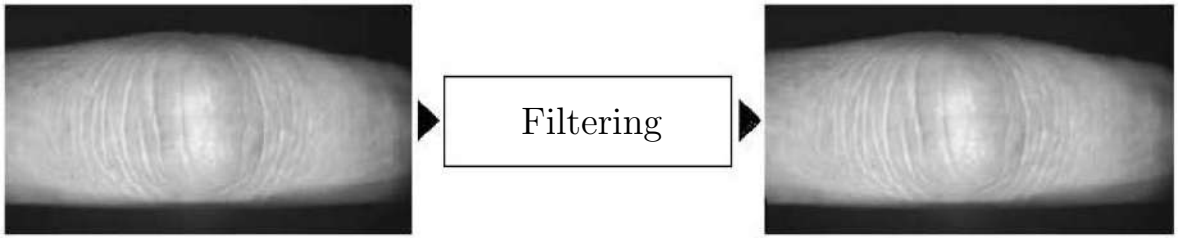


FIGURE A.9: Filtering and Sub-sampling of the image finger.

Step2 : X axis determination

Once the print image was filtered and sub-sampled, the algorithm determines the horizontal axis X. The finger lower limit can be easily extracted by a Canny edge detector type. Canny filter is used because of its advantages (good detection, good localization). In fact, this lower limit is almost consistent with all the images because all the fingers are put on the base block in the image acquisition. By adapting this boundary as a straight line, the X axis is determined. Figure A.10 shows the X axis in the finger lower boundary .

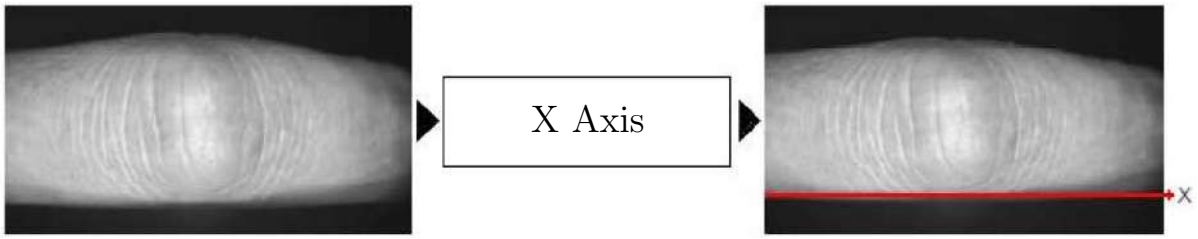


FIGURE A.10: X axis determination.

Step3 : Sub-image Extraction

The useful information that can be used for a biometric identification resides only in part of the finger image. Therefore, we first cut a sub-image, I_S, from the original image. The I_S left and right limits two values are empirically determined. The high and low limits are estimated according to the real fingers limit. Figure A.11 shows an example of a sub-image. This sub-image is used to calculate the Y axis.

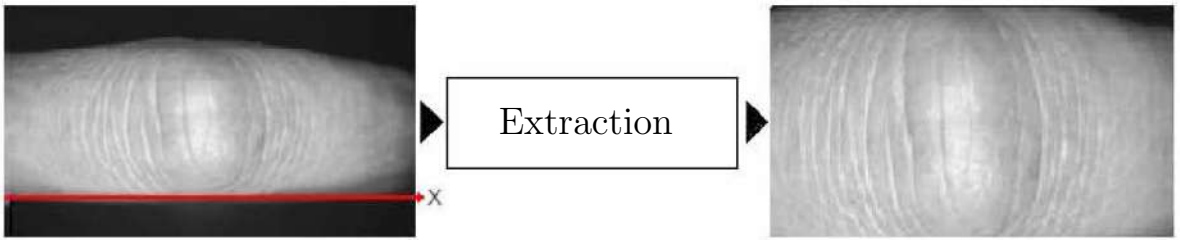


FIGURE A.11: The extracted sub-image before the ROI extraction.

Step4 : Edge Detection

By applying the Canny-type based edge detector to the I_S image, the edge image I_E can be obtained. See Figure A.12 for an example.

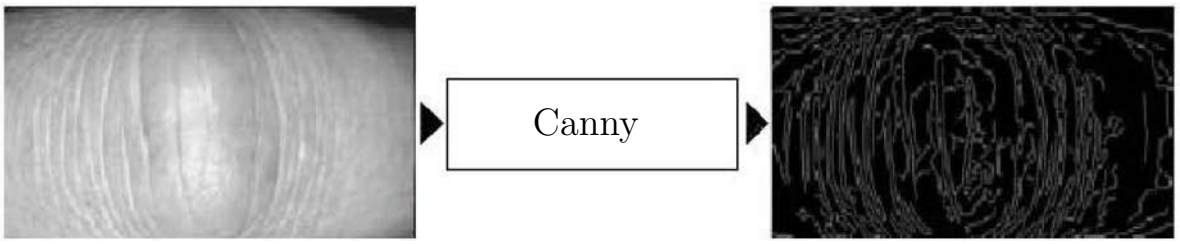


FIGURE A.12: The obtained Edge image.

Step5 : Coding convex directions

Based on the edge curves characteristics in the image, I_E, we can code I_E to obtain an encoded image, I_{CD}, which represents the curves convex directions. At this step, each pixel in I_E will therefore be designated by a code in order to represent the local (convex) direction of this pixel. Based on the finger images observation, we can represent an ideal curves model in the finger image as shown in Figure A.13.

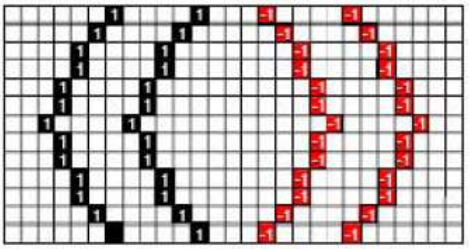


FIGURE A.13: Curves on the finger image.

In this model, a curve in the image is either convex to the left or convex to the right. We can code the pixels on the convex curves (to the left) by "1", the pixels on the convex curves (to the right) by "−1" and the other pixels (do not belong to these two curves) by "0". Figure A.14 shows the convex directions I_{CD}.

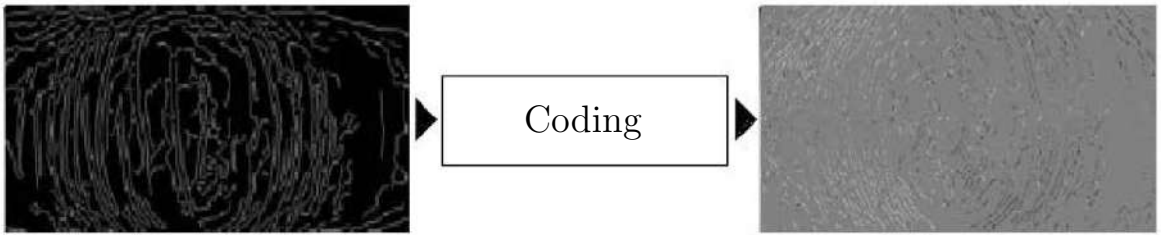


FIGURE A.14: Image obtained by the coding application of the convex direction..

Step6 : Y Axis Determination

For a finger image, most of the curves on the image left side are directed to the left and those on the right side are directed to the right. However, there are no obvious convex directions in a small area around the joint. From this observation, we can define a convexity magnitude, as follows:

$$\varrho(x) = (\sum_{W} I_{CD}) \tag{A.2}$$

where is x the horizontal position (represents a column) of the window. W is a symmetrical window with respect to the axis $X = x$. The window W is of size $d \times h$, with h equal to the image I_S height and d is chosen, in our work, equal to 35. The magnitude $\varrho(x)$ can reach its minimum around the Knuckle center. The window must make a path from the left and will scan the different x. The Y axis is defined as follows:

$$Y = arg\ min_x[\varrho(x)] \tag{A.3}$$

This position can be used to define the Y axis. Figure A.15 shows the position of the Y axis in the finger image.

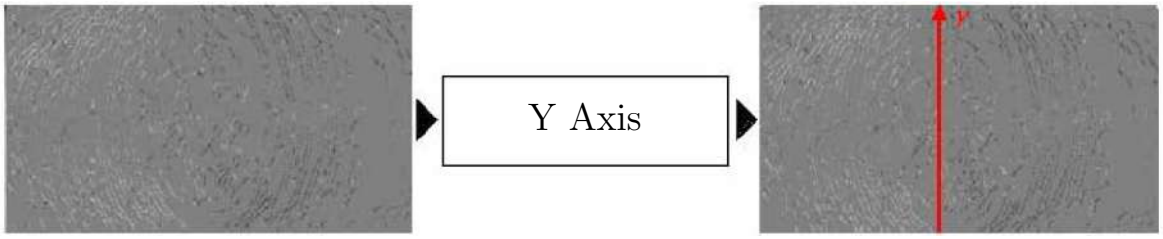


FIGURE A.15: Y Axis determination.

Step7 : ROI Localization

After locating the X and Y axes, we can determine an area in the I_D image, named I_{ROI}, that represents the region of interest. According to Figure A.16, the ROI, with a fixed size, can be extracted from the I_D image.

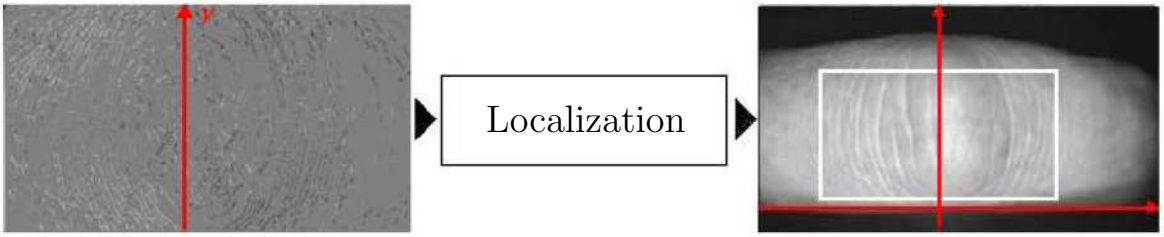


FIGURE A.16: ROI Localization in the finger image.

◗ Step8 : ROI Extraction

A finger-knuckle print region of interest is defined and cut around the Y axis (as shown in Figure A.17). A rectangular region, which corresponds to the ROI, with a fixed dimension (110×220 pixels) and containing the majority of the Knuckle, is then extracted.

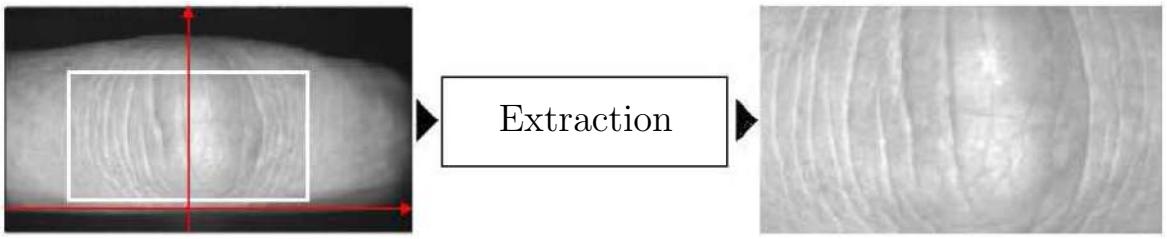


FIGURE A.17: ROI Extraction from the finger image.

Finally, we can see that the X and Y axes locating method, as well as the ROI extraction method, can effectively align the different fingers images , by normalizing the area that is the object of the various treatments for extract the finger biometric features. These operations considerably reduce the variations caused by the different finger poses in the acquisition system.

A.4 EAR Region Of Interest Extraction

One of the most challenging aspects of the 2D automated ear identification is related to the automated and accurate segmentation of ear or the region of interest that encloses discriminant gray level information. The human ear is highly curved 3D surface and therefore generates in uneven reflections which also generate shadows. Therefore the acquired images have uneven illumination, low contrast, and often surrounded by hairs and skin with varying pigmentation.

In order to localize the ROI area, the first step is to preprocess the ear images; we use the preprocessing technique described in [123] to align the ear images. In this technique, Gaussian filter which helps to suppress noise is used to smoothing the image, and then an histogram equalization is applied. The resulting image is used to automatically generate a binarized mask that can outline the surrounding region of interest. This step requires the binarization of image using Otsu's threshold. After that, the boundary tracing using Fourier descriptors of ear shape image is then employed to generate the ear shape boundary. The two key points on the located contour which achieve the maximum distance between them are selected as reference points on the reconstructed ear shape contour; these key points are used to align the ear ROI. Then, the image is rotated for normalized the ear ROI sub-image. Finally, the ROI part of the image, which is 180×50 pixels, is then cropped to represent the whole ear ROI sub-image. Figure A.18 shows the ear preprocessing steps.

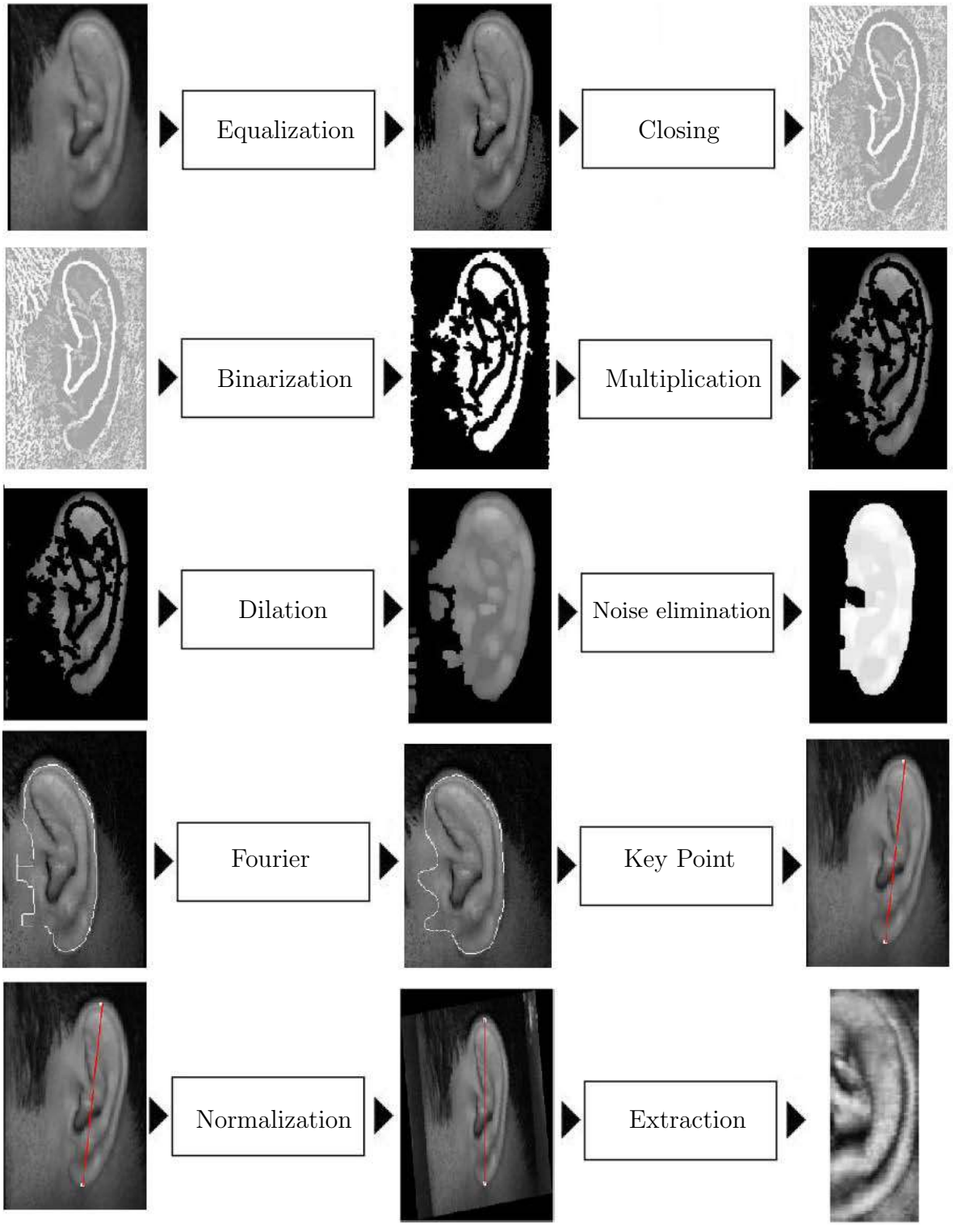


FIGURE A.18: Various steps in a typical EAR Region Of Interest (ROI) extraction algorithm.

Appendix B

Experimental Databases

B.1 The used databases description

THE development of a biometric identification or verification system involves the use of a database for the evaluation phase. In recent years, several public and free databases have been developed for the biometric recognition algorithms evaluation . one can cite, among others, the FERET database (*FacE REcognition Technology*) [124] and ORL (*Olivetti Research Laboratory*) [125] for faces, CASIA (*Chinese Academy of Sciences Institute of Automation*) [126] for iris and the multi-spectral palmprint, and other databases [127, 128]. These public databases have become a standards (such as, FERET, CASIA) which makes it possible to compare the recognition results of the developed algorithms with those of the existing algorithms. However, there are factors influencing the images of databases biometric modalities such as changes in lighting and poses. The variations in the biometric modalities are studied through the acquisition of several sessions with a definite interval of time. However, in these databases, we only have access to the output images of the various capture devices. The reality of real-environmental data acquisition can then be different.

The biometric recognition systems that have been implemented are based on palmprints (2D gray level, multi-spectral images) , Finger-Knuckle print (2D gray level) and the EAR modality (2D gray level). The images used in our experiments come from databases developed by the biometrics research center of the Polytechnic University of Hong Kong [129]. Our choice of these databases is justified by the fact that most of the works published in the literature have used these data bases for the evaluation of their results. In addition, these databases contain a large number of images for each person. Another reason is that the PolyU is the only organization that has made acquisitions of the Finger-Knuckle print images.

B.2 Palmprint database

① **Gray level palmprint (PolyU-PLM-2D):** the palmprint capture device , fig.B.1.(*b*) ,consists of a light source in the form of a ring, a CCD camera, a lens, an image acquisition card, and an analog-to-digital converter (ADC). To obtain a stable image print, a body and a blanket are used to form a semi-enclosed area, and the light source (the ring) provides a uniform illumination conditions

during the images capture operation. Six dowels on the platform serve as control points for setting up the user's hand. The ADC transmits the images captured by the CCD camera directly to a computer. Figure.B.1.(a) , shows the online palmprint capture device. The palmprint images can be obtained in two different sizes, 384×284 pixels and 768×568 pixels.

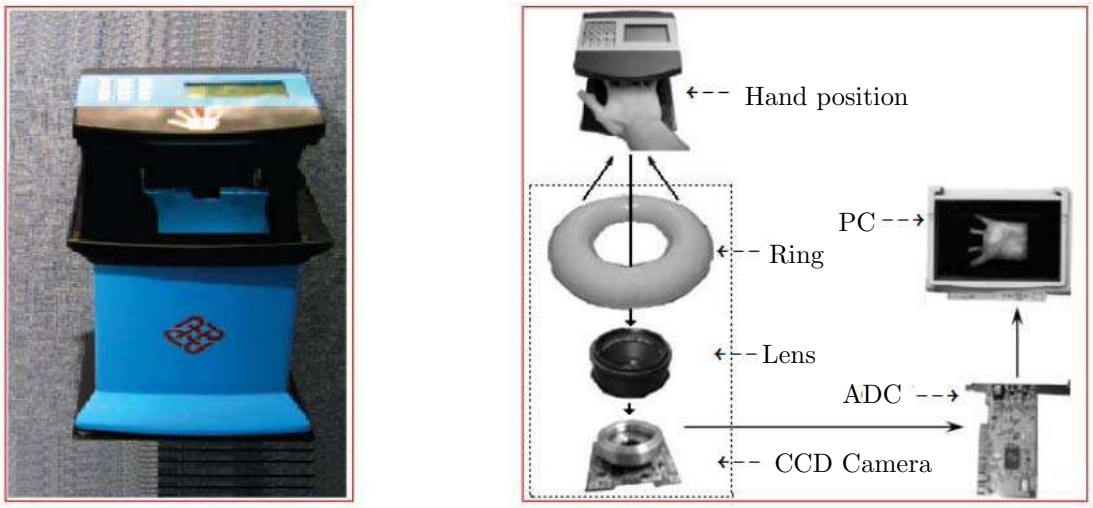


FIGURE B.1: 2D palmprint capture device developed by PolyU [29]. (a) acquisition device and (b) schematic diagram of the device.

Palmprint images of the 193 volunteers, among the PolyU students and staff, were taken by this device [130]. 131 persons ($\simeq 68\%$) are male. The age of the people is distributed as follows: about 86% are people under the age of 30, about 3% are people over the age of 50, and the remaining 11% are people between the ages of 30 and 50. The palmprint images are captured in two sessions, each session contains ten images for each palm, right and left, for a total of forty images per person, so the database contains a total of 7720 images of 386 different palms. These images contain variations in brightness, small variations in poses and a more judicious adjustment of the CCD camera focus so that the images obtained on the first and second sessions could be considered as being obtained by two different devices. The average time interval between the first and the second session is 69 days. Figure.B.2 shows an example of some samples from this database.

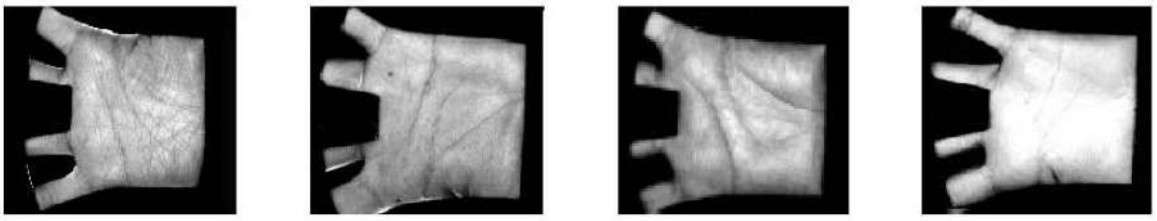


FIGURE B.2: Some sample images of the PolyU-PLM-2D database

② **Multi-spectral palmprint (PolyU-MSP):** The Near-InfraRed(NIR) region lies in a spectral window between the visible band and the mid-infrared band. The NIR light absorption in the spectral

window is low for water. In addition, the human tissue (skin, subcutaneous grease, etc.) is composed of 70% of water and the plasma which occupies 40% of the blood consists of 95% of water. As a result, the NIR light penetrates deep into the different layers of human tissue. This NIR light is then scattered or dispersed by the skin and subcutaneous grease and absorbed by the blood through hemoglobin. As a result, blood appears as a dark region, while skin and grease appear brighter. Thus, the NIR light can be exploited to study the layers of the skin. Which leads us to use this light for the extraction of the hand vein structure which represents itself a proper modality to each person.

The acquisition system that has been established by PolyU can capture multi-spectacles images in four spectral bands with the use of visible and NIR lights. For the visible spectrum, beams of light from a projector to a network of three monochrome LEDs illuminate the hand, the wavelengths of these three colors are $660nm$, $525nm$ and $470nm$ for, the RED, the GREEN and BLUE respectively. For the NIR spectrum, infrared LEDs with an $880nm$ wavelength could be placed as a row. Figure B.3.(a) shows the prototype multi-spectral capture device. It consists of a CCD camera, lens, an ADC, a multi-spectral light source, and a light controller. The acquisition device structure is shown in Figure. B.3.(b) . A CCD monochrome is placed at the bottom of the device. The ADC converter connects the CCD camera and the computer. The light controller device is used to control the multi-spectral light.

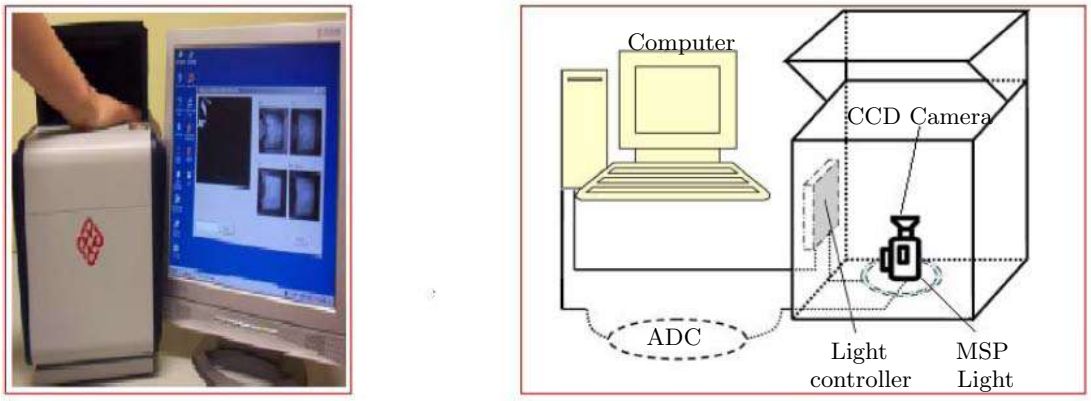


FIGURE B.3: Multispectral image acquisition device (MSP) developed by PolyU [131]. (a) Acquisition device and (b) schematic diagram of the device.

The system can capture the palmprint images with a resolution of 352×288 pixels or 704×576 pixels. A user, male or female, is invited to place his hand at a specific place (a platform) which can simplify the recognition task. Several dowels are placed on the platform to control exactly the hand placement. Four palmprint images are grouped under different spectral lights. The switching time between the two consecutive lights is very short, and the four images can be captured in a very short time ($< 1s$). In this system, the acquired palmprint vein structure in the NIR band is not clear enough because of the used CCD camera (To reduce costs, a standard television camera is used instead of a sensitive infrared camera). In addition, there is no infrared filter in front of the CCD camera because the infrared filter cuts the visible light.

The image database contains a 250 different people which is still represented by the students and staff of PolyU [117]. In this database, 195 people are male with an age range between 20 and 60 years. The image collection is made in two separate sessions. The interval time between the two sessions is 9 days. At each session and for each person, six images of each left and right hands were captured. Therefore, this image database contains 6000 images for each band from 500 different palms. At each shot, the system collects four images from four bands (Red, Green, Blue, and NIR). Figure B.4 shows a multi-spectral palmprint samples under the four spectral bands.

FIGURE B.4: Some sample images of the PolyU-PLM-MSP database

B.3 Finger-Knuckle Print (FKP) Database

The critical problem in data acquisition is to make the acquisition environment as stable as possible so that the variations on the collected images of the same person are reduced. Generally, a stable acquisition process can effectively reduce the complexity of the processing algorithms, which improves the recognition performance. To solve this problem of stability, a semi-closed acquisition environment is designed in this system.The data acquisition device is composed of a finger holder, a LED light source in a ring form, a lens, a CCD camera and an acquisition card. The image acquisition mechanism of this database is illustrated in Figure B.5.(a) .The LED light source and the CCD camera are placed in a closed box so that the lighting is constant. The box contains a finger holder to fix the position

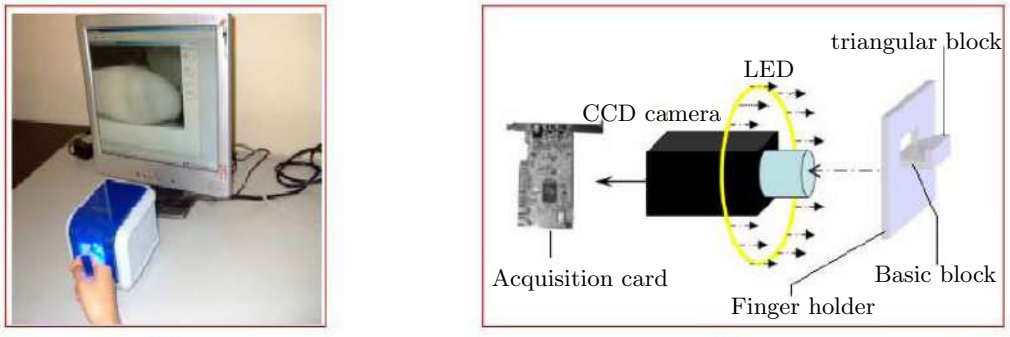


FIGURE B.5: FKP image acquisition device developed by PolyU [132]. (a) Acquisition device and (b) schematic diagram of the device.

of its articulation. This support has two blocks, basic block and triangular block, in order to reduce the finger spatial position variations in the different sessions. The obtained images size is 768×576 pixels with a resolution of $\simeq 400dpi$. Figure B.5.*(b)* shows the schematic diagram of this system (FKP acquisition device).

These database images [111] are captured using the device described above in PolyU. The PolyU-FKP database contains 165 people including 125 male. 143 people between the ages of 20 and 30 and the others between the ages of 30 and 50. Each finger images are captured in two sessions with an interval of 25 days between the two sessions. Six images of each finger were collected. Four fingers for each person are captured, namely, Left Index Finger (LIF), Right Index Finger(RIF), Left Middle Finger(LMF), and Right Middle Finger (RMF). As a result, 48 images of the four fingers are collected for each person. The final database collects a total of 7920 grayscale images of the fingers, left and right. Figure. B.6 shows some examples of images from this database.

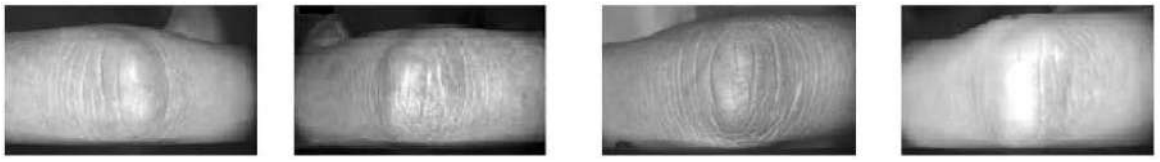


FIGURE B.6: Some sample images of the PolyU-FKP database

B.4 IIT Delhi Ear Database

Personal identification based on ear images has received increasing attention in the biometrics literature. Absence of any unified large scale publicly available ear database poses problem in the objective evaluation of ear identification approaches. Therefore the Biometrics Research Laboratory at IIT Delhi has been engaged in the collection of ear image database from the volunteers since October 2006. Their objective was to establish large scale collection of ear images and make this database available in the public domain to support research efforts in ear biometrics.

The IIT Delhi ear image database consists of the ear image database collected from the students and staff at IIT Delhi, New Delhi, India. This database has been acquired in IIT Delhi campus during Oct 2006 - Jun 2007 (still in progress) using a simple imaging setup. All the images are acquired from a distance (touchless) using simple imaging setup and the imaging is performed in the indoor environment. The currently available database is acquired from the 121 different subjects and each subject has at least three ear images. All the subjects in the database are in the age group $14 - 58$ years. The database of 471 images has been sequentially numbered for every user with an integer identification/number. The resolution of these images is 272×204 pixels and all these images are available in jpeg format. In addition to the original images, this database also provides the automatically normalized and cropped ear images of size 50×180 pixels. Recently, a larger version of ear database (automatically cropped and normalized) from 212 users with 754 ear images is also integrated and made available on request.

The acquired database is saved in the folder named 'raw' images. In addition, a new folder 'processed' is also made available. This folder contains automatically segmented and normalized images corresponding to raw images from 125 subjects. Each of the 50×180 pixel images is named as 'XXX-Y.bmp., where XXX represents user identification number and Y represents image sample number. Automatically segmented and normalized images from 221 subjects, which also includes the images from 125 subjects, are also available in this folder.

The sample images from the IIT Delhi ear database are reproduced in Figure.B.7

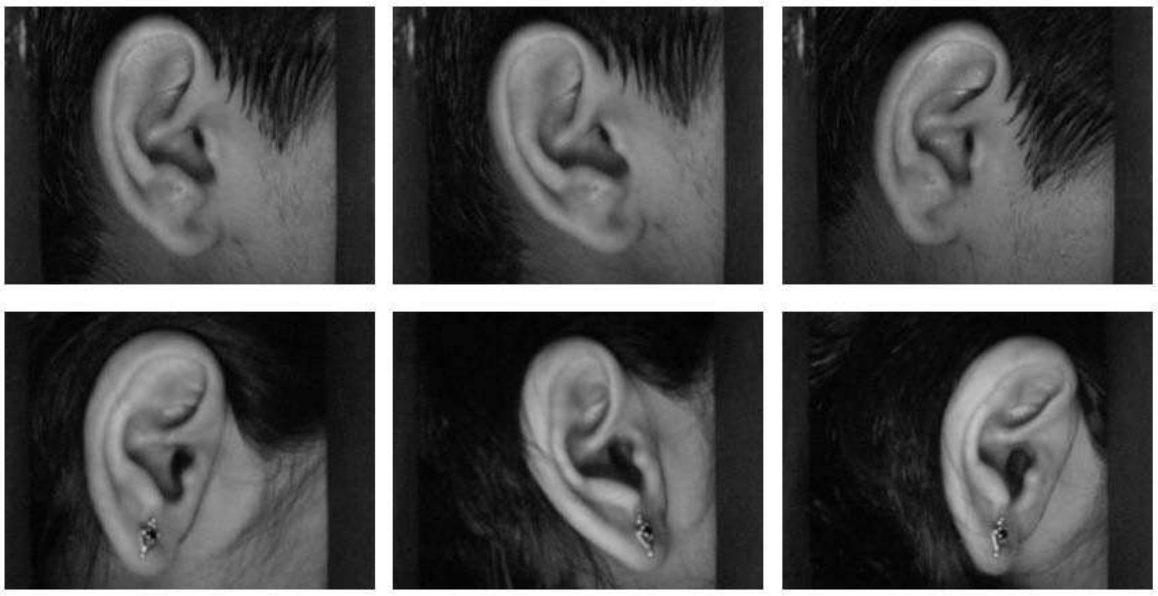


FIGURE B.7: Some sample images of the IIT Delhi EAR database

Appendix C

Matching and Normalization process

C.1 Introduction

REGARDING the general structure of the biometric system, it consist of a feature matching between the enrolled template the the query template to be recognized. The feature matching process plays an important role in biometric system development because the decision output of the system, accepting or rejecting a user's, is directly relies to results of the matcher or classifier. When it is desired to compare two feature vectors from the biometric system feature extraction module, one can either perform a similarity measure or a distance measure (divergence). However, for the fusion process, the matching scores output by the various sub-systems are heterogeneous; score normalization is needed to transform these scores into a common domain, prior to combining them.

In this part of thesis, we are attempting to present the different classifiers as well as the normalization techniques that are used during the conception of the biometric based identification system or even in Biometric-Crypto system construction. For that, numerous classier was proposed to performing the matching task. Among them, we choose to deploy the Hamming distance which can be considered a strength tools to compare between two binary templates. To compare between two histogram vector, we propose the use of the Chi-square distance. Another popular classifier is proposed for performing the matching task, that classifier is the Support Vector Machine (SVM). For the normalization process, the *Min-Max* is used for performing this task.

Bellow we give the mathematical description of the proposed classifiers for Features Matching

C.2 Feature Matching

Features matching or generally image matching, a part of many computer vision applications such as pattern and biometric based recognition system, is the task of establishing correspondences between

two images of the same persons. A common approach to image matching consists of detecting a set of interest points each associated with image descriptors from image data. Once the features and their descriptors have been extracted from two or more images, the next step is to establish some preliminary feature matches between these images.

The features matching between an input and a stored template consists of computing matching scores between them. Therefore, the score vector is given by: $\mathcal{D} = [d_1,\ d_2,\ d_3,\ d_4 \cdots d_N]$, where d_i denotes the i^{th} output value of the classifier provided by the test feature vector and N represents the size of the system database (the number of the enrolled persons). T compare the similarity of two vectors, we can use several techniques. Among them, the matching task in our experimental schemes based on Chi-square distance, Hamming distance and Euclidean distance.

C.2.1 Hamming Distance

When the matching task between two binary templates is needed, Hamming distance [133] becomes a powerful solution for performing this task. It is defined as the number of places where two templates differ. The Hamming distance ($\mathcal{D}_h$) can be defined as:

$$\mathcal{D}_h = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \mathcal{V}_X^t(i,j) \oplus \mathcal{V}_X^r(i,j) \tag{C.1}$$

where $\mathcal{V}_X^t$ and $\mathcal{V}_X^r$ are the test (input) and stored templates. The $\oplus$ is the Boolean operator (XOR) and $N \times N$ is the size of the templates. It is noted that $\mathcal{D}_h$ is between 1 and 0. For perfect matching, the matching score is zero.

C.2.2 Euclidean Distance

Among all the image metrics, Euclidean distance is the most commonly used due to its simplicity, The Euclidean distance $d_E(x,y)$ is given by:

$$\mathcal{D}_E^2(x,y) = \sum_{k=1}^{MN} (x^k - y^k)^2 \tag{C.2}$$

where (x,y) are two $M \times N$ images defined by:

$$x = \begin{bmatrix} x^1 & x^2 & \cdots & x^{MN} \end{bmatrix}, y = \begin{bmatrix} y^1 & y^2 & \cdots & y^{MN} \end{bmatrix}$$

C.2.3 Chi-Square distance

In some cases, the output of the feature extraction descriptor is a histogram. So, in this case, it will be better to use a classifier designed fo histograms matching. Chi square statistic is a successful

metric that can be used for histogram comparison. It can be defined as fellows:

$$\chi^2 = \sum_i \frac{(x_1 - y_i)^2}{x_i + y_i} \tag{C.3}$$

where x, y are two histogram feature vector, i is the number of histogram bins. We use this form of Chi-square to be able to interpret it as a distance where 0 value means the identical histograms.

C.3 Normalization process

The matching scores output are heterogeneous; score normalization is needed to transform these scores into a common domain, prior to combining them. Indeed, the scores from each system may be different in nature. Some systems produce similarity scores(the higher the score, the more the reference looks like the test, so the user is a genuine),others produce distances(the lower the distance,the more the reference looks like the test, so the user is a genuine). Moreover, each system can have different scores variations intervals, as an example for a system the scores vary between 0 and 1 and for another the scores vary between 0 and 1000. This is make us understand the need of scores normalizing. The scores normalizations methods presented in the following, deal with scores that all vary in the same direction (in general we consider all scores as similarity). To transform distances into similarity there are two solutions: the inverse or the opposite. In the following, we will consider that all the fused scores have been transformed into similarity scores. Numerous normalization technique have been proposed in the literature, among them one can cite:

- Min-Max normalization method.
- Quadratic-line-Quadratic (QLQ) normalization method.
- Z-score normalization technique.
- Hyperbolic tangent (HTan) normalization method.
- double sigmoid normalization method.

Among all the existed normalization techniques, the *min-max* method [134] is chosen for performing the normalization. *Min-max* normalization is often known as feature scaling where the values of a numeric range of a feature of data, i.e. a property, are reduced to a scale between 0 and 1. Therefore, in order to calculate $\widetilde{\mathcal{D}}$, i.e. the normalized value of a member of the set of observed values of $\mathcal{D}$, we must employ the following formula:

$$\widetilde{\mathcal{D}} = \left[\frac{\mathcal{D} - min(\mathcal{D})}{max(\mathcal{D}) - min(\mathcal{D})}\right] \tag{C.4}$$

where $\widetilde{\mathcal{D}}$ represents the normalized scores vector. It can be easily seen that when $\mathcal{D} = min(\mathcal{D})$, then $\widetilde{\mathcal{D}} = 0$, and When $\mathcal{D} = max(\mathcal{D})$, then $\widetilde{\mathcal{D}} = 1$. This means, the minimum value in $\mathcal{D}$ is mapped to 0 and the maximum value in $\mathcal{D}$ is mapped to 1. So, the entire range of values of $\mathcal{D}$ from min to max are mapped to the range 0 to 1.

Appendix D

Data Classifiers

In machine learning and statistics, classification is a supervised learning approach in which the computer program learns from the data input given to it and then uses this learning to classify new observation. This data set may simply be bi-class (like identifying whether the person gender is male or female or that the person is a genuine or an impostor) or it may be multi-class too. Some examples of classification problems are: biometric identification like palmprint recognition, handwriting recognition or even document classification etc.

Literally, numerous algorithms was proposed in order to perform the classification task, one can cite : Support Vector Machines(SVM), Decision Trees, Random Forest, Nearest Neighbor,... and etc. Moreover, two classification algorithms were used in the context of this thesis which are the Support Vector Machine (SVM) and the K-Nearest Neighbor. This appendix will give give a brief overview concerning those two classification algorithms.

D.1 Support Vector Machine (SVM)- A brief overview

There are multiple ways to classify data with machine learning. Support Vector Machines (SVMs) [135] are new learning machines and they are receiving increasing attention and have shown superior performance in pattern recognition. The SVM is firstly proposed by Vladimir Vapnik and Alexey Chervonenkis in 1963. Vapnik refined this classification method in the 1990's and extended uses for SVMs. Support vector machines have become a great tool for the data scientist.

Theoretically[136], Support vector machines attempt to pass a linearly separable hyperplane through a dataset in order to classify the data into two groups. This hyperplane is a linear separator for any dimension; it could be a line (2D), plane (3D), and hyperplane (4D+). An example of separation hyperplane is illustrated in Figure D.1

We can separate the red and blue objects with an infinite number of hyperplanes. Which hyperplane is the best? Well, the best hyperplane is the one that maximizes the margin. The margin is the distance between the hyperplane and a few close points. These close points are the support vectors

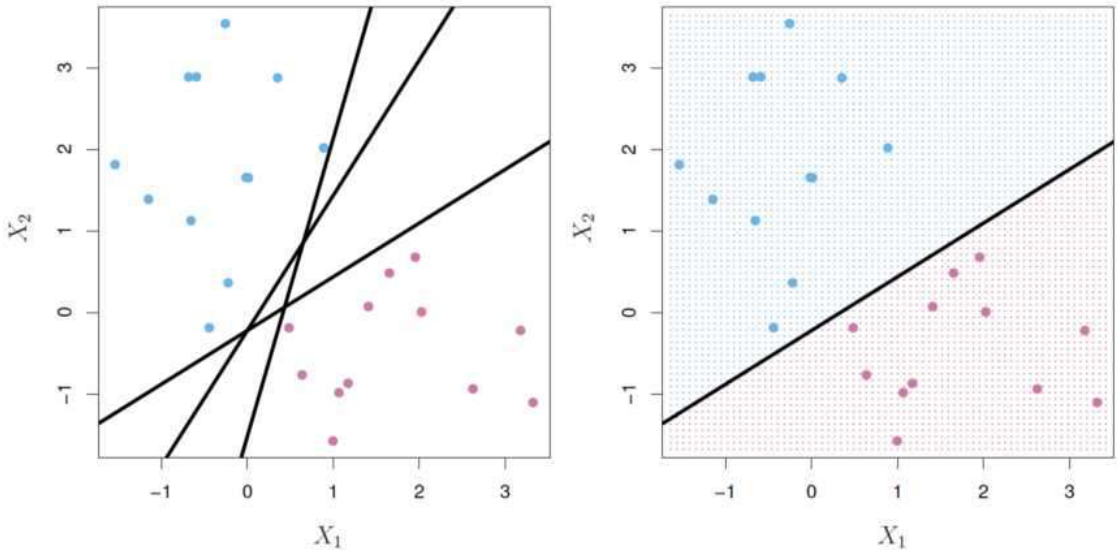


FIGURE D.1: Separating Hyperplane

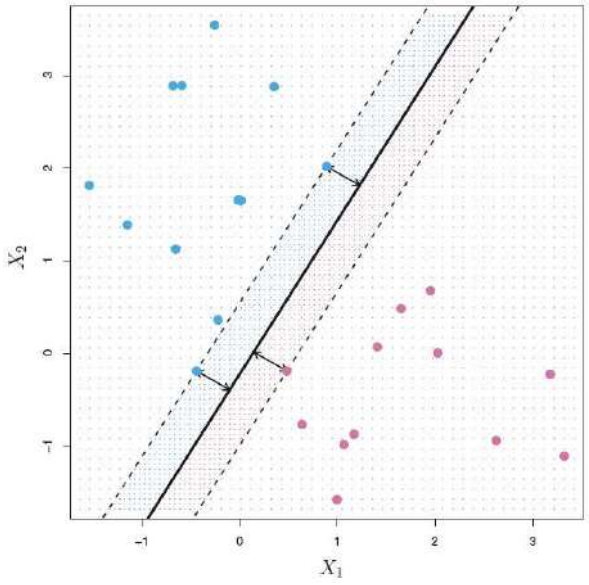


FIGURE D.2: Best Hyperplane Separating

because they control the hyperplane. The graph below (Figure D.2) illustrates the best hyperplane for the red and blue objects.

This is the Maximum Margin Classifier. It maximizes the margin of the hyperplane. This is the best hyperplane because it reduces the generalization error the most. If we add new data, the Maximum Margin Classifier is the best hyperplane to correctly classify the new data. The Maximum Margin Classifier is the first SVM. But this SVM requires the two classes to be completely linearly separated. This isn't always the case so in 1993 Vapnik developed another one of his machines.

Figure D.3 shows data that is not perfectly separable.

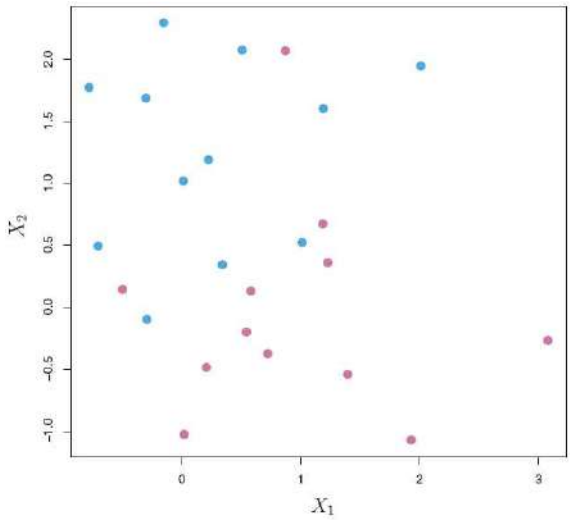


FIGURE D.3: Case of no separately data

In this case, the Maximum Margin Classifier would not work. Vapnik developed a soft margin that would allow for some misclassification of data. This is known as a Soft Margin Classifier or a Support Vector Classifier. It also attempts to maximize the margin separating the two classes. The Figure D.4 illustrates this SVM.

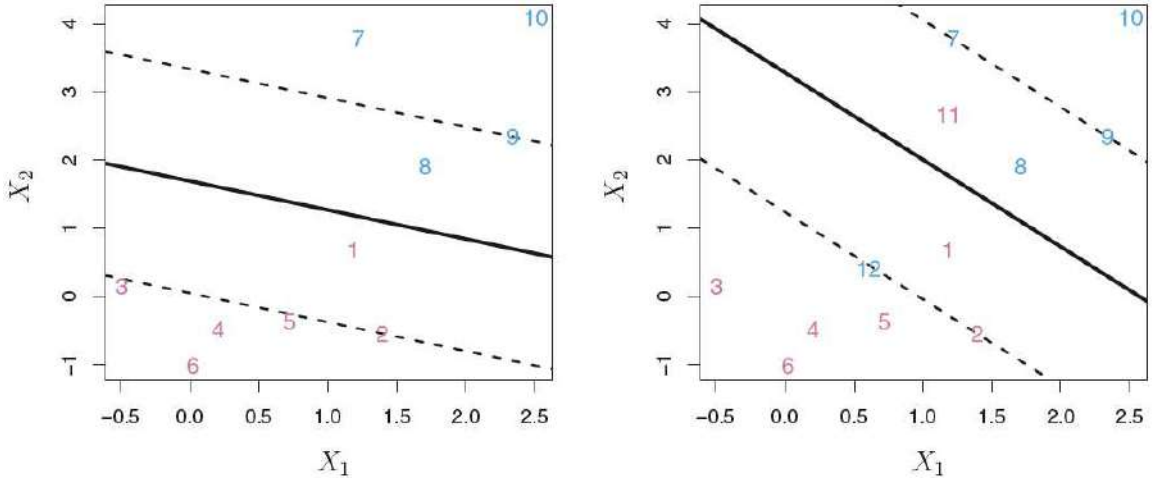


FIGURE D.4: Support Vector Classifier

The support vector classifier contains a tuning parameter in order to control how much misclassification it will allow. This tuning parameter is important when looking to minimize error. As with all supervised learning, there is a bias-variance trade-off. When the tuning parameter (often denoted as C) is small, the classifier allows only a small bit of misclassification. The support vector classifier will have low bias but may not generalize well and have high variance. We may overfit the training data if the tuning parameter is too small. If C is large, the number of misclassification allowed has been increased. This classifier would generalize better but may have a high amount of bias. When

the tuning parameter is zero, there can be no misclassification and we have the maximum margin classifier.

The support vector classifier can fail if the data is not linearly separable. In 1992, Vapnik developed a method of handling non-linearly separable classes. This method uses the kernel trick. Kernels are functions that quantify similarities between observations. Common types of kernels used to separate non-linear data are polynomial kernels, radial basis kernels, and linear kernels (which are the same as support vector classifiers). Simply, these kernels transform the data in order to pass a linear hyperplane and thus classify data.

Extensions of support vector machines can be used to solve a variety of other problems. We can have multiple class SVMs using One-Versus-One Classification or One-Versus-All Classification. A brief description of these can be found in [132].

D.2 K-Nearest Neighbors (KNN)

The K-Nearest Neighbors (KNN) algorithm [137] is a simple, easy-to-implement supervised machine learning algorithm that can be used to solve classification problems. The main idea of the KNN algorithm comes from assuming that similar things exist in close proximity. In other words, similar things are near to each other.

KNN is a nonparametric lazy learning algorithm. When you say a technique is nonparametric, it means that it does not make any assumptions on the underlying data distribution, as, in the real world, most of the practical data does not obey the typical theoretical assumptions made.

It is also a lazy algorithm. What this means is that it does not use the training data points to do any generalization. In other words, there is no explicit training phase or it is very minimal. This means the training phase is pretty fast. Lack of generalization means that KNN keeps all the training data. More exactly, all the training data is needed during the testing phase. This is in contrast to other techniques like SVM where you can discard all nonsupport vectors without any problem. Most of the lazy algorithms, especially KNN, make a decision based on the entire training data set.

For KNN classification, an input is classified by a majority vote of its neighbors. That is, the algorithm obtains the class membership of its k neighbors and outputs the class that represents a majority of the k neighbors. To understand how the classification KNN functioning, let's introduce this example:

Suppose we are trying to classify the green rectangle. It needs to be classified into red five-point star or blue triangle. Let us begin with $k = 5$ (the dotted line). In this case, the algorithm would return a blue triangle, since it constitutes a majority of the 5 neighbors. Likewise, with $k = 10$ (the solid line), the algorithm would return a red five-point star(see Figure D.5).

If no majority is reached with the k neighbors, many courses of action can be taken. For example, one could use a plurality system or even use a different algorithm to determine the membership of that data point.

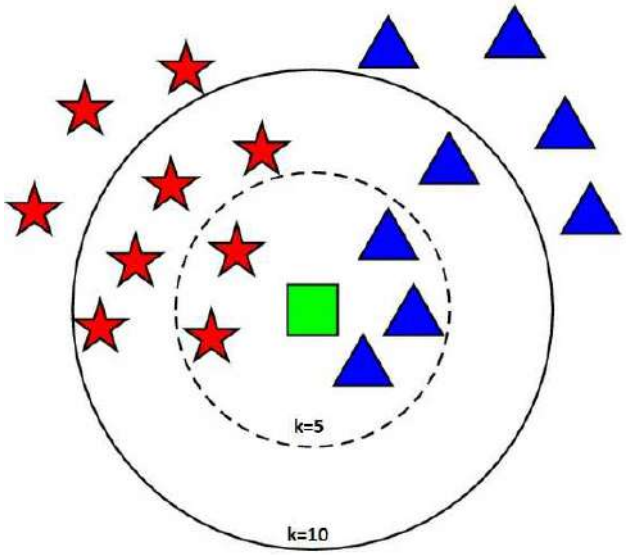


FIGURE D.5: An example of KNN classification

Determining a neighbor can be performed using many different notions of distance, with the most common being Euclidean and Hamming distance.

The special case where the class is predicted to be the class of the closest training sample (i.e. when $k = 1$) is called the nearest neighbor algorithm or minimal distance classifier (1-Nearest Neighbor). The one nearest neighbor (1-NN) is the most intuitive nearest neighbor type classifier that assigns a point x to the class of its closest neighbor in the feature space. Using 1-NN classifier for performing the classification task becomes like classification based distances (like euclidean distance, hamming distance and ...etc).

Appendix E

Personal Contributions

E.1 Publications

1. Korichi M, Meraoumia A, AIADI KE,"Improved Biometric Identification System Using a New Scheme of 3D Local Binary Pattern, " *In: International journal of information and communication technology, inderscience publisher*,2017.
2. Chlaoua R, Meraoumia A, Aiadi KE, Korichi M, "deep learning for finger knuckle print identification system based on PCANet and SVM classifier", *In: EVOLVING system, Springer*, 2018.

E.2 International Communications indexed in the IEEE xplore database

1. A.Meraoumia, M.Korichi, S.Chitroub, and A.Bouridane, "Finger-Knuckle-Print identification based on histogram of oriented gradients and SVM classifier," *In: International Conference on New Technologies of Information and Communication, NTIC'15*, Mila, Algeria, 2015.
2. A.Meraoumia, M.Korichi, S.Chitroub, and A.Bouridane, "Hidden Markov models & principal component analysis for multispectral palmprint identification," *In:* 5^{th} *International Conference on Information and Communication Technology Access, ICTA'15*, Morocco, 2015.
3. R. Chlaoua, A. Meraoumia, M. Korichi, and K. Aiadi, , " Visible spectrum bands of palmprint image for a robust biometric identification system," *In:* 2^{nd} *International Conference on Information Technology for Organization Development, IT4OD'16*, Fez,Morocco, 2016.
4. A. Meraoumia, M.Korichi, H.Bendjenna, and S.Chitroub, " Multispectral palmprint identification method using rotation invariant variance measures," *In:* 2^{nd} *International Conference on Information Technology for Organization Development, IT4OD'16*,Fez,Morocco, 2016.
5. M. Chaa, N. E. Boukezzoula, A. Meraoumia, and M. Korichi, " An efficient biometric based personal authentication system using Finger Knuckle Prints features," *In:* 2^{nd} *International*

Conference on Information Technology for Organization Development, IT4OD'16,Fez,Morocco, 2016.

6. M. korichi, Meraoumia A, Aiadi KE,"A small look at the ear recognition process using a Binarized Statistical Image Features (ML-BSIF)," *In: The* 3^{rd} *IEEE International Conference on Pattern Analysis and Intelligent Systems,PAIS'18*, Tebessa, Algeria,2018.

7. M. Korichi, A. Meraoumia, M. Saigaa and H. Bendjenna,"Securing Person Identification by Combining Hand Biometric Modalities",*In: The* 4^{th} *IEEE International Conference on Signal, Image, Vision and their Applications,SIVA'18*, Guelma, Algeria,2018.

E.3 International Communications with international reading committees

1. M. Korichi, A. Meraoumia, S. Chitroub, and A. K. Eddine, "Palmprint Features Selection," *In: The* 1^{st} *International Conference on Automatic, Telecommunication and Signals, ICATS'15*, Annaba, Algeria, 2015.

2. M. Korichi, A. Meraoumia, S. Chitroub, and A. K. Eddine, "An automated ear identification system using Gabor filter responses," *In International Symposium on Complex Systems and Intelligent Computing , CompSIC'15*, Souk Ahrass, Algeria, 2015.

3. M.Korichi, A.Meraoumia,H.Bendjenna, K.E.Aiadi, K.Bensid, "Enhancing the Privacy Technologies by Using the Finger-Knuckle-Print Features," *In: The* 2^{nd} *International Conference on Pattern Analysis and Intelligent Systems, PAIS'16*, Khenchla, Algeria, 2016.

4. A.Meraoumia, M.Korichi,R. Chlaoua, H.Bendjenna,"Can Handwriting Style Help Strengthen the Person Identity¿," *In: The* 2^{nd} *International Conference on Artificial Intelligence and Information Technology, ICAIIT'19*, Ouargla, Algeria, 2019.

5. K. Ben Sid, D. Samai, F. Z. Laalem, A. Tidjani, and M. Korichi, "Multimodal Palmprint Biometric System Using New Variant Of Local Phase Quantization and Support Vector Machine methods,"*In: The* 2^{nd} *International Conference on Pattern Analysis and Intelligent Systems, PAIS'16*, Khenchla, Algeria, 2016.

6. Rachid Chlaoua, Abdallah Meraoumia, Kamal Eddine Aiadi and Maarouf Korichi,"Hyperspectral Vs Multispectral Palmprint Recognition using Random Forest Tree,"*In:* 10^{th} *Conference on electrical engineering ,CGE'10*, EMP, Algeria, 2017.

Bibliography

[1] Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi and Yong-Haur Tay,"Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *In: Pattern Recognition,* Vol. 56, pp. 50-62,2016.

[2] F. Perronnin, J-L. Dugelay, "Introduction à la Biométrie : Authentification des Individus par Traitement Audio-Vidéo ," *In: Traitement du Signal*, Vol 19, N4, pp. 253-265, 2002.

[3] T. Rajani Devi "Importance of Cryptography in Network Security," *In:International Conference on Communication Systems and Network Technologies*, Gwalior, India,2013.

[4] F. Chafia, C. Salim and B. Farid, "A biometric crypto-system for authentication," *In: International Conference on Machine and Web Intelligence (ICMWI)*, pp. 434 ? 438, Algiers, Algeria,2010.

[5] Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," *In: IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081-1088, 2006.

[6] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance,"*In: IEEE Trans.Inf. Forensics Security*,vol. 2, no. 4, pp. 744-757, 2007.

[7] Sasa Adamovic, Milan Milosavljevic, Mladen Veinovic, Marko Sarac, Aleksandar Jevremovic, "Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics," *In: IET Biometrics*, Vol. 6, No. 2, pp. 89-96, 2017.

[8] Gandhimathi Amirthalingam, G.Radhamani,"New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization," *In: Journal of King Saud University Computer and Information Sciences*, Vol. 28, No. 4, pp. 381-394,2016.

[9] A. Jagadeesan, K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," *In: International Journal of Computer Science and Information Security*,vol. 7, no. 2, pp.28-37, February 2010.

[10] Christian Rathgeb and Andreas Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *In: EURASIP Journal on Information Security*, 2011:3,2011.

[11] M. El-abed, "Évaluation du systémes biometriques",Thése Doctorat,Université de CAEN/BASSE-NORMANDIE,France,2011.

[12] W. A. Ahmad, S. M. Ali, B. Adnan, "Applications As Access Control Tools of Information Security," *Int. J. Innov. Comput. Inf. Control*, vol. 8, no. 11, pp. 7983-7999, 2012.

[13] K. Ben Sid, D. Samai, F. Z. Laalem, A. Tidjani, and M. Korichi, "Multimodal Palmprint Biometric System Using New Variant Of Local Phase Quantization and Support Vector Machine methods,", *2nd International Conference on Pattern Analysis and Intelligent Systems,*,Kenchla,Algeria, pp. 1-6,2016.

[14] M.Korichi, A.Meraoumia,H.Bendjenna, K.E.Aiadi, K.Bensid, "Enhancing the Privacy Technologies by Using the Finger-Knuckle-Print Features," , *2nd International Conference on Pattern Analysis and Intelligent Systems,*,Kenchla,Algeria, pp. 1-6,2016.

[15] A. Kumar and D. Zhang, "Improving biometric authentication performance from the user quality," *IEEE Trans. Instrum. Meas.,* vol. 59, no. 3, pp. 730-735, 2010.

[16] A. Meraoumia, M. Korichi, H. Bendjenna, and S. Chitroub, "Multispectral palmprint identification method using rotation invariant variance measures," *2nd International Conference on Information Technology for Organization Development*,Fez,Moroco, pp. 1-6, 2016.

[17] R. Chlaoua, A. Meraoumia, M. Korichi, and K. Aiadi, "Visible spectrum bands of palmprint image for a robust biometric identification system," *2nd International Conference on Information Technology for Organization Development*,Fez,Moroco, pp. 1-4, 2016.

[18] Abdallah Meraoumia,"Modèle de Markov caché appliqué à la multi-biométrie",Thése Doctorat,Université de DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOMEDIENNE (USTHB),Algeria,2014.

[19] A. Meraoumia, M. Korichi, S. Chitroub, and A. Bouridane, "Finger-Knuckle-Print identification based on histogram of oriented gradients and SVM classifier," *1st Int. IEEE Conf. New Technol. Inf. Commun.* NTIC 2015.

[20] Anis CHAARI,"Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée,"Thése Doctorat,Université de la Manouba,Tunisia,2009.

[21] Nicolas MORIZET,"Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris,"Thése Doctorat,École Doctorale d'Informatique,Télécommunications et Électronique de Paris,France,2009.

[22] Frédéric MASSICOTTE,"LA BIOMÉTRIE, SA FIABILITÉ ET SES IMPACTS SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE",Thése Doctorat,Université Du QUÉBEC à MONTRÉAL,Canada,2007.

[23] D.Bala , "Biometrics and Information Security,"*Proceedings of the 5th annual conference on Information security curriculum development*, Kennesaw, Georgia, ISBN:978-1-60558-333-4, pp 64-66,2008.

[24] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric Recognition: Security and Privacy Concerns,"*IEEE Security & Privacy,*Vol 99, Issu 2,2003.

[25] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. "Biometric authentication, "*Encyclopedia of Information Science and Technology*, pages 346-354, 2008.

[26] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition 1," *IEEE Trans. Circuits Syst. Video Technol*, vol. 14, no. 1, pp. 4-20, 2004.

[27] Matos H., Oliveira H.P., Magalhães F., "Hand-Geometry Based Recognition System," *In: Campilho A., Kamel M. (eds) Image Analysis and Recognition. ICIAR 2012. Lecture Notes in Computer Science*, vol 7325. *Springer*, Berlin, Heidelberg,2012.

[28] Lin Zhang,Lei Zhang;David Zhang,"Finger-knuckle-print: A new biometric identifier," *16th IEEE International Conference onImage Processing (ICIP)*,Cairo, Egypt,2009.

[29] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol. 25, no. 9, pp. 1041-1050, 2003.

[30] G.Betta; D.Capriglione ;M.Corvino ;C.Liguori ; A.Paolillo.,"Face Based Recognition Algorithms: A First Step Toward a Metrological Characterization," *IEEE Transactions on Instrumentation and Measurement*, Vol 62 Issue 5,pp 1008-1016,2013.

[31] N.Sinha; A.Joshi; A.Gangwar; A.Bhise; Z.Saquib,"Iris segmentation using deep neural networks,"2^{nd} *International Conference for Convergence in Technology (I2CT)*,Mumbai, India,2017.

[32] Lajevardi, S.M. ; Arakala, A. ; Davis, S.A. , Horadam, K.J. , "Retina Verification System Based on Biometric Graph Matching", *IEEE Transactions onImage Processing*, Vol. 22, No. 9, pp. 3625-3635, 2013

[33] L. Yuan, Z. Mu, and Z. Xu, "Using ear biometrics for personal recognition," *Adv. Biometric Pers. Authentication*, vol. 3781, pp. 221-228, 2005.

[34] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *Journal of Information Security and Applications*, vol. 37, pp. 28-37, 2017.

[35] Yu D., Deng L. "Deep Neural Network-Hidden Markov Model Hybrid Systems." *In: Automatic Speech Recognition. Signals and Communication Technology*, Springer, London,2015.

[36] A. Karouni, B. Daya, and S. Bahlak, "Offline signature recognition using neural networks approach," *Procedia Computer Science*, vol. 3, pp. 155-161,2011.

[37] A. Ahmed; Issa Traore."Biometric Recognition Based on Free-Text Keystroke Dynamics," *IEEE Transactions on Cybernetics*, Vol 44, Issue 4,pp. 458 - 472, 2014.

[38] I.Buciu, A.Gacsadi,"Biometrics systems and technologies: A survey," *International Journal of Computers, Communications and Control*, pp. 315-330, 2016.

[39] Butler, J.M., Shen, Y., McCord, B.R, "The development of reduced size STR amplicons as tools for analysis of degraded DNA",*Journal of Forensic Sciences*, Vol. 48, No. 5, pp. 1054-1064, 2003.

[40] D.Abhijit; P.Umapada; A. Miguel,F.Ballester ; M.Blumenstein,"A new wrist vein biometric system," *IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)*,Orlando, FL, USA, 2014.

[41] Khan, M.M.Ward, R.D. Ingleby, M,"Automated Classification and Recognition of Facial Expressions Using Infrared Thermal Imaging," *IEEE Conference on Cybernetics and Intelligent Systems*, Singapore, pp. 202-206, Dec. 2004.

[42] A.K.Jain, A.Ross. "Information fusion in biometrics," *Pattern Recognition Letters*, Vol. 24, pp. 2115–2125, 2003.

[43] Igor Bohm, Florian Testor, "Biometric Systems". *In paper for biometrics Department of Telecooperation University of Linz 4040 Linz*, Austria.

[44] J.L. Wayman,"Digital signal processing in biometric identification: a review," *in Proceeding of International Conference on Image Processing.*,Rochester, NY, USA, USA,2002.

[45] Al-Waisy, A.S., Qahwaji, R., Ipson, S. et al."A multi-biometric iris recognition system based on a deep learning approach," *Pattern Analysis and Applications*,Springer,pp 1-20, 2017.

[46] . Golfarelli M, Maio D, Malton D " On the error-reject trade-of in biometric verifcation systems". *IEEE Trans Pattern Anal Mach Intell* 19(7):786-796,1997.

[47] A. Ross, and A. K. Jain, "Biometric Fusion: Does Modeling Correlation Really Matter? ", *The 3rd Int'l Conf. on Biometrics: Theory, Applications and Systems*, Washington DC, Sept. 2009.

[48] Yongjin Lee, Kyunghee Lee, Hyung keun Jee, Youn-Hee Gil, Woo-Yong Choi, Dosung Ahn, Sung Bum Pan, "Fusion for Multimodal Biometric Identification", *In: The* 5^{th} *International conference on Audio and video-based biometric person authentication-AVBPA*, Hilton Rye Town, N.Y. USA, pp. 1071-1079, July 2005.

[49] Suo Jidong, Liu Xiaoming, Fusion of Radar and AIS Data", The 7th International Conference on Signal Processing-ICSP'04, Beijing, China, Vol.3, pp, 2604-2607, 2004.

[50] A. Ross, and A. K. Jain,"Information fusion in biometrics;" *in Pattern Recognition Letters*, Vol 24, Issue 13, pp 2115-2125 , 2003.

[51] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. "Handbook of Multi biometrics". *International Series on Biometrics*, Springer, 2006.

[52] A. Ross, A. K. Jain and K. Nandakumar, "Levels of Fusion in Biometrics", *Handbook of Multibiometrics*, Springer, US, 2006.

[53] Raghavendra. R , Rao. A. and Kumar. G.H, "Multisensor biometric evidence fusion of face and palmprint for person authentication using Particle Swarm Optimization (PSO)", *International Journal of Biometrics (IJBM)*, Vol. 2, No. 1, 2010.

[54] Hassan Soliman, "Feature level fusion of Palm veins and Signature Biometrics," *International Journal of video and Image Processing and Network Security (IJVIPNS-IJENS)*, vol:12, no.01,2006.

[55] Priyanka S. Patil and A. S. Abhyankar, "Multimodal Biometric Identification System Based on Iris and Fingerprint," *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, Volume 1, Issue 6,pp: 76-83, 2013.

[56] Yu. P, Xu. D, Zhou. H and Li. H, "Decision fusion for hand biometric authentication," *In proc. of IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS)*, vol. 4, pp. 486-490, Shanghai, China, 2009.

[57] M.El-Abed, C.Charrier," Evaluation of biometric systems,". *In New trends and developments in biometrics*,pp. 149-169, Rijeka: Intech,2012.

[58] S. N. Yanushkevich and A. V. Shmerko, "Fundamentals of biometric system design: New course for electrical, computer, and software engineering students," *Symposium on Bio-inspired, Learning, and Intelligent Systems for Security, ECSIS*, pp. 3-8, 2009.

[59] Sanjay Ganesh Kanade. "Enhancing information security and privacy by combining biometrics with cryptography," *Doctoral thesis.* Institut National des Télécommunications,Université d'Evry-Val d'Essonne,Fance,2010.

[60] Aswin Achuthshankar; Aswathy Achuthshankar,"A novel symmetric cryptography algorithm for fast and secure encryption", 9^{th} *International IEEE Conference on Intelligent Systems and Control (ISCO)*,Coimbatore, India,2015.

[61] C.Paar , J.Pelzl, "The Advanced Encryption Standard (AES)" *In: Understanding Cryptography*, Springer, Berlin, Heidelberg, pp 87-121, 2010.

[62] T.Wollinger , S.Kumar "Fundamentals of Asymmetric Cryptograph," In: *Lemke K., Paar C., Wolf M. (eds) Embedded Security in Cars*, Springer, Berlin,Heidelberg, 2006.

[63] Ronald Rivest, Adi Shamir, and Len Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp. 120-126, 1978. DOI: 10.1145/359340.359342

[64] Whitfield Diffie and Martin Hellman. "New Directions in Cryptography". *IEEETransactions on Information Theory*, 22(6):644-654, 1976. DOI: 10.1109/TIT.1976.1055638

[65] Victor Miller. "Use of Elliptic Curves in Cryptography". In *Advances in Cryptology (CRYPTO '85)*, 1986.

[66] Auguste Kerckhoffs'. "La Cryptographie Militaire," *Journal des Sciences Militaires*, 9:5-38, 161-191, February, 1883.

[67] Christian Rathgeb and Andreas Uhl. "A Survey on Biometric Cryptosystems and Cancelable Biometrics". *EURASIP Journal on Information Security*, 2011(3):1-25, 2011. DOI: 10.1186/1687-417X-2011-3

[68] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. "Biometric template security", *EURASIP Journal on Advances in Signal Processing*, 2008 (Article ID 579416):17 pages. DOI: 10.1155/2008/579416

[69] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition," New York: Springer- Verlag, 2003.

[70] Microsoft Corporation. Windows Biometric Framework - Guidelines for IHV, ISVs and OEMs. Online, March 19 2009. http://www.microsoft.com/whdc/Device/biometric/WBFIntro.mspx.

[71] Y. Itakura and S. Tsujii. "Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures," *In: International Journal of Information Security*,Springer, pages 288-296, 2005.

[72] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *In Proceedings of Sixth ACM Conference on Computer and Communications Security*, Singapore, pp. 28-36,November 1999.

[73] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *In Proceedingsof IEEE International Symposium on Information Theory*, Lausanne, Switzerland,p. 408, 2002.

[74] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," *In Proc. Biometrics: Theory, Applications and Systems*,2008.

[75] Hooda, R., Gupta, S."Fingerprint Fuzzy Vault: A Review", *In:International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4), pp.479-482,April 2013.

[76] Abhishek Nagar,"Biometric Template Security", *In: PHD Thesis*,Michigan State University, USA,2012.

[77] K. Nandakumar, A. K. Jain, and S. Pankanti. "Fingerprint-based Fuzzy Vault: Implementation and Performance", *In:IEEE Transactions on Information Forensics and Security*, 2(4):744-757, December 2007.

[78] Y. C. Feng and P. C. Yuen. "Protecting Face Biometric Data on Smartcard with Reed-Solomon Code", *In Proceedings of CVPR Workshop on Biometrics*, page 29, New York, USA, June 2006.

[79] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim. "Biometric Key Binding: Fuzzy Vault based on Iris Images", *In: Proceedings of Second International Conference on Biometrics*, pages 800?808, Seoul, South Korea, August 2007.

[80] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia. "Cryptographic Key Generation Using Handwritten Signature", *In: Proceedings of SPIE Conference on Biometric Technologies for Human Identification*, volume 6202, pages 225?231, Orlando, USA, April 2006.

[81] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor. "Theoretical and practical boundaries of binary secure sketches", *In: IEEE Transactions on Information Forensics and Security*, 3:673-683, 2008.

[82] T. A. M. Kevenaar, G. J. Schrijen, M. vanderVeen, A. H. M. Akkermans, and F. Zuo. "Face recognition with renewable and privacy preserving binary templates", *In: Proc. AutoID*, pages 21-26, 2005.

[83] F. Hao, R. Anderson, and J. Daugman. "Combining Crypto with Biometrics Effectively", *In: IEEE Transactions on Computers*, 55(9):1081?1088, September 2006.

[84] E. Maiorana and P. Campisi. "Fuzzy commitment for function based signature template protection", *In: IEEE Signal Processing Letters*, 17(3):249?252, 2010.

[85] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate string keys from biometrics and other noisy data," *In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT'04), Lecture Notes in Computer Science*, pp: 523-540, springer Verlag, 2004.

[86] De Santos Sierra, Alberto; Sánchez Ávila, Carmen; Bailador del Pozo, Gonzalo; Guerra Casanova, Javier., "Invariant Hand Biometrics Feature Extraction", *In: The 6th Chinese Conference on Biometric Recognition-CCBR*, Beijing, China, LNCS, Vol 7098, pp. 108-115, Dec 2011.

[87] M. Korichi, A. Meraoumia, S. Chitroub, and A. K. Eddine, "An automated ear identification system using Gabor filter responses," *In International Symposium on Complex Systems and Intelligent Computing , CompSIC'15*, Souk Ahrass, Algeria, 2015.

[88] A. W. K. Kong, D. Zhang, and M. S. Kamel, "A survey of palmprint recognition",*In :Pattern Recogniton*, vol. 42, no. 7, pp. 1408-1418, Jul 2009.

[89] El-Tarhouni, Wafa. "Finger Knuckle Print and Palmprint for efficient person recognition", *In: Doctoral thesis*, Northumbria University,2017.

[90] Juho Kannala and Esa Rahtu,"BSIF: Binarized Statistical Image Features," University of Oulu, Finland,2012.

[91] Dalal, N., Triggs, B. "Histograms of oriented gradients for human detection," *In: Proc. CVPR 2005*, vol. 1, pp. 886?893,, 2005.

[92] R. S. Choras, "Image Feature Extraction Techniques and Their Application for CBIR and Biometrics Systems", *In: International Journal of Biology and Biomedical Engineering* , vol. 1 (1), pp. 6-16, 2007.

[93] Wai Kin Kong, David Zhang, Wenxin Li., "Palmprint feature extraction using 2-D Gabor filters", *In: Pattern Recognition* 36, pp. 2339-2347, 2003.

[94] D. Zhang, W. Kong, J. You, and M. Wong, "On-line Palmprint Identification", *In: IEEE Trans. on PAMI*, Vol. 25, No. 9, pp. 1041-1050, 2003.

[95] John Daugman, "Complete Discrete 2-D Gabor Transforms by Neural Networks for Image,Analysis and Compression,"*In: IEEE Trans on Acoustics, Speech, and Signal Processing*, Vol. 36. No.7. pp. 1169-1179, July 1988.

[96] T.Ojala, M.Pietikäinen, and D.Harwood, " A Comparative Study of Texture Measures with Classification Based on Feature Distributions", *In: Pattern Recognition* ,19(3):51-59,1996.

[97] C. F. Shan, S. G. Gong, P. W. McOwan, "Facial expression recognition based on local binary patterns: A comprehensive study," *In: Image and Vision Computing*, vol. 27, no. 6, pp. 803816, 2009.

[98] Chengjun Liu, "New Color Features for Pattern Recognition," *In: chapter book in intelligent systems references library*,pp:14-34,2012.

[99] S. Banerji, A. Sinha, and C. Liu, "New image descriptors based on color, texture, shape, and wavelets for object and scene image classification," *In: Neurocomputing*, vol. 117, pp. 173-185, 2013.

[100] J. M. Guo and H. Prasetyo, "Incorporating color feature on LBP-based image retrieval," *In: IEEE Int. Conf. Consum. Electron. -Taiwan, ICCE-TW 2015*, pp. 31-32, 2015.

[101] A. Bhagyalakshmi,V. Vijaya Chamundeeswari, "Image retrieval using color and texture binary patterns," *In: IEEE International Conference on Green Computing and Internet of Things (ICG-CIoT)*, pp 715-719,2015.

[102] Shiv Ram Dubey, Satish Kumar Singh and Rajat Kumar Singh, "Multichannel Decoded Local Binary Patterns for Content-Based Image Retrieval," *In:IEEE Transactions on Image Processing*, Vol. 25, No. 9, September 2016.

[103] Abdallah Meraoumia, Salim Chitroub and Ahmed Bouridane, "Robust Human Identity Identification System by Using Hand Biometric Traits," *In: 26th International Conference on Microelectronics- ICM2014*, Doha, qatar, December 14-17, pp.17-20,2014.

[104] K. Chang, K.W. Bowyer, S. Sarkar, and B. Victor, "Comparison and combination of ear and face images in appearance based biometrics", *In :IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 25, No. 9, pp. 1160-1165, Sept. 2003.

[105] Mu Zhichun, Yuan Li, Xu Zhengguang, "Shape and Structural Feature Based Ear Recognition", *In: Advances in Biometric Person Authentication*, Guangzhou, China, pp. 663-670, 2004.

[106] Peter Varchol, Dusan Levicky, "Using of Hand Geometry in Biometric Security Systems", Radioengineering, VOL. 16, NO. 4, pp:82-87, December 2007.

[107] S. Kumra and T. Rao, "A Novel Design for a Palm Prints Enabled Biometric System," *In:IOSR Journal of Computer Engineering (IOSRJCE)*, vol. 7, no. 3, pp. 1-8, 2012.

[108] Abdallah Meraoumia, Salim Chitroub and Ahmed Bouridane,"Robust Human Identity Identification System by Using Hand Biometric Traits", *In:* 26^{th} *International Conference on Microelectronics- ICM2014*, Qatar, December 14-17, 2014.

[109] S. Soviany and M. Jurian, "Multimodal biometric securing methods for informatics systems", *In: Proceedings of the* 34^{th} *International Spring Seminar on Electronic Technology*, pp. 1214, Phoenix, Ariz, USA, May 2011.

[110] IIT Delhi Touchless EAR Database version 1.0, Available online at: http://webold.iitd.ac.in/∼biometrics/Database Ear.htm.

[111] The Hong Kong Polytechnic University, PolyU FKP Database, Available online at: http://www.comp.polyu.edu.hk/∼biometrics/FKP/polyudb.htm.

[112] MSP Database. The Hong Kong Polytechnic University (PolyU), available online at: https://www4.comp.polyu.edu.hk/∼biometrics/MultispectralPalmprint/MSP.htm.

[113] Maarouf K,Abdellah M , Kamal eddine A,"A small look at the ear recognition process using a Binarized Statistical Image Features (ML-BSIF)," *In: The* 3^{rd} *International IEEE Conference on Pattern Analysis and Intelligent Systems PAIS'2018*, Tebessa,Algeria,2018.

[114] M.Korichi, A.Meraoumia,H.Bendjenna, K.E.Aiadi, K.Bensid, "Enhancing the Privacy Technologies by Using the Finger-Knuckle-Print Features," , *In: The* 2^{nd} *International Conference on Pattern Analysis and Intelligent Systems PAIS'16*, Khenchla,Algeria,2016.

[115] M. Chaa, N. E. Boukezzoula, A. Meraoumia, and M. Korichi, "An efficient biometric based personal authentication system using Finger Knuckle Prints features," *In: The* 2^{nd} *International Conference on Information Technology for Organization Development IT4OD'16*,Fez,Morocco,2016.

[116] A.Meraoumia, M.Korichi, S.Chitroub, and A.Bouridane, "Hidden Markov models & principal component analysis for multispectral palmprint identification," *In:* 5^{th} *International Conference on Information and Communication Technology Access, ICTA'15*, Morocco, 2015.

[117] M. Korichi, A. Meraoumia, M. Saigaa and H. Bendjenna,"Securing Person Identification by Combining Hand Biometric Modalities",*In: The* 4^{th} *IEEE International Conference on Signal, Image, Vision and their Applications,SIVA'18*, Guelma, Algeria,2018.

[118] Ajay Kumar n, Tak-ShingT.Chan,"Robust ear identification using sparse representation of local texture descriptors," *In: Pattern Recognition*,46(1), 73-85,2013.

[119] H. Chen," An efficient palmprint recognition method based on block dominant orientation code", *In: Int. J. Light Electron Optics*, 126(21), 2869-2875, 2015.

[120] A. Shoichiro, K.Ito, and T. Aoki , "A finger-knuckle-print recognition algorithm using phase-based local block matching," *In: Information Sciences*, 268 (2014), 53?64, 2014.

[121] Ajay Kumar, David Zhang., "Integrating Shape and Texture for Hand Verification", *In: Third International Conference on Image and Graphics-ICIG04*, 2004.

[122] Lin Zhang, Lei Zhang, David Zhang and Hailong Zhu, "Online finger-knuckle-print verification for personal authentication", *Pattern Recognition*, Vol. 430, pp. 2560-2571, 2010.

[123] Kumar, A., Wu, C. "Automated human identification using ear imaging," *In: Pattern Recognit.,* 45, (3), pp. 956-968,2012.

[124] The FERET Database, http://www.nist.gov/itl/iad/ig/feret.cfm.

[125] The ORL Database, http://www.cl.cam.ac.uk/Research/DTG/attarchive:pub/data/att_faces.zip.

[126] The CASIA Database, http://www.cbsr.ia.ac.cn/english/index.asp.

[127] The AR Face Database, http://www2.ece.ohio-state.edu/∼aleix/ARdatabase.html.

[128] The Extended M2VTS Database, http://www.ee.surrey.ac.uk/CVSSP/xm2vtsdb/.

[129] PolyU Biometrics Research Centre http://www4.comp.polyu.edu.hk/.

[130] The Hong Kong Polytechnic University, PolyU Palmprint Database, http://www.comp.polyu.edu.hk/∼biometrics/.

[131] Zhang D, Guo Z, Guangming L, Zhang L, Zuo W, "An online system of multispectral palmprint verification", *In: IEEE transactions on instrumentation and measurement*, Vol. 59, N 2, pp.480-490, 2010.

[132] L. Zhang, L. Zhang, D. Zhang, "Finger-knuckle-print verification based on band-limited phase-only correlation", *In: The* 13^{th} *International Conference on Computer Analysis of Images and Patterns-CAIP*, Münster, Germany, pp. 141-148, 2009.

[133] F. Wang, J. Han, "Iris recognition method using Log-Gabor filtering and feature fusion," *In: Journal of Xian Jiaotong University*, Vol.41, 2007.

[134] Anil Jain, Karthik Nandakumar, Arun Ross, "Score normalization in multimodal biometric systems", *In: Pattern Recognition*, Vol. 38, pp. 2270- 2285, 2005.

[135] Pereira LFA, Pinheiro HN, Silva JIS, Silva AG, Pina TM, et al, "A fingerprint spoof detection based on MLP and SVM," *In: IEEE International Joint Conference on Neural Networks (IJCNN)*, pp. 17, 2012.

[136] James, G., Witten, D., Hastie, T. & Tibshirani, R. "An Introduction to Statistical Learning",*In: Springer Texts in Statistics series* , 2013.

[137] C.Xia,W.Hsu, andM. L. Lee, "ERkNN: efficient reverse k-nearest neighbors retrieval with local kNN-distance estimation," *In: Proceedings of the* 14^{th} *ACM International Conference on Information and Knowledge Management (CIKM'05)*, pp. 533-540, November 2005.