



HAL
open science

Biometric system for identification and authentication

Foudil Belhadj

► **To cite this version:**

Foudil Belhadj. Biometric system for identification and authentication. Computer Vision and Pattern Recognition [cs.CV]. Ecole nationale Supérieure en Informatique Alger, 2017. English. NNT: . tel-01456829

HAL Id: tel-01456829

<https://hal.science/tel-01456829>

Submitted on 6 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
École nationale Supérieure d'Informatique
16270, Oued-Smar, Algiers, Algeria

Doctoral dissertation, 2017

By: Foudil BELHADJ

Biometric system for identification and authentication

Examination Committee

President:	Walid Khaled HIDOUCI	Professor, ESI, Algiers, Algeria
Examiners:	Latifa HAMAMI	Professor, EMP, Algiers, Algeria
	Hamid HADDADOU	MCA, ESI, Algiers, Algeria
	Saliha AOUAT	MCA, USTHB, Algiers, Algeria
Thesis Supervisor:	Samy AIT-AOUDIA	Professor, ESI, Algiers, Algeria

-February 05th, 2017-



Biometric system for identification and authentication

Foudil BELHADJ

National High School of Computer Science (ESI)
BP 68M, 16270 Oued Smar, Algiers Algeria.
e-mail: f_belhadj@esi.dz



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



To my parents,
To my small family: my wife, Anes and Iyed,
To my brothers and sisters and their families.

Abstract

Biometrics is widely used in identification systems to improve their security. The leading modality is fingerprint thanks to its wide user's acceptability, accuracy, security as well as to its relative inexpensive cost. Although fingerprint identification systems know certain maturity, still some challenging tasks need more researches. In this thesis, we addressed three main problems related to fingerprint identification: the first is related to singular points detection, for which we have proposed an efficient algorithm based on pixel-wise orientation deviation descriptor. The proposed descriptor has the power to capture the orientation field variations in a local neighborhood of a pixel that will be expressed later in the form of orientation field energy. Thus, pixels with local maxima in the fingerprint energy are considered as candidate singular points. They are refined by analyzing some topological characteristics exhibited by the orientation-deviation descriptor. To validate definitively the singularities list and get the type of each singular point, we have extended the Poincaré Index to be defined over the orientation deviation space as a pair of two attributes. The second problem refers to the effects of added/missed minutiae on the matching algorithm performance. Such minutiae can mislead the correspondence scheme to take erroneous local pairing decisions and, thereby, decrease the global matching performance. To overcome this problem, we have proposed a dynamic minutia descriptor that is more tolerant to the occurrence of such erroneous minutiae. It can adjust dynamically its features at the matching step according to the local context of the underlying minutia to let propagating the correspondence synchronization, and thus maximizing the number of genuine paired minutiae. Finally, the third problem we have considered is related to remote authentication to secure access to remote resources. We have described a fingerprint-based scheme that provides a secure remote authentication, communication and non-repudiation scheme exploiting recent advances in cancelable biometrics.

Keywords: Biometrics, fingerprint, identification, matching, remote authentication, singular points.

Acknowledgements

I would like to thank my supervisor Professor Ait-Aoudia Samy for his continuous support along the magister and doctoral studies and related researches. I wish to thank him again for the greatest flexibility that has given to me in deciding the global directions of the research.

Many thanks are addressed to all members off my thesis committee.

Special thanks are addressed to Mr. Akrouf Samir, associate professor at Mohamed El-Bachir Elibrahimi University, BBA, for his valuable aids.

I would like to express my sincere thanks to Mr. Harous Saad, United Arab Emirates University, for his continuous help and support.

Without forgetting my colleagues in both universities Mohamed El-Bachir Elibrahimi University, BBA, and Mohamed Boudhiaf University, M'silâ, my friends together with my students: thanks a lot.

Table of contents

Abstract.....	I
Acknowledgements	II
Table of contents	III
List of Figures	VII
List of tables	X
<hr/>	
Introduction.....	1
<hr/>	
<i>I.1 The identification problem</i>	1
<i>I.2 Biometrics</i>	2
<i>I.3 Fingerprint recognition</i>	2
<i>I.4 Thesis objectives</i>	2
<i>I.5 Thesis outline</i>	3
<i>I.6 Principal contributions</i>	4
Chapter I. Biometrics fundamentals	5
<hr/>	
<i>I.1 Definition</i>	5
I.1.1 Biometric characteristics requirements.....	6
<i>I.2 Biometric system architecture</i>	7
<i>I.3 Performance evaluation</i>	8
I.3.1 False rejection and false acceptance rates.....	9
I.3.2 ROC curve.....	10
I.3.3 Equal Error Rate	11
<i>I.4 Biometrics versus classical authentication schemes: benefits and limitations</i>	11
I.4.1 Benefits of biometrics	12
I.4.1.1 Increased security: anti identity-theft service	12
I.4.1.2 Increased convenience	12
I.4.1.3 Increased accountability: transferability concerns	12
I.4.1.4 Negative recognition	12
I.4.1.5 Non-repudiation service.....	12
I.4.2 Limitations of biometrics	13

I.5	<i>Biometrics market and applications</i>	13
I.6	<i>Biometrics modalities overview</i>	14
I.7	<i>Security and privacy in biometrics</i>	16
I.8	<i>Multimodal biometrics</i>	17
I.8.1	Algerian biometric passport	18
I.9	<i>Conclusion</i>	18
Chapter II. Fingerprint recognition		21
II.1	<i>Fingerprints</i>	21
II.1.1	History of fingerprint recognition.....	22
II.2	<i>Fingerprint ridge pattern characteristics</i>	23
II.2.1	Level-1 features or global features	23
II.2.1.1	Orientation field	24
II.2.1.2	Ridge frequency.....	24
II.2.1.3	Singular regions, singular points and fingerprint patterns	24
II.2.2	Level-2 features.....	25
II.2.3	Level-3 features.....	25
II.3	<i>Fingerprint Individuality</i>	26
II.4	<i>Automated fingerprint identification system</i>	28
II.4.1	Definition.....	28
II.4.2	Recognition process	28
II.4.2.1	Image acquisition.....	29
II.4.2.2	Image quality assessment.....	30
II.4.2.3	Global features estimation	32
II.4.2.3.1	Orientation field estimation	32
II.4.2.3.2	Ridge frequency estimation	35
II.4.2.3.3	Singularity detection	36
II.4.2.4	Fingerprint image enhancement algorithms	36
II.4.2.5	Fingerprint segmentation	38
II.4.2.6	Features extraction.....	39
II.4.2.6.1	Binarization	39
II.4.2.6.2	Ridge extraction: thinning	40
II.4.2.6.3	Minutiae extraction and filtering	42

II.4.2.7	The ISO/IEC 19794-2 (2005) minutia template representation standard	44
II.4.2.8	Matching.....	44
II.4.2.8.1	Minutia-based matching principle.....	46
II.4.3	Performance evaluation.....	47
II.4.3.1	FVC Databases	47
II.5	Conclusion	48
<hr/>		
Chapter III.	Fingerprint singular points detection.....	50
III.1	Singular points.....	50
III.2	Singular points detection: challenges & algorithms.....	51
III.3	Proposed Method.....	53
III.3.1	Principle.....	53
III.3.2	Orientation field estimation	54
III.3.3	Pixel-wise Orientation deviations based descriptor	55
III.3.3.1	Orientation deviation distribution analysis.....	56
III.3.4	Singular point detection	56
III.3.4.1	Orientation field energy measure	57
III.3.4.2	Candidate singular points localization.....	58
III.3.4.3	Singular points validation and type extraction.....	60
III.3.4.3.1	OD-based descriptor profile.....	61
III.3.4.3.2	Extended Poincaré Index	61
III.3.5	SP detection algorithm description	64
III.4	Experimental results.....	65
III.4.1	OD-Descriptor implementation discussion	65
III.4.2	The effect of the OD-descriptor size.....	66
III.4.3	Time performance evaluation	66
III.4.4	Comparative study	67
III.4.5	Singular point for arch-type fingerprint.....	67
III.4.6	Special cases.....	69
III.5	Conclusion	70
<hr/>		
Chapter IV.	Fingerprint matching using a dynamic minutia descriptor.....	72
IV.1	Local minutia descriptor.....	72

IV.2	<i>Issues around matching using local minutia descriptor</i>	73
IV.2.1	The unstable static descriptor problem.....	73
IV.2.2	The search-space size problem	74
IV.2.3	Some proposed solutions	74
IV.3	<i>Minutiae features extraction and core point detection</i>	76
IV.3.1	Minutiae features extraction.....	76
IV.3.2	Core point detection	76
IV.3.3	Minutiae-based Polysegment structure construction.....	77
IV.3.3.1	MPS structure properties.....	77
IV.3.4	The Proposed Matching Algorithm	78
IV.3.4.1	Minutiae node Descriptor	78
IV.3.4.2	MPS-Based matching algorithm	80
IV.3.4.3	Global matching score computation	81
IV.4	<i>Complexity analysis and Experimental results</i>	82
IV.4.1	Complexity analysis	82
IV.4.2	Experimental Results	83
IV.5	<i>Conclusion</i>	84
Chapter V.	Remote fingerprint-based authentication and non-repudiation services for mobile learning systems	86
<hr/>		
V.1	<i>Mobile learning</i>	86
V.1.1	Definition.....	86
V.1.2	Current security concerns.....	87
V.1.3	Related works	87
V.2	<i>Cancelable biometrics</i>	88
V.3	<i>Fingerprint-based authentication scheme for mobile learning</i>	90
V.3.1	Subscription.....	90
V.3.2	Resources access	92
V.3.3	Assessment process	94
V.4	<i>Conclusion</i>	94
Conclusion		95
Bibliography		97
<hr/>		

List of Figures

Figure I.1. Principal biometric modalities.....	6
Figure I.2. A typical biometric system architecture.....	7
Figure I.3. Intra-class and inter-class variations among fingerprints. (a) and (b) two fingerprints from the same finger with low intra-class variation, (c) and (d) two fingerprints from different users with high inter-class variation.....	9
Figure I.4. (a) Genuine and imposter distributions defining the FAR and FRR rates. (b) The ROC curve illustrating the three different security zones.....	10
Figure I.5 Biometrics Market by modality (2015) (Wright & Kreissl, 2014).....	14
Figure I.6. Electronic Passport principle.....	18
Figure II.1. Fingerprint image with marked ridge and valley.....	21
Figure II.2. Brief history timeline of the fingerprint recognition.....	23
Figure II.3. Different levels' features in a fingerprint. (a) Original image showing the friction ridges with labeled singular points, (b) orientation field, (c) frequency image, and (d) partial fingerprint with pores.	24
Figure II.4. The five principal classes of fingerprints with marked cores (as circles) and deltas (as triangles). Note that the plain arch doesn't have, by definition, any singular point.	25
Figure II.5. General process of features-based fingerprint recognition	29
Figure II.6. Some fingerprint images acquired from (a) optical scanner, (b) capacitive scanner, (c) piezoelectric scanner, (d) thermal scanner, (e) inked image and (f) latent image	30
Figure II.7 fingerprint images with marked quality regions: circles for unrecoverable regions, rectangles for good quality regions, continuous triangles for recoverable regions and dashed triangles for background regions	32
Figure II.8. Orientation field estimation approaches	32
Figure II.9. original image and its enhanced images (a) original image, (b) enhanced image using (Hong et al., 1998) technique, (c) the corresponding enhanced image using (Willis & Myers, 2001), and (d) the corresponding enhanced image using (Chikkerur et al., 2007)	37
Figure II.10. Fingerprint image thinning approaches.....	41
Figure II.11. Results of processing a fingerprint image, (a) original image, (b) enhanced image, (c) segmented and binarized image, (d) thinned image, (e) extracted minutiae, and (f) extracted minutiae superimposed on the original image.....	42

Figure II.12 crossing number configurations of a central pixel, (a) intra-ridge continuity, (b) ending minutia, (c) bifurcation minutia.....	42
Figure II.13. Spurious and missed minutiae. Minutiae marked with green constitute ground truth. Detected minutiae are marked with red.....	43
Figure II.14. Some common false minutiae structures and the new structures to which they will be reduced used by (Jiang et al., 2001)	44
Figure III.1. Fingerprint ridge pattern with marked singular regions and singular points. (a) Core point marked with circle; delta point marked with triangle. (b) The associated estimated orientation field showing samples of singular and normal regions: normal-region sample marked with rectangles manifesting smooth parallel pattern in particular direction. The variation of the orientation field is very low; Singular regions marked with ovals showing inconsistent oriented pattern. The variation of the orientation field is very high.	51
Figure III.2. Orientation field estimation approaches.....	52
Figure III.3. The flowchart of the proposed method	54
Figure III.4 Pixel-wise orientation-deviation based descriptor	56
Figure III.5. Orientation deviations distribution in both normal and singular region.	57
Figure III.6 Orientation field energy map of a whorl fingerprint. (a) Original image, (b) orientation field energy map (OFEM) in 3D view, (c) the corresponding 2D view of the OFEM superimposed on the original image. Candidate singular regions are labelled with rectangles (true) and circles (spurious) (d) the gradual transition tendency of the energy in true double-core region, (e) the tendency of the energy in a spurious singular region.	59
Figure III.7 Candidate singular points extracted by global and local thresholding. (a) Original image, (b) corresponding energy map, (c) detected candidate singular regions after thresholding, (d) final candidate singular points superimposed on the original image; the encircled ones are spurious.	60
Figure III.8 Labelled singular, normal and spurious points on some partial fingerprints and their OD-based descriptor profiles. All the descriptors are calculated over 4 circles. (a) True core point, (b) true delta point, (c) arch-type point, (d) normal point, (e) spurious delta point.....	62
Figure III.9 Candidate singular points detection using the extended Poincaré Index. (a) Resulting singular points superimposed on the original image, blue colour indicates core points and red colour indicates delta points, (b) the Δ^- attribute plot which is responsible for detecting the core points, (c) the Δ^+ attribute plot which is responsible for detecting the delta points.	64
Figure III.10 The detection rate evolution on the FVC databases DB1 and DB2 in function of the descriptor size.	66
Figure III.11 Arch-type singular point detection flow chart. (1) Compute the OFEM map, (2) compute the positive attribute Δ^+ , (3) OFEM global thresholding (4) Δ^+ global	

thresholding, (5) pixel intersection between the two images, (6) local energy thresholding that gives the final singular point.	69
Figure III.12 some difficult cases to deal in which the algorithm was able to detect the singularities. (a) and (b) singularities are close to each other, (a) whorl fingerprint, (b) tented arch fingerprint, (c) partial fingerprint with no singularities, (d) and (e) core point localized at border, (f) fingerprint with low quality.....	70
Figure IV.1. The effect of added/missed minutiae on the structure of a 2-Neighbors-based minutia descriptor. (a), (b) and (c) are partial fingerprints of the same finger from FVC2002 database with labelled minutiae. (a) Reference descriptor of minutia m consisting in g1 and g2; (b) the descriptor of ‘m’ has changed, it consists in g2 and s1. The error is due to spurious minutia s1 that has replaced g1; (c) The minutia g1 is missed, the descriptor has been changed to comprise this time g2 and g3.	74
Figure IV.2. Two fingerprints from the same finger with their respective MDGs.	75
Figure IV.3 Some fingerprints with their associated MPS structures. (a) and (b) are impressions of the same finger. Their MPS structures look similar but influenced by the added/missed minutiae. (c) A fingerprint from another finger, its MPS is totally different.....	77
Figure IV.4. The effect of added/missed minutiae on the MPS structure.	78
Figure IV.5. A minutia-node descriptor structure N_i consisted of its 2-predecessors nodes N_{i-1} and N_{i-2}	79
Figure IV.6. Matching of two dynamic descriptors. (a) descriptor of the template node N_i , (b) descriptor of the query node M_i . (c) The new descriptor obtained by adapting (b) to the local context of N_i in (a).....	80
Figure IV.7. Matching results of genuine fingerprints pair. (a) and (b) two fingerprints with their respective MPS; (c) and (d) the final adapted MPSs. Big blue circles are paired nodes whereas squares designate virtual nodes. Note the total similarity between the final MPSs.	82
Figure IV.8 Evolution of the FMR and FNMR	83
Figure V.1 Recent mobile technology capabilities.....	87
Figure V.2 The learning Process	91
Figure V.3 The subscription process	91
Figure V.4 The authentication process.....	92
Figure V.5 The assessment process.....	93

List of tables

Table I.1. Comparison between biometrics and some classical identifiers	13
Table I.2. Comparison of some leading biometric technologies.....	15
Table II.1. Summarized study between some minutiae-based individuality models proposed in literature	27
Table II.2. Some global characteristics of the FVC databases.....	47
Table III.1 parameters used in our algorithm.....	65
Table III.2 Execution times for different stages in the algorithm	67
Table III.3 The comparative results between some proposed SP detection algorithms on FVC2002 DB1.....	68
Table III.4 The comparative results between some proposed SP detection algorithms on FVC2002 DB2.....	68
Table III.5 performance comparison between some selected SP detection methods.....	68
Table IV.1 Complexity of the proposed algorithm with some known matching algorithms.....	83
Table IV.2 Performance indicators of the proposed algorithm.....	83

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 intelligent machines that can be accessed remotely. These include banking, e-commerce, governmental-services to citizens, hotel booking, social aides, and many other fields related to work, traveling, defense, education, business and social relationships.

I.1 The identification problem

Services are now much easier and more immediate. The consumption of the services is generally based on the client-server paradigm where the machine is the server and the client is the individual user. Security of such systems must be highly considered, since the service must be delivered only to legitimate user who has to be initially identified. Traditionally, these systems used, and still are, classical authentication schemes based on credentials consisting in secret information (such as passwords) and/or possessed tokens (certificates, smartcards). Unfortunately, such systems are not enough secure since credentials can be forgotten, stolen or duplicated. In fact, serious concerns revolved around the security of such systems since their vulnerability has been widely exploited by malicious persons to get fraudulently access to privileged rights. These fraudulent incidents are with limited scale in countries such as Algeria where e-services are in their first stages; however, it is reported that over 17 million of US persons were victims of one or more incidents of identity theft in 2014 (Harrell & Langton, 2015). Statistics confirm that governmental and big private organizations are the most targeted ones. The number is growing year after year.

Three main actors could be determined to be responsible for such inconveniences, i) the user is being accused of not taking enough care to protect his credentials, ii) the hacker who has exploited the carelessness of the user as well as some security flaws in the system, and iii) the security strategy adopted by the identification system.

It seems that the system shall be liable for most associated security failures since it has to take into consideration the two first lacks. In fact, the identification strategy adopted is not related to the user himself, rather it is based on what he shall know or what is in his possession. This is the main source of vulnerability and the subsequent security issues.

The establishment of identity problem is not limited to e-services systems only, it is particularly encountered in controlled areas such as airports, traveling stations, governmental and private premises where individuals should be identified based on some collected data. The issue arises acutely in forensic applications where corpses must be identified and crime evidences must be collected. It is very clear that the classical identification systems are useless in such situations.

In any cases, governments, private organization as well as individuals are deeply concerned about the growth of identity scams. Stronger identification mechanisms are of their major priority.

I.2 Biometrics

Biometrics seems to be well ready to deal efficiently with the above issues. It refers to the use of physiological and/or behavioral characteristics to identify an individual. Being dependent on the person himself, biometric identification is more reliable than traditional systems. In fact, biometric identification is based on what the user “is” or what he “does”. These characteristics are intrinsically associated to the user himself and cannot be disassociated from him; transferring or copying biometric traits to be used instead of someone are well infeasible. Hence, we can reliably verify the identity claimed by the user.

Biometrics has revolutionized the way identification is performed. It is becoming a matter of any security system, especially in access control, government-based and forensic applications. Several biometric traits are used in individuals’ identification, these include among others: face, iris, voice, fingerprint, signature, hand geometry, ear, etc. The biometrics market is becoming increasingly wide, it is expected to reach the 30 billion dollars by 2020. The most dominant modality is fingerprint. This latter constitutes the focal point of our thesis.

I.3 Fingerprint recognition

Fingerprint is the oldest and the most used biometrics trait in identification problems thanks to its wide user’s acceptability, accuracy, security as well as to its relative inexpensive cost. Fingerprint analysis can be done at three levels of details: at the global level, useful information are related to the oriented pattern exhibited by the ridge flow. At the local level, minutiae are the most prominent features ensuring the individuality of the fingerprint; they are defined by locations with local ridges discontinuities. At the finer level, pores and ridge contours are considered. A fingerprint analysis algorithm may use one or multiple levels information to design a recognition process. Fingerprint exploitation is going beyond identification and security domains to include some specific applications such as gender identification (Rattani, Chen, & Ross, 2014) and individual ancestor determination (Fournier & Ross, 2015).

The automation of the fingerprint recognition was an absolute necessity due to the huge amount of data to be processed every day by manual inspection. Advanced technologies registered in electronic-sensing and computing technologies have made the automation a reality.

Automated fingerprint identification system is principally a minutia-based process that goes through several steps starting by acquisition, image enhancement, segmentation, features extraction up to matching. The system decision is taken in function of the matching results.

I.4 Thesis objectives

Although automated fingerprint identification systems (AFIS) are of mature technologies, still some challenging tasks need more enhancement and continuous research. In this thesis, we are basically interested in minutiae-based AFISs; in particular, we will focus on three main open problems in fingerprint recognition:

- 1- **Singularity detection problem:** singular points are special locations in the global fingerprint pattern where the ridge structure is of high curvature. Two main types of singularities exist: core and delta points; the first is the center of convergence of the ridge

flow whereas the second is its divergence center. Traditionally, expert examiners used singular points locations (cores and deltas) to visually classify and align fingerprints. The automation of such task to accurately detect both locations and types as well as the number of existing singular points is not a trivial task especially when the fingerprint is of poor quality or the size of the useful ridge structure is reduced.

In this thesis, we have developed an efficient fingerprint singular points detection algorithm based on the estimation of the local orientation field variations (Belhadj, Akrouf, Harous, & Ait-Aoudia, 2015).

- 2- **Presence of spurious minutiae and absence of genuine minutiae problem and its effect on the matching performance:** the minutiae extraction process could deliver some falsely detected minutiae called *spurious* minutiae, as it could also miss true ones called *genuine minutiae*. Although the reliability of this process is largely dependent of the quality of the input fingerprint and the subsequent enhancement steps applied, the presence of spurious minutiae might mislead the matching process to decide erroneous intermediate correspondences that might seriously affect the final matching decision, hence, the global performance of the identification system.

To deal with this issue, we have described a matching algorithm based on an adaptive minutia descriptor that has the ability to adapt dynamically its features in function of the local minutia context. In contrast to most of the state-of-the-art matching algorithms, the descriptor creation is done at the matching step to allow a more flexible adaptation.

- 3- **Remote fingerprint authentication problem:** although AFISs are deployed in all areas, they operate locally. That is, both acquisition and matching steps as well as decision are achieved locally. The proliferation of e-services implies that the user must be identified remotely. The state-of-the-art of the biometrics-based remote authentication solutions is not well established, this latter does not yet exploit the full potentiality of biometrics and still rely on password-based authentication schemes wrapped around PKI infrastructure. Some advanced wanted services such as non-repudiation can't be guaranteed.

In this thesis, we have described a remote authentication scheme based on fingerprint applied to mobile-learning. It is based on advances in cancellable fingerprint systems (Belhadj, Ait-Aoudia, & Akrouf, 2015).

Although, the proposed algorithm is dealing with mobile learning context, it can be considered as being a general framework to ensure fingerprint-based remote authentication.

I.5 Thesis outline

The present thesis is organized as follows:

Chapter I gives general background information on biometrics. It provides a detailed description of the biometric-based recognition process and discusses in details how biometric systems performance are established.

Chapter II is dedicated to the fingerprint modality. We discuss in particular the fingerprint individuality estimation issues, after that we describe the fingerprint recognition process focusing, essentially, on automated minutiae-based systems. Each step of this process is discussed in details;

for each step we review shortly the state-of-the-art of the common methods proposed in literature.

The subsequent chapters present our principal contributions in this field.

Chapter III deals with the problem of detecting singular points in fingerprint images. After discussing what do we mean with singular regions and singular points according to the Henry definitions (Henry, 1905), we give a short but relevant background and literature in singular points detection methods. Next, we detail our proposed algorithm in which we describe the proposed pixel-wise orientation descriptor that has the capability to measure the orientation field variations in a local neighborhood of a pixel. These variations are expressed later in terms of orientation energy. Pixels with high energy determine candidate singular points list. Thereafter, the chapter focuses on techniques to exclude spurious singularities. Some topological characteristics related to the proposed descriptor help to exclude such singularities. To refine definitively the singularities list and get the type of each singular point, we extend the Poincaré Index to be defined over the orientation deviation space. Finally, the chapter gives a comparative study in terms of detection accuracy between the proposed algorithm and some leading techniques in this field.

In Chapter IV, we address the problem of matching two fingerprints in presence of spurious minutiae and missing of genuine ones. After discussing the effect of these outcomes on the matching process, we present our matching algorithm that is based on dynamic minutia descriptor. The complexity of the algorithm as well as its performance are then evaluated.

Chapter V exploits the state-of-the-art in cancellable biometrics to design a remote authentication scheme to secure access to distant resources. The proposed scheme is applied to secure mobile learning systems. We start by identifying the most potential security problems in existing m-learning systems to propose a fingerprint-based authentication scheme that covers all the learning system steps starting by subscription, communication and assessments.

Finally, we terminate this thesis by a conclusions and some future directions.

I.6 Principal contributions

The principal contributions related to this work are:

1. Belhadj, F., Akrouf, S., Harous, S., & Ait-Aoudia, S. (2015). Efficient fingerprint singular points detection algorithm using orientation-deviation features. *Journal of Electronic Imaging*, 24(3), 033016. <http://doi.org/10.1117/1.JEI.24.3.033016> (SPIE Publisher)
2. Belhadj, F., Ait-Aoudia, S., & Akrouf, S. (2015). Secure Fingerprint-based authentication and non-repudiation services for mobile learning systems. In *Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on* (pp. 200–204). <http://doi.org/10.1109/IMCTL.2015.7359586> (IEEE Publisher)

Chapter I

Biometrics Fundamentals

Chapter I.

Biometrics fundamentals

Biometrics, as an automated tool to recognize persons, aims to imitate the wonderful recognition process of human beings. The human ability to recognize a familiar face, voice or an individual manner of walking is a pure mental pattern-recognition process that initially captures and stores some characteristics about the observed subject and recall them, in an acceptable time, in case of need. Biometrics has gone further in person identification; it does not only allow speeding up the identification process, but it introduces some new modalities, such as iris, veins and EEG, based on which the human recognition process fails to recognize the subject. The efficiency, the rapidity and the diversity are the major added values of biometrics compared to the recognition faculty of human beings.

In this chapter, we introduce the fundamental concepts of biometrics. We provide a detailed description of the recognition process, including a brief overview of how a biometric system works, why it is an efficient alternative to the classical identification systems, to discuss after how biometric systems are evaluated in terms of performance. The most used modalities are presented and compared. Finally, we cite some applications where biometrics is of interesting choice.

I.1 Definition

The International Standardization Organization (ISO) defines the term biometrics, or biometric recognition, as being “*the automated recognition of individuals based on their biological and behavioral characteristics*” (ISO/IEC2382-37, 2012).

The definition uses the word ‘*automatic*’ to imply the design of algorithms to be executed by a machine system to recognize individuals. The system could be assisted by a human to get better results. The ‘recognition’ aims to associate an identity with an individual based on some physical characteristics exhibited intrinsically by his body parts and/or some behavioral characteristics created by the body. These characteristics are called “identifiers” or “traits”. Examples of physical characteristics include among others: fingerprints, face, iris, etc. On the other hand, behavioral characteristics may include: signature, voice, keystroke dynamics, etc.

Differently to the classical identification systems that establish the identity of an individual based on what he knows (secret information such as passwords) and/or what he has (possession of objects such as tokens, smartcards, licenses, ...); biometric systems are based on what the person is (biological attributes) and/or what he does (behavioral attributes). These identifiers are directly related to the individual, thus cannot be forgotten, neither copied nor transmitted.

Biometric systems exploit a variety of biometric characteristics (or modalities) including fingerprint, face, ear, iris, retina, palmprint, vein, voice, signature, gait, odor, ... The most leading biometric modalities are listed in Figure I.1 and compared in Table I.2.

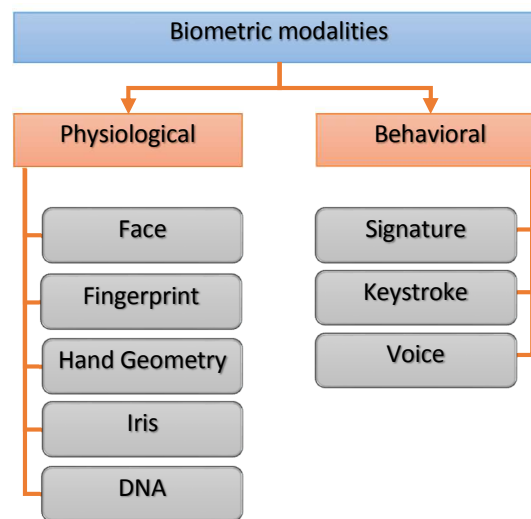


Figure I.1. Principal biometric modalities

I.1.1 Biometric characteristics requirements

A biometric characteristic (or trait) is a measurable physical or behavioral characteristic of an individual that is distinguishable. It determines how an individual is going to be recognized. An important issue in designing a practical biometric system is to answer the question: what characteristics should the system employ to make decision about the individual identity?

Each biometric trait has its own strengths and weaknesses, the choice typically depends on the application domain and, sometimes, on the population intended to be identified. In some cases, more than one characteristics are chosen.

(Anil K Jain, Flynn, & Ross, 2007) have identified some requirements that a typical biometric characteristics must fulfill:

- 1- **Universality:** Every individual accessing the application should possess the characteristics. As an example, we can't use the iris characteristics to identify blind persons, as we can't use signature in an environment where most of the population don't write.
- 2- **Uniqueness:** The underlying characteristics should be sufficiently different across individuals to be able to distinguish between two persons.
- 3- **Permanence:** The biometric characteristics should be resistant to changing in time at least with respect to the operating recognition system period. A trait that changes significantly over time is not a useful biometric.
- 4- **Measurability:** The biometric characteristics must be quantitatively measurable to be further processed by a machine. Suitable devices connected to the machine can be used to acquire and digitize the biometric trait to be transferred later to the recognition system.
- 5- **Performance:** The application that uses the biometric characteristics must ensure an acceptable degree of performance. This includes the matching accuracy/time as well as the resources devoted to build the overall recognition system.

- 6- **Acceptability:** this indicates how much people that are intended to be identified using this characteristics are willing to cooperate with the system by presenting their biometric.
- 7- **Circumvention:** It measures the robustness of the system; i.e. how much is easy to fool the system to make it taking wrong decision or to compromise information about the users biometric data.

It is hard to find a single biometric characteristic that fulfills all the requirements. A practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the users, accepted by the intended population, and sufficiently robust to various fraudulent attacks (Maltoni, Maio, Jain, & Prabhakar, 2009).

I.2 Biometric system architecture

A typical biometric system is constituted of four principal modules (**Figure I.2**):

- 1- **Biometric sensor:** it is responsible for capturing the biometric characteristics from the biometric subject and converting it to a digital form to be transferred to the subsequent module. The performance of the overall process depends heavily on the quality of the acquired raw data. In fact, this data is a result of transforming a real continuous phenomenon (such as a face) to a digital discreet form (face image) resulting in a loss of data. The quality of the acquired data depends on the technology of the reader, the added noise and the degree of the interoperability of the user with the system.
- 2- **Enrollment:** the acquired raw data is first preprocessed to enhance its quality. After that, some relevant *discriminatory* features are extracted, by the extractor sub-module, to generate a compact representation called “*template*” that efficiently resumes the biometric characteristics. The generated template is then sent to the storage system. Generally, the enrollment step allows the biometrics recognition system to learn the identities of the authentic persons in working environment.

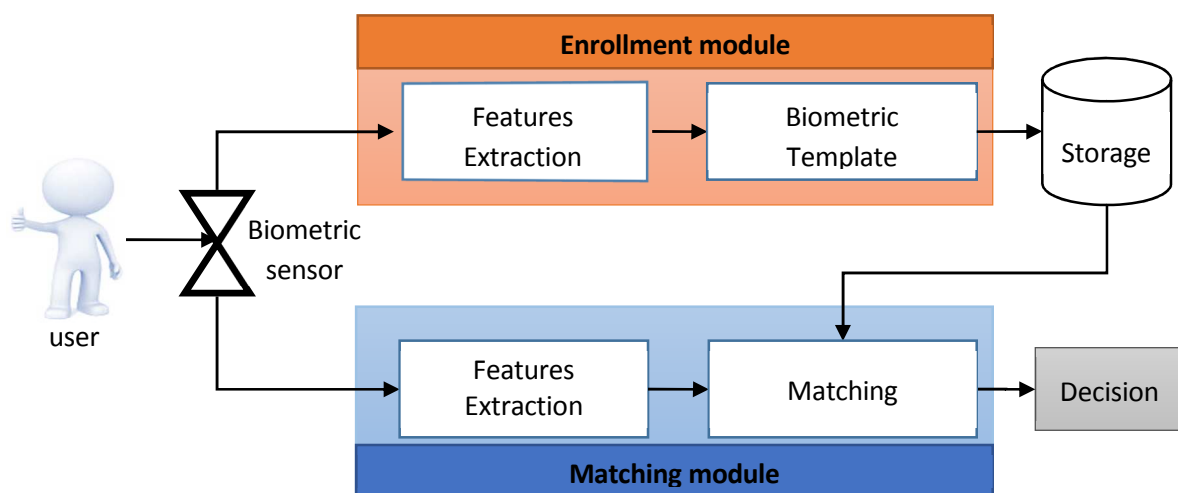


Figure I.2. A typical biometric system architecture

- 3- **Storage system:** the storage system can be a simple file in a simple smartcard as it can be a big database managed by an SGBD. In association with the generated template, some biographic information (name, passwords, address, etc.) can be stored. In any case, the important factor to deal with is the security of the stored template. A compromised template can help to reconstruct the original biometric characteristics, which constitutes a real threat.
- 4- **Matching module:** during the operating phase, the system is requested to identify a person. It proceeds to extract his discriminatory features using the extractor sub-module in the same manner that it has been done in the enrollment step. These extracted features are called query features. After that, the stored template is revoked to be compared with the query. The comparison aims to confirm that both the query and the template features originate from the same biometric subject (person). Generally, the comparison result is a degree of similarity ranging between 0 (total mismatch) and 1 (perfect match) that allows the system to take the suitable decision about the identity of the user.

On the other hand, the biometric system can operate either in *verification* or *identification* mode. In verification mode, the comparison is made only against one template in the system by conducting 1 to 1 comparison. This is possible when we want to confirm the identity claimed by a user. In the identification mode, the comparison is achieved against all records in the database by conducting 1 to many comparisons. This is the case when we want to know if the individual already exists in the database. So, the system try to answer the question “who is the user?”

I.3 Performance evaluation

Two classes of users are intended to be identified by the recognition system. Users who are enrolled in the system constitute the “*genuine*” class. They already have biometric templates stored in the database. The second class, “*imposter*” class, is constituted of all other users that are not genuine. The task of the system is to recognize a genuine user as being genuine and imposter as being imposter. Unfortunately, that is not always the case. In practice, several factors are having an impact on the acquisition of the biometric characteristics in such a manner that two samples originating from the same user’s biometric subject are generally not similar. These include:

- 1- Imperfections related to the sensor: that directly influence the quality of sensed data such as noise and resolution.
- 2- Acquiring environment conditions: any change in the environment conditions, such as illumination, distances or technologies, with respect to the initial acquiring conditions can lead to dissimilarities between acquired samples.
- 3- Interaction of the users with the sensor: the manner that the user interacts with the sensor can change from one acquisition to another. This is the case, for example, of applying more or less pressure on the fingerprint reader that affects the skin elasticity.

The variability observed in the biometric features set of an individual is referred to as *intra-class variation*, it tends to be small; and the variability between features sets originating from two different individuals is known as *inter-class variation* which tends to be large. Figure I.3 illustrates these two types of variations in fingerprint modality. In case of large intra-class variation, the system fails to identify “genuine” persons and considers them as “imposters”, but in case of small

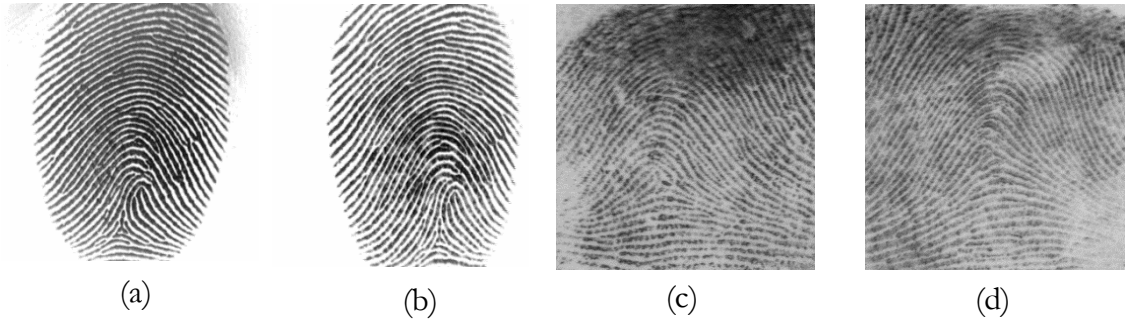


Figure I.3. Intra-class and inter-class variations among fingerprints. (a) and (b) two fingerprints from the same finger with low intra-class variation, (c) and (d) two fingerprints from different users with high inter-class variation

inter-class variation, the system fails to exclude an “imposter” and considers him as “genuine”. These are the main errors that a recognition system can make at the matching step. The ratio of falsely recognized users to the total number of users in each class can be a basic indicator of the effectiveness of the underlying system.

I.3.1 False rejection and false acceptance error rates

Let $s(T, Q)$ be a similarity score that quantifies how much an ‘input’ query features Q are similar to the ‘stored’ template features T . So, the matching result is not a simple “yes/no” answer but, instead, it is a value ranging between 0 and 1. The closer the score is to 1, the more perfect is the matching between the template and the query. To take the matching decision, the system defines a threshold η so that:

$$\begin{cases} \text{score}(T, Q) \geq \eta & \Rightarrow \text{T and Q match (T = Q)} \\ \text{score}(T, Q) < \eta & \Rightarrow \text{T and Q don't match (T \neq Q)} \end{cases} \quad (\text{I.1})$$

The errors that a biometric system can make at the matching step are essentially two:

- 1- False rejection error: this corresponds to a genuine individual that is recognized as imposter user. The expected probability that two samples T and Q obtained from the same subject are declared as a “non-match” defines the False Rejection Rate (FRR).

$$FRR = p(s(T, Q) < \eta / T = Q) = \int_0^{\eta} p(s(T, Q) / T = Q) ds \quad (\text{I.2})$$

where $p(s(T, Q) / T = Q)$ is the genuine score distribution.

- 2- False acceptance error: which corresponds to an imposter individual that is recognized as a genuine user. The expected probability that two samples of the same biometric characteristics obtained from different users are incorrectly declared as “match” defines the False Acceptance Rate (FAR).

$$FAR = p(s(T, Q) \geq \eta / T \neq Q) = \int_{\eta}^1 p(s(T, Q) / T \neq Q) ds \quad (\text{I.3})$$

where $p(s(T, Q) / T \neq Q)$ is the imposter score distribution.

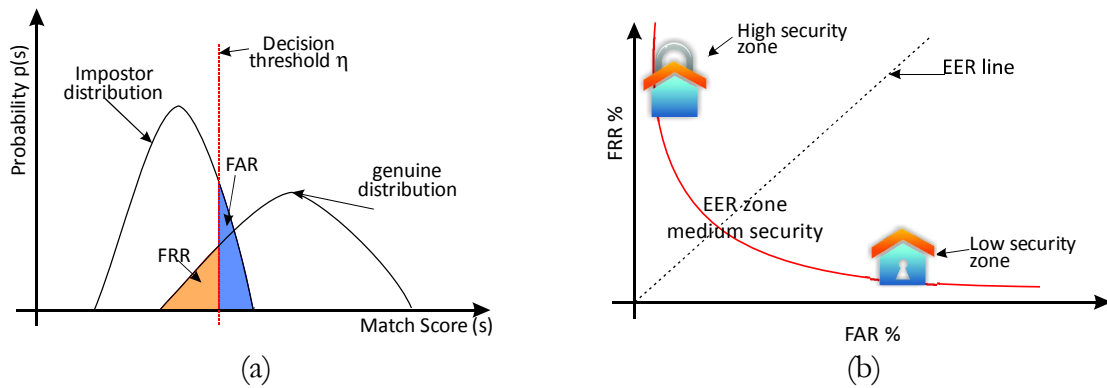


Figure I.4. (a) Genuine and impostor distributions defining the FAR and FRR rates. (b) The ROC curve illustrating the three different security zones.

In some references, (Maio, Maltoni, Cappelli, Wayman, & Jain, 2004; Maltoni et al., 2009) and others, we across other terms such as False Match Rate (FMR) and False Non-Match Rate (FNMR) instead of using respectively FAR and FRR. FMR and FNMR are generally used in identification systems where a query biometrics is compared to a set of stored templates.

Figure I.4-(a) illustrates an example of genuine and impostor score distributions and the associated FAR and FRR for a given threshold η .

Note that both FRR and FAR are functions dependent on the variable threshold η . Decreasing the value of this threshold to make the system tolerant to handle some genuine users intra-variations and noises, and so to decrement the FRR, results in increasing FAR. On the other hand, if η is increased to exclude some small inter-users variations, and so to more secure the system with low FAR, then the FRR raises. It is impossible to decrease both the values. In practice, one has to make a trade-off between these two rates so that the parameters are optimized based on the targeted application. However, how a system designer could describe the recognition performance independently of the threshold η ?

I.3.2 ROC curve

The ROC Curve is a graphical illustration of the evolution of the FRR against FAR for all possible operating thresholds. It permits to describe the recognition system performance independently of the threshold η . Figure I.4-(b) shows an example of a ROC curve. According to this figure, we can distinguish three security zones:

- 1- High-security zone: It is defined by high values of FRR (corresponding to low values of FAR) so that the system considers the majority of users as being imposters (even some genuine ones). This is suitable for critical applications needing high-security level such as military defense and bank accounts.
- 2- Low-security zone: It is defined by high values of FAR (corresponding to low values of FRR) so that the system grants authorization to the majority of users. This is suitable for low secure access control systems such as universities or restaurants where “a stable and quick access

for genuine persons is desirable and security is desired but it is not a critical issue”. This is also the case in forensic applications where we don’t want to miss any suspect.

- 3- Medium security zone: determined by values of FAR and FRR closer to each other. This zone defines a trade-off in terms of security where a medium level is required such as in regular civilian biometric applications. The intersection point between the first bisecting line and the ROC curve is called Equal Error Rate that determines the threshold η for which both FAR and FRR are equal with the simultaneous lowest value that can be.

Depending on the targeted application where the biometric recognition system will be deployed, one can adjust the threshold η in function of the wanted security level (low, medium or high).

I.3.3 Equal Error Rate

The Equal Error Rate (EER) is the most important indicator to evaluate the performance of a recognition system. It guarantees the same false acceptance and false rejection errors. It is common in the biometrics literature to compare the efficiency of proposed matching algorithms in terms of this indicator. An algorithm efficiency is as better as lower the EER is. However, the EER, as a single criterion, doesn’t summarize all the system characteristics.

The FVC competitions (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002; Maio et al., 2004) used, besides the EER, other performance criteria such as:

- ZeroFNMR: is defined as the lowest FAR at which the false rejection is zero,
- ZeroFMR: is defined as the lowest FRR at which the false acceptance is zero,
- average matching time and average enrollment time,
- maximum memory (RAM) size allocated for enrollment and for matching,
- Average and maximum template size.

It’s worth noting that all the errors mentioned above are related to the matcher module, other error types associated with each module of the biometrics system can be defined. For instance, the Failure to Enroll Error (FER) is associated with the enrollment module to indicate that it was unable to acquire the individual biometric traits for any reason.

For further reading about the performance evaluation of biometric systems, the reader should refer to (Schuckers, 2010).

I.4 Biometrics versus classical authentication schemes: benefits and limitations

As stated before, classical authentication schemes are based on what the user knows such as secret information (password) or/and what’s in his possession as identifiers (tokens). They were, and still are, deployed in most security applications even the most critical ones such as banking. These systems have the advantage to be simple to be implemented and integrated in current working systems with low cost. Additionally, they are renewable at any time (cancelable). Biometrics can provide advanced services that are unavailable or weaker in classical schemes. How does biometrics do that?

I.4.1 Benefits of biometrics

I.4.1.1 Increased security: anti identity-theft service

Security provided by classical systems is limited since passwords can be easily guessed, copied or forgot whereas tokens can be hacked or stolen. (Harrell & Langton, 2015) reported that over 17.6 million persons in USA were victims of one or more incidents of identity theft in 2014. Among the victims, existing bank (38%) or credit card (42%) accounts were the most common types of misused information. On the other hand, identity theft incidents in biometric systems are very limited (John, 2003). Biometrics, as intrinsic characteristics, can't be guessed nor copied neither forgotten or stolen. They can't be separated from the person, so his presence is necessary at the time of authentication and nobody can be able to do it instead.

I.4.1.2 Increased convenience

In classical systems, users have to remember, or to put down on paper, their passwords or to carry along with them their tokens. They can't be granted access to services if they forget or lose their credentials. In contrast to classical systems, biometrics don't need to be remembered or to carry anything. The available services can be accessed at any time.

I.4.1.3 Increased accountability: transferability concerns

“Biometrics are excellent technologies when transferability is of concern” (V. M. Lee, 2015). Users can be willingly replaced by others in token-based attendance systems by transferring their identifiers. Accountability of attending people is based on the possession of token not on whom is presenting the token.

Biometrics can solve this problem in accountability applications, such as recording the biometric identities of individuals boarding an aircraft, signing for a piece of equipment, etc.

I.4.1.4 Negative recognition

In classical recognition systems, one user can enroll himself twice or more with two different identities to get illegally supplement advantage of the functionalities offered by the system. For example, a user can submit two or more applications for a visa, for social welfare, etc. Users can easily deny one enrolled identity after having benefited from the service. It is obvious that classical systems can't detect this fraudulent acts.

The problem can be formulated as follows: “how can a recognition system confirm that a certain individual is enrolled in the system although he might deny it?” this is known as negative recognition problem. Biometrics is ready to answer this question.

I.4.1.5 Non-repudiation service

Non-repudiation service refers to the ability of the system to associate an action to a user who performed it in such a manner that this person can't deny his responsibility for that act.

Tokens and passwords based systems can't provide such service since they can't confirm that one user is responsible for an act audited by the system as being performed by him. The user can deny the act and claims that another person did it using his credentials. For example, a person

accesses certain computer resources and later denies his responsibility. To consolidate the system reports, managers would use the usual alternatives of video surveillance which don't make employees feel comfortable.

Since biometric characteristics are difficult to be tricked, “then any action taken that can be linked to that biometric is likely to have been undertaken by the legitimate possessor of the biometric in question. This makes it difficult to believe excuses in which a misdeed was allegedly committed by another who fraudulently obtained one's biometric” (V. M. Lee, 2015).

I.4.2 Limitations of biometrics

The fundamental advantage of passwords and token over biometrics, besides the simplicity and integration facilities, resides in their cancelability. In fact, this characteristic constitutes a considerable “handicap” of biometrics. Unlike passwords and tokens that can be cancelled and renewed at any time (although it is highly recommended to do that even if they are not compromised); biometric characteristics can't be reissued since they can't be disassociated from the owner and replaced by other traits. Consequently, once compromised, biometrics characteristics become useless and are lost forever. Fortunately, recent advances in cancellable biometrics, which is actually an active area of research, have proposed some prominent solutions to overcome this problem (Campisi, 2013; Patel, Ratha, & Chellappa, 2015).

A brief comparison between biometrics and other classical authentication schemes along some factors is given in Table I.1. Other issues related to the security and privacy of biometric systems are discussed in Section I.7.

Table I.1. Comparison between biometrics and some classical identifiers
P = Possible, NP= Not Possible, H = High, L = Low

	Copy	Theft	Oblivion	Loss	User dissociability	Renewability	User acceptability
Clef	P	P	P	P	P	P	H
Token	NP	P	P	P	P	P	H
Code	P	P	P	NP	P	P	H
Biometry	NP	NP	NP	NP	NP	NP	L

I.5 Biometrics market and applications

Biometrics has successfully convinced wide range of applications to be adopted not only as a fundamental component in their security architecture, but as an economical tool that can lead directly or indirectly to saving costs and reducing financial risks (Nanavati, Thieme, Raj, & Nanavati, 2002). It had advanced quickly and significantly over the two decades. Recent researches confirm that the market of biometrics would grow from 8,7 billion dollars in 2013 to nearly 27,5 billion dollars by 2019 registering an annual growth of 19,8% between 2014 and 2019 (Miller, 2015). Fingerprint modality will still dominate the market as shown in Figure I.5). This acceleration is justified by the proliferation of the electronic services that necessitate identification, along with the rise of fraud acts and identity theft that must be fought. In addition

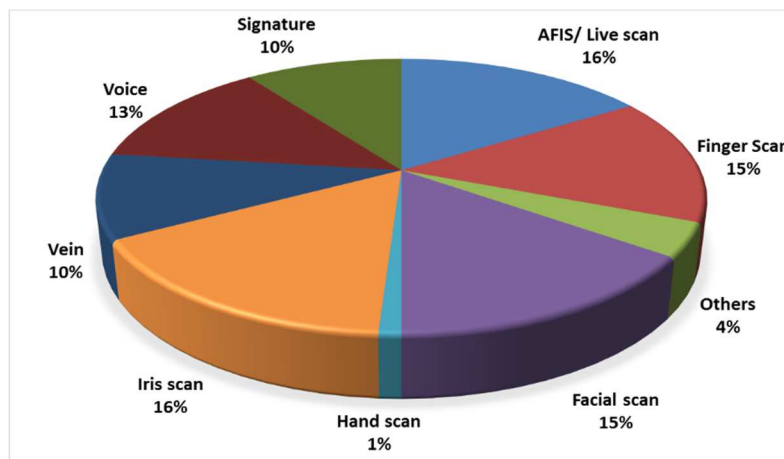


Figure I.5 Biometrics Market by modality (2015) (Wright & Kreissl, 2014)

to that, the adoption of the electronic documents, especially biometric passports and national ID cards, by major governments will participate to largely increase its use.

Biometrics is now adopted in, but not limited to:

- Governmental applications: biometric national identity card, biometric passport, border control, social security, e-voting ...
- Access control: it can be physical such as time-attendance systems and door security, or logical such as accessing remote computer resources and information systems.
- Mobile applications: recent mobiles are equipped with biometrics technologies that allow identifying the owner, to unlock the device, to make commercial transactions, etc. For instance, Apple iPhone 5s and Samsung Galaxy A5 are delivered with a built-in fingerprint reader along with smart software that are attended to recognition purposes.
- Commercial applications: most products integrate biometrics to enhance the user's experience. Access to computers, internet applications, e-commerce, banking transactions, etc.
- Forensics applications: forensic laboratories usually use biometrics in their criminal investigations and parenthood determination as well as to identify corpses. New researches have confirmed the possibility to determine a person's ancestor origin based on his fingerprint.
- Military applications: these include identification systems for use in the field, access control and monitoring applications to sensible areas, as well as large database deployments.






I.6 Biometrics modalities overview


Nowadays, many competitive biometrics modalities and technologies are proposed. As stated before, the choice of one modality with known technology is dependent on the targeted application and the desired performance. Some modalities as well as technologies, such as iris

and retina, are preferred for their high reliability; others are chosen for their user-acceptability and applicability such as fingerprint and face.

Table I.2 summarizes the most used modalities in recognition systems in terms of principles, advantages and disadvantages. This table shows that fingerprint is a trade-off solution between all the other modalities in terms of accuracy, user acceptability, speed and cost.

Table I.2. Comparison of some leading biometric technologies

Biometrics modality	Biometric characteristics ensuring individuality	Advantages	Disadvantages
Fingerprint 	<ul style="list-style-type: none"> • Texture pattern determined by the interleaved ridges and valleys on a fingertip. • Positions and directions of Minutiae, which are local discontinuities caused by sudden broken ridges or merged ridges. 	<ul style="list-style-type: none"> • Most used biometrics. • Mature technology • Relatively high matching accuracy • High matching speed • low cost • multiple fingers • twins-discrimination power 	<ul style="list-style-type: none"> • Dedicated sensor that requires to be touched and maintained. • Sensors can be foiled by tricked fingerprints. • Small but significant failure to enroll rate. • Accuracy dependent of the sensor and the interoperability of the user.
Face 	<ul style="list-style-type: none"> • Location and shape of facial attributes. • Eigenface (weighted combination of a number of canonical faces) 	<ul style="list-style-type: none"> • Can operate on simple 2D images or 3D in static or movies images. • high user's acceptability • Reasonable accuracy. 	<ul style="list-style-type: none"> • Accuracy dependent on controlled acquisition (background, light, ...) • sensitive to simple changes (glasses, face hair, emotions, age, ...) • Possibility of circumvention
Hand geometry 	<ul style="list-style-type: none"> • Geometric structure of the hand (height, width thickness, and surface area of the back of the hand and fingers). 	<ul style="list-style-type: none"> • The acquisition sensor can operate in very challenging environment. • Ease of use. • Small template size. • High user acceptability 	<ul style="list-style-type: none"> • Medium distinctive characteristics. • Low accuracy • High cost compared to other modalities
Iris 	<ul style="list-style-type: none"> • Texture pattern of the Iris (the colored part of the eye: IrisCode, Over 200 points). • 	<ul style="list-style-type: none"> • High accuracy. • Difficult to be tricked (even using lens or dead iris). • Low sensitivity to outside influences 	<ul style="list-style-type: none"> • Low user acceptability (physical discomfort) • Cost tend to be high.
Voice 	<ul style="list-style-type: none"> • distinctive aspects of the voice • can be combined with other physical aspects (e.g., vocal tracts, mouth, nasal cavities, and lips) 	<ul style="list-style-type: none"> • Ease of use. • Low cost. • easy Interface with phrases and words • High user acceptance. 	<ul style="list-style-type: none"> • Low accuracy • Possible replay attack • Possibility of circumvention by persons skilled in mimicking

			<ul style="list-style-type: none"> • Can be affected by recording conditions (noise, recorder tech...) • Sensitive to voice changes.
Palmprint 	<ul style="list-style-type: none"> • Pattern of ridges and valleys • Minutiae 	<ul style="list-style-type: none"> • Area larger than fingerprint • High accuracy • High user acceptability 	<ul style="list-style-type: none"> • Scanners expensive with large surface • Accuracy dependent of the sensor and the interoperability of the user.
Signature 	<ul style="list-style-type: none"> • The manner that a person signs: hand movement + signature image 	<ul style="list-style-type: none"> • Accepted in government, legal, and commercial transactions. 	<ul style="list-style-type: none"> • Can be affected by physical and emotional conditions • Significant inter-user variability • Possible reproducibility
Ear 	<ul style="list-style-type: none"> • The appearance, structure, and morphology of the human ear define individual earmarks. 	<ul style="list-style-type: none"> • Minimally impacted by changes in facial expression • acquisition with no explicit contact with the sensor 	<ul style="list-style-type: none"> • Ear occlusion due to the subject's hair. • Affected by ear modifications such as ear piercing, age, ...
Gait 	<ul style="list-style-type: none"> • The manner a person walks. 	<ul style="list-style-type: none"> • distance-based identification • Independent of the acquisition conditions. 	<ul style="list-style-type: none"> • Low accuracy • Can be affected by footwear, nature of clothing, affliction of the legs, walking surface. • Affected by age
DNA 	<ul style="list-style-type: none"> • genetic code 	<ul style="list-style-type: none"> • Most used for forensic applications. • Ideal for determining parenthood relation. 	<ul style="list-style-type: none"> • Requires chemical operations with specific skills. • Two twins have the same DNA sequence. • It is easy to steal a one' piece of DNA to be misused later.

I.7 Security and privacy in biometrics

With the intense deployment of biometric systems, several security concerns about the vulnerability of the template are emerged. The system can be attacked at each stage of the

recognition process (Maltoni et al., 2009). If biometric data are captured or stolen by an attacker, they may be replicated, misused and, furthermore, used to reconstruct original biometric subject. For instance, (Cappelli, Lumini, Maio, & Maltoni, 2007) have described a successful approach to reconstruct a fingerprint image from the standard ISO template (ISO/IEC19794-2:2005, 2005). This international standard specifies template formats for minutiae-based fingerprint systems. It recommends using plain fundamental information relative to minutiae such as 2D coordinates, minutiae type, direction and some optional information about ridges and singular points.

The reconstructed fingerprint can be misused to circumvent the identification system and to track the user from one application to another by cross-matching biometric data.

A compromised template “may reveal sensitive information about an individual that can be stored, processed, and distributed without his authorization. This information can be used to discriminate against people for instance by denying insurance to people with latent health problems” (Campisi, 2013).

It is, therefore, necessary to enhance the privacy and security aspects of the ‘conventional’ biometric systems by adopting rigorous strategies when designing such systems (Belgouchi, Cherrier, Rosenberger, & Ait-Aoudia, 2013)

I.8 Multimodal biometrics

A biometric system that relies on one biometric characteristic as a single information can never ensure a high level of accuracy. This fact is due to many reasons: 1) no biometric modality is universal at 100%. Fingerprint, for example, knows 2% to 4% of fail to enroll error. Iris is not very acceptable modality in spite of its high accuracy, 2) sensor technology, acquisition conditions and noise have a direct negative effect on the quality of the acquired data and, so, on the performance of the system, 3) user’s interoperability, inter-class and intra-class variations cooperate to mitigate the matching accuracy, and, 4) spoof attacks that aim to reveal personal data.

To get better performance in terms of accuracy and security, one can make multiple modalities working in conjunction to take advantage of their complementarity, and so, to consolidate the decision. This can be possible by:

- 4- Fusing multiple characteristics of an individual, for example, face, Iris and fingerprint
- 5- Using a single modality along with multiple features extraction and matching algorithms. For example, using fingerprint modality with minutiae and pores features.

Hence, the system can operate in multiple unimodal modes or in full multimodal functionalities. The principal issue in multimodal systems is decision fusion in case of inconsistent results from each unimodal stage.

The next subsection discusses a typical example of multimodal applications: the biometric passport.

I.8.1 Algerian biometric passport

The Algerian biometric passport is conform to the technical specifications recommended by the International Civil Aviation Organization (ICAO) standards (ICAO, 2015).

It is an identification document that combines both individual biographic information and biometric characteristics. It embeds a contactless RFID microchip with a microprocessor that has cryptographic abilities. It is used to identify travelers at borders to be sure of their identities.

The personal information is printed on the passport paper as well as embedded in the chip. These include nouns, date of birth, photograph and signature. Biometric characteristics included in the chip are face and fingerprints as described in the (“Journal Officiel, Arrêté du Aouel Safar 1433 correspondant au 26 décembre 2011,” 2011). The passport is prepared for additional biometrics such as Iris and palmprint (see Figure I.6).

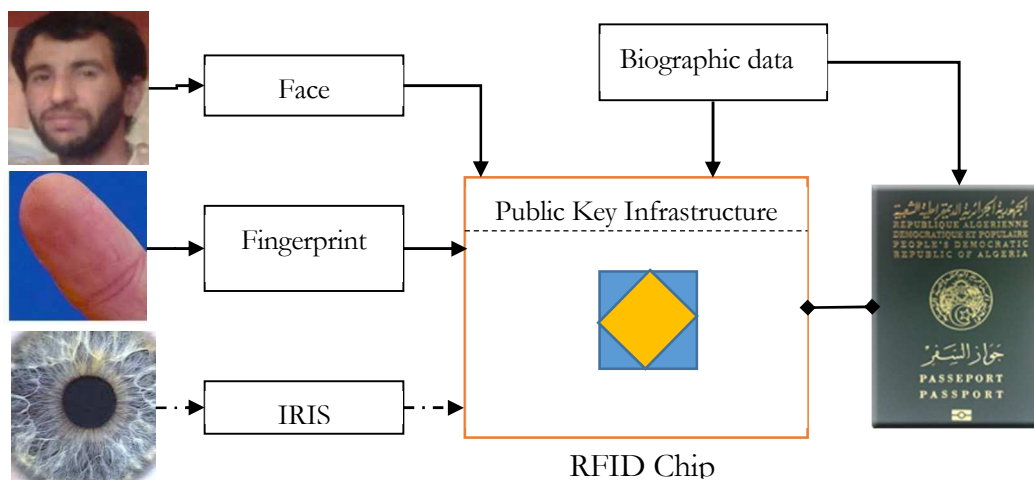


Figure I.6. Electronic Passport principle

The storage of data in the chip as well as the communication between the electronic border control systems, that establishes the authentication, are ensured using a Public Key Infrastructure (PKI) (Bosworth, Kabay, & Whyne, 2014). The comparison of biometric features is performed outside the passport chip.

I.9 Conclusion

Biometrics aims to imitate the mental pattern recognition process in the manner that it identifies persons. It is a more secure and reliable alternative to the classical authentication schemes based on secrets and tokens. Biometrics technologies use human physiological and behavioral characteristics to recognize individuals in an automated process. These characteristics have to fulfill some requirements in particular universality, performance and applicability.

The recognition process is based on two steps: the first, enrollment step, aims to allow the system to learn the identity of the person. It starts by extracting some discriminant attributes from the sensed data which will be compacted to construct a template that will be stored in a database. The template is a highly representative structure that efficiently summarizes the individual biometric characteristics. The second step, matching step, recalls the already stored template to

be compared with newly extracted attributes. Upon the comparison results, the system makes a decision whether the individual is truly the enrolled identity that he is claiming or not with a certain degree of confidence ranging between 0 and 1.

Due to large inter-class and small intra-class variations of some biometric samples, the decision of the system can be erroneous. The performance of the recognition system is traditionally characterized by two error statistics: FRR and FAR. The first occurs when a system rejects a genuine identity where the second occurs when an imposter identity is incorrectly accepted. A tradeoff between these two errors is called Equal Error Rate (ERR) where FAR and FRR meet with equal values.

It is largely believed that no biometric trait can be accurate at 100%; the conjunction of multiple biometric characteristics to operate in conjunction in a single recognition system can largely consolidate the recognition decision and, so, increase the accuracy.

The market and industry of biometrics know a high acceleration justified by the growth of the unsupervised electronic services that need an accurate individual authentication along with simultaneous growth of fraud acts all over the world. Fingerprint is the most dominant modality in the market; it constitutes a trade-off in terms of accuracy, security and cost among other modalities.

The details of the fingerprint as biometric characteristics and the automated recognition process based on this modality will be discussed in the next chapter.

Chapter II

Fingerprint Recognition



سورة القيامة (75)، 4-1

I CALL TO WITNESS the Day of Resurrection, (1) And I call the reprehensive soul to witness: (2) Does man think We shall not put his bones together? (3) Surely We are able to reform even his finger-tips. (4)

AL-QUR'AN 75:1-4

Ahmed Ali translation

Chapter II.

Fingerprint recognition

Fingerprint is the oldest biometric modality used by human beings to solve identity problems related to commerce, children parenthood, signing contracts, etc. in ancient Babylon, Egyptian and Chinese civilizations that go back before the third century B.C (Maltoni, Maio, Jain, & Prabhakar, 2009). It is still the most dominant modality in today's world thanks to its wide user's acceptability and mature technology as well as to its relatively inexpensive cost. The most beautiful thing resulted from the humanity experience in the fingerprint recognition is the automation of the identification process.

Nowadays, automated fingerprint identification systems (AFIS) are deployed as an important part in most applications where security is of major concerns. AFIS combines advanced sensing technologies with sophisticated recognition software to build smart identification applications. Moreover, recent advances in fingerprint researches have shown that fingerprints can reveal more than just the individual's identity, they can determine the person's gender and even his ancestor origins (Fournier & Ross, 2015).

In this chapter, we describe the fingerprint recognition process focusing, in particular, on minutiae-based automated systems. First, we define what do we mean with a fingerprint, what does make it suitable for recognition to discuss later its individuality. Next, the automated recognition process is detailed step by step. A short exploration of the commonly proposed methods in literature to achieve each step is given.

Although the literature makes difference between authentication, identification and recognition, we use these terms interchangeably throughout the rest of this document.

II.1 Fingerprints

In biometrics science, a fingerprint is the texture pattern formed by the interleaved ridges and valleys on the fingertips (Maltoni et al., 2009). In forensic science, it is “the impression, visible or

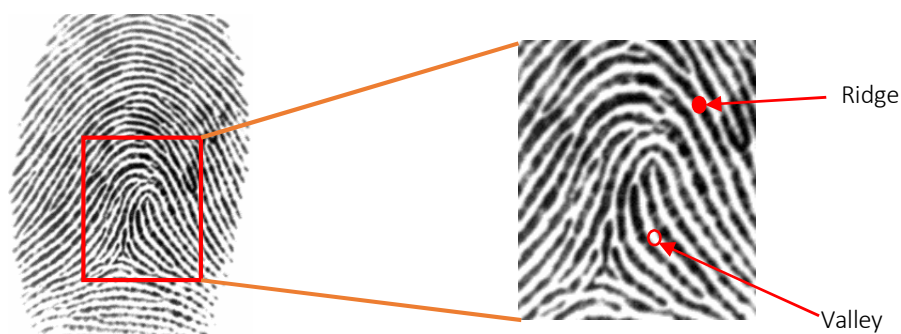


Figure II.1. Fingerprint image with marked ridge and valley

not, left when a person's finger(s) comes into contact with a surface, leaving behind a characteristic pattern of ridges, grooves, whorls, arches and other features by which the print can be identified.” (Newton, 2008).

Ridges are the upper skin layer segments of the finger that touch a surface, and valleys are the lower segments. Once acquired, ridge lines represent the dark areas in a fingerprint image whereas valleys are viewed as inter-ridge spaces constituting the bright areas (see Figure II.1). Though friction ridges seem to be well organized with the same width and height, they are extremely variable. They vary in width from 100 μm , for very thin ridges, to 300 μm for thick ridges. Generally, the period of a ridge/valley cycle is about 500 μm (Maltoni et al., 2009). Furthermore, friction ridges differ in details between males' and females' fingerprints. In a male's fingerprint, ridges tend to be thicker and altered, whereas in female's fingerprint ridges are more structured and less thick with high density. These variations are not so easy to be captured by a naked eye.

Cuts and burns to a finger can't change the ridge structure, it will be reproduced as original as it was when the skin grows. Fingerprint ridges formation is a result of interaction between the genes and the environment in which the fetus evolves. The DNA gives instructions on how the skin should evolve and the environment (the womb and the amniotic fluid flow) affects its form. Therefore, two fingers of the same person or from two twins can't have the same fingerprint since this last one is dependent on the randomness of the environment factors (Anil K Jain, Flynn, & Ross, 2007). The final form of the fingerprint is fully established at the seven month of the fetus life and remains unchanged throughout the whole individual lifetime. This is one of the most attractive characteristic based on which fingerprint identification systems rely.

II.1.1 History of fingerprint recognition

Although recent researches confirm that ancient human beings were aware of the individuality of the fingerprint, systematic studies of the fingerprint structure were initiated in the late of the seventeenth century. The story starts in 1684 by the anatomist Nehemiah Grew who was the first who scientifically studied the friction ridges. Later, Marcello Malpighi is credited to be the first who used the microscope to study the skin. He noted the presence of ridges, spirals and loops in fingerprints. Since then, friction ridge had been studied for many years. In 1788, the uniqueness of the ridge structure was announced by the German J. C. A. Mayer, whereas Hermann Welcker remarked that his fingerprint hadn't change between the first impression and the second one taken after 40 years, he is credited to be the first who claimed the permanence of the friction ridges. In 1880, Henry Faulds published in a journal the value of friction ridge skin for individualization, especially its use as evidence of crimes. He is credited to be the first who used the ink to take fingerprint impressions. Just later, Francis Galton wrote a book on fingerprints, he introduced the notion of 'minutia' as permanent and unique characteristic. At the beginning of the 20th century, recognition of criminals by means of fingerprints became standard practices. “It would seem that nothing much more happened with regard to the wider area of biometrics until the 1960s, when the advent of electronics and integrated circuits presented the promise of automation” (Krishan, Kanchan, & Bumbrah, 2012). This helped a lot to make it possible at the beginning of 1970s to write algorithms and to use sensors to identify humans.

A brief history timeline about the fingerprint recognition is given in Figure II.2. Further detailed reading on fingerprint history can be found in (Krishan et al., 2012)

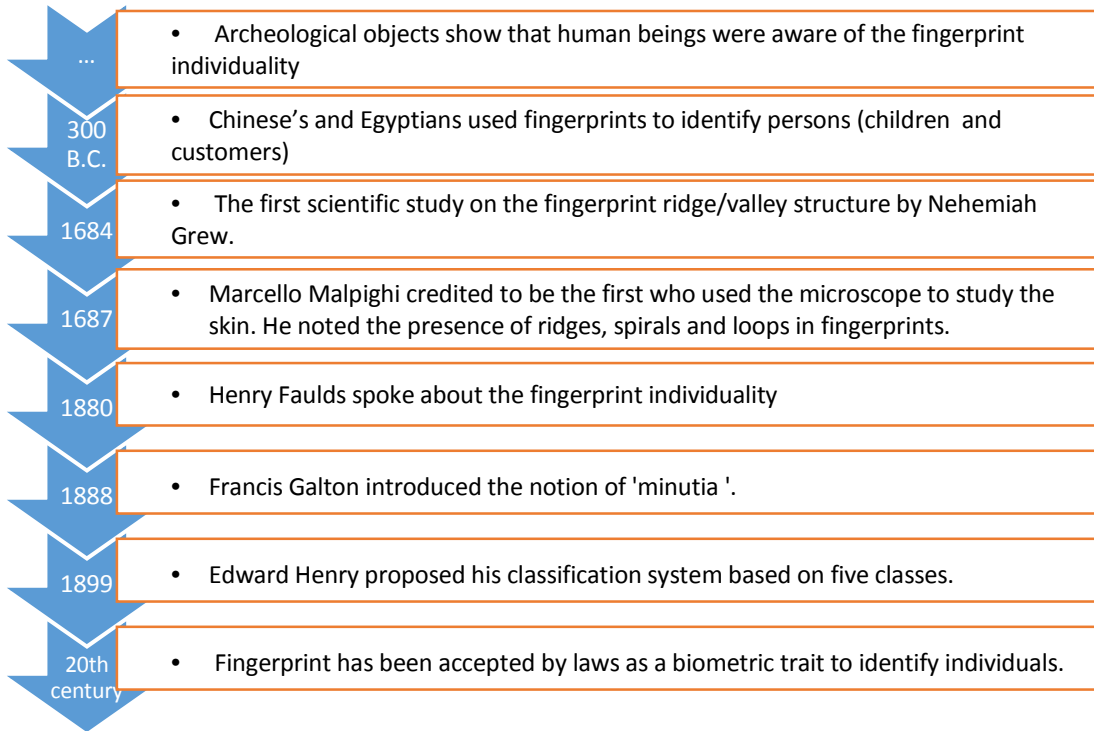


Figure II.2. Brief history timeline of the fingerprint recognition

Thanks to these efforts, automated fingerprint recognition technologies have now rapidly grown to be used not only in forensic applications, that were the first adopters of the fingerprint recognition, but also in a wide range of applications such as control access, computer logon, e-commerce, etc. This is due to its high accuracy and acceptability as well as its low-cost technology.

II.2 Fingerprint ridge pattern characteristics

There are several important factors, such as noise, distortions, acquiring conditions and interoperability of the user, that make two impressions of the same finger consecutively acquired not exactly similar. Consequently, fingerprints cannot be matched directly using a simple distance between their brute gray scale data; instead of that, fingerprint recognition, whether done manually by a human expert or automatically, is basically a feature-based process. This means that an individual finger, once its fingerprint is acquired, is represented as a set of features extracted from the image that will be later compacted and stored in a template to be recalled at the matching step.

Fingerprint can be viewed at three different levels: global, local and finer. Throughout each level, some relevant features describing the fingerprint can be extracted. Levels of detail in a print are simple descriptions of the different types of information throughout the print.

II.2.1 Level-1 features or global features

Level-1 features enclose the fingerprint in a global perspective with which are attached all global characteristics related to the oriented texture pattern exhibited by the ridge/valley structure. These include the orientation field, the ridge frequency and singularities. Although these features don't carry any information about the individuality of a fingerprint, they can be used as exclusive

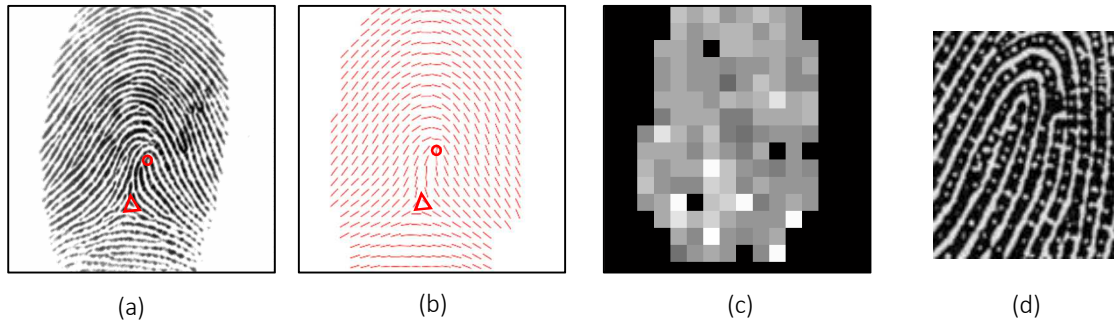


Figure II.3. Different levels' features in a fingerprint. (a) Original image showing the friction ridges with labeled singular points, (b) orientation field, (c) frequency image, and (d) partial fingerprint with pores.

tools to decrease the search space at the matching step, by ensuring fingerprint classification, as well as to make difference between a fingerprint and palmprint patterns.

II.2.1.1 Orientation field

Fingerprints exhibit everywhere a well-defined local ridge orientation. At each pixel location $p(x, y)$ can be associated a value ranging between 0 and π indicating the slope of the tangent line to the ridge at the point p . All the pixels' orientations, once calculated, constitute the orientation field (OF) of the image. Figure II.3-(a and b) shows a fingerprint and its associated estimated OF. Methods to estimate the orientation field are discussed in Section II.4.2.3.1.

II.2.1.2 Ridge frequency

Similarly, a fingerprint exhibits a ridge spacing at each pixel location. The local ridge frequency at a point $p(x, y)$ is the number of ridges per unit length along a segment centered at p and orthogonal to the local ridge orientation (Maltoni et al., 2009). It is another intrinsic property that characterizes a fingerprint. Figure II.3-(c) shows an example of a fingerprint image frequency. Methods to estimate the ridge frequency image are discussed in Section II.4.2.3.2.

II.2.1.3 Singular regions, singular points and fingerprint patterns

The ridge structure in any fingerprint tends to take a global configuration with a special shape. It delimits two distinctive regions: 1) normal regions: where the ridges are arranged in smooth parallel lines having a predominant direction, and 2) singular regions: where the ridge pattern exhibits high curvatures with no dominant direction.

Singular regions define some special points called singular points determined by locations where the OF changes rapidly with maximum ridge curvature. Edward Hennery in (E. R. Henry, 1990) has defined two main singular points: The first is the core point and is defined as "the topmost point of the innermost curving ridge". The second is the delta point and it is at "the center of a triangular region where three different ridge flows meet".

The number and locations of singular points have a direct influence on the 'shape' of the orientation field that can be systematically classified into five classes according to Henry classification system (E. R. Henry, 1990): whorl, left loop, right loop, arch and tented arch (see Figure II.4). The three first classes constitute over 95% of the population (Maltoni et al., 2009).

More about singular points can be found in the next chapter. The main advantage of level-1 features is their ability to be captured even with low image resolution.



Figure II.4. The five principal classes of fingerprints with marked cores (as circles) and deltas (as triangles). Note that the plain arch doesn't have, by definition, any singular point.

II.2.2 Level-2 features

Level-2 features refer to all local details related to the paths of the ridges. These include the starting position of the ridge (relative to the image frame), the path taken by the ridge (in terms of adjacent pixels), its size (number of pixels) and the ending position where the ridge stops. Note that all these details are measured in terms of one pixel in width related to the skeleton (or thinned) image of the input fingerprint.

The most noticeable level-2 characteristics are local discontinuities exhibited by the ridges. In fact, ridges often run in continuous curves and suddenly terminate at specific points locations called ridge endings. Others split at some points called bifurcations to yield other ridges. Both ridge endings and bifurcations points are called *minutiae* (or Galton features). Other forms of discontinuities already exist in fingerprints such as forks, spurs, bridges, dots, crossovers and trifurcations. These features take forms of several local composite minutiae that can be expressed in terms of bifurcation and/or ending minutiae (Daluz, 2014). It has been reported that almost 50 % of minutiae consist in ending points, 25 % are bifurcations, 15 % are dots. The number, locations directions and types, as well as spatial relationships between them are sources of individuality so they can be used for identification. A fingerprint image and the associated minutiae are shown in Figure II.12.-(e and f)

II.2.3 Level-3 features

Fingerprints, once acquired with high resolution, typically 1000dpi, exhibit some useful information that is not visible to the naked human eye in the standard resolution, given by major sensors in the market working typically in 500 dpi. This information are attached to the pores and shapes of the ridges. Pores refer to the holes existing along the ridges path (Figure II.3-d). The arrangement of pores along the fingerprint ridges guarantees the individuality of the finger provided that a reliable extractor is used. In practice, pores are used conjointly with minutiae or ridges (A K Jain, Chen, & Demirkus, 2007), in a multi-biometrics sense, to enhance recognition

accuracy especially when partial fingerprints are submitted that lack a sufficient number of minutiae.

II.3 Fingerprint Individuality

Fingerprint recognition is based on two fundamental principles:

- 1- Fingerprint ridge structure is unchangeable (permanence property; refer to Chapter I),
- 2- Fingerprint ridge structure is unique to an individual (individuality property).

The first principle has been validated and established by empirical observations as well as by ridge anatomy studies. However, the second claim is still accepted, as it has been through the history of fingerprint recognition, as a fact based on a manual inspection of millions of fingerprints (S. Dass, 2014). Upon these assumptions, fingerprints have been used in courts of law for almost 100 years and the testimony based on fingerprints carries substantial credibility and weight (Maltoni et al., 2009).

The word unique means that no duplicate or full similar ridge structure can be found among all fingers of all human beings. The scientific American magazine has claimed in 1911 that “*Two like fingerprints would be found only once every 10^{48} years*”. Thus, the question is: to what extent can a set of fingerprint features be distinctive?

The answer to the above question involves to propose a comprehensive mathematical model that describes the ridge features taking in account three requirements (Lee, Ramotowski, & Gaensslen, 2001):

- 1- Measure of the amount of the fingerprint features that is available to compare,
- 2- Measure of the amount of the fingerprint features in correspondence between the two fingerprints,
- 3- Objectively interpret the meaning of the similarity of a given correspondence of two fingerprints.

Hence, the fingerprint individuality problem returns to establish the probability of non-correspondence $PNC = P(M(F_1, F_2) = k / F_1(m) \neq F_2(n))$ that ‘k’ features match between two arbitrary fingerprints F_1 and F_2 belonging to different fingers having ‘m’ and ‘n’ features respectively, provided that a matching similarity metric has been already defined.

Another issue, that the fingerprint individuality estimation studies have to answer, is related to the minimum number of matched features, k, to be absolutely sure that the two fingerprints belong or not to the same finger.

In literature, most proposed individuality models are based on minutiae configurations, since these are mostly used in fingerprint matching (J. Chen & Moon, 2008). The effectiveness of such models is conditioned by finding a reliable representation that depicts the inter-user variations as well as a suitable minutiae distribution model.

(Pankanti, Prabhakar, & Jain, 2002) proposed a uniform distribution to model both the location and direction of each minutia with the restriction of that they are not close to each other. Only bifurcation and ending minutiae are considered. They supposed also that only one

correspondence exists between two fingerprints. The matcher used is a simple tolerance box matcher.

(J. Chen & Moon, 2007) judged that the uniform distribution associated to minutiae in (Pankanti et al., 2002) model in terms of locations and directions is not suitable. They suggested to extend this model by considering the minutia direction not independent of its location and propose the von-Mises distribution as suitable representation to this dependency.

(Zhu, Dass, & Jain, 2007) noted that minutiae tend to cluster inside singular regions and disperse outside. Hence, they reviewed the (J. Chen & Moon, 2007) model to propose a sophisticated minutiae distribution model based on a mixture of Gaussians, for minutiae locations, and Von-Mises distributions for minutiae directions.

(Su & Srihari, 2008) considered the previous model to include ridge information into their generative model by using the distribution for ridge points' locations and orientations. The ridge length is modeled using the normal distribution.

(Y. Chen & Jain, 2009) argued that the previous models have ignored the variety of distinctive features that a fingerprint image exhibits. To be more accurate in individuality estimation, they propose to consider the ridge information contained in the three levels (see Section II.2) into account to build their model. Parameters of the distributions are adapted in function of the class to which the fingerprint belongs (see Section II.2.1.3).

(Nagar, Choi, & Jain, 2012) reproached previous studies for two principal limitations: i) the matching criteria used are far different from those used in practical matchers, and ii) the intra-variations between fingerprints is not considered anymore.

The generative model proposed by (Q. Zhao, Zhang, Jain, Paulter, & Taylor, 2013) has further taken into account the correlation between minutiae and other fingerprint features levels such as level-1 (orientation field).

Table II.1 summarizes some minutiae-based individuality models.

Table II.1. Summarized study between some minutiae-based individuality models proposed in literature

Authors	Modeled features	Features distribution
(Pankanti et al., 2002)	Minutia (Bifurcation and ending points)	- Uniform distribution for both locations and directions. - Independence between minutia location and direction
(J. Chen & Moon, 2007)	Minutia (Bifurcation and ending points)	- Uniform distribution for locations - Von-Mises distribution for directions
(Zhu et al., 2007)	Minutia (Bifurcation and ending points)	Mixture model using Gaussian and Von-Mises distributions
(Su & Srihari, 2008)	Minutia (Bifurcation and ending points) + representative ridge points	Mixture model using Gaussian, Von-Mises distributions and Empirical distribution for ridge type
(Y. Chen & Jain, 2009)	Minutia (Bifurcation and ending points) + ridges and pores	Bivariate Gaussian Von-Mises distributions

II.4 Automated fingerprint identification system

The adoption of fingerprint recognition by many agencies especially in forensic and law enforcement applications has led to the appearance of large databases that contain millions of fingerprints against thousands of requests to be daily analyzed. The manual system established for searching and verifying fingerprints was requiring more and more human resources as well as extended time to answer one request. Nonetheless, it was approaching the point of being unable to handle the daily workload (Krishan et al., 2012). The automation of the recognition process was an absolute and urgent necessity to speed up requests processing. Three main problems were encountered in designing such automated system: 1) how to acquire a fingerprint whether it is recorded on an object or from a live finger? 2) how to process the acquired image to extract salient features? and, 3) how to achieve the comparison between two sets of features?

As a result, the first automated fingerprint identification system prototype was installed in 1972 that was fully operational in 1983. Since then, many improvements have been brought to the system at both the hardware and the software levels.

II.4.1 Definition

Automated fingerprint identification system (AFIS) is a computerized technology that allows to collect, process and store individual's fingerprint features to make a decision about his identity.

The system comprises hardware and software subsystems. The hardware components consist principally in a fingerprint reader, a (or multiples) CPU, storage and communication infrastructures, whereas the software subsystem consists in efficient algorithms to process fingerprints.

II.4.2 Recognition process

The goal of an AFIS is to establish the identity of an individual based on his fingerprint. In case of a genuine user, who is already enrolled in the system database, a record of his personal information is reported; otherwise, a null identity is reported to indicate that the person in question is an imposter.

The recognition process starts by acquiring the fingerprint of the individual's finger, using an electronic reader, as a bitmap image where darker areas depict the ridges and brighter ones indicate valleys. The quality of the acquired image can be affected by the reader technology, the acquisition conditions and the finger state. The digitized image may need some enhancement steps to be prepared to the segmentation phase. This last one aims to extract the useful ridge structure from the background. The segmented image is then ready to the features extraction procedure that has to efficiently extract salient features that represent, together, the finger. These features are compacted in a summarized form into the so-called 'descriptor' or 'template'. In the enrollment mode (see chapter I), the obtained descriptor is stored in a database, whereas in identification mode, it is compared against each stored template. The comparison result is a similarity score, ranging between 0 and 1, that quantifies to what extent the input fingerprint represents the claimed identity found by the system.

Figure II.5 depicts a general process of an automated fingerprint identification. The subsequent sections give more details about each step.

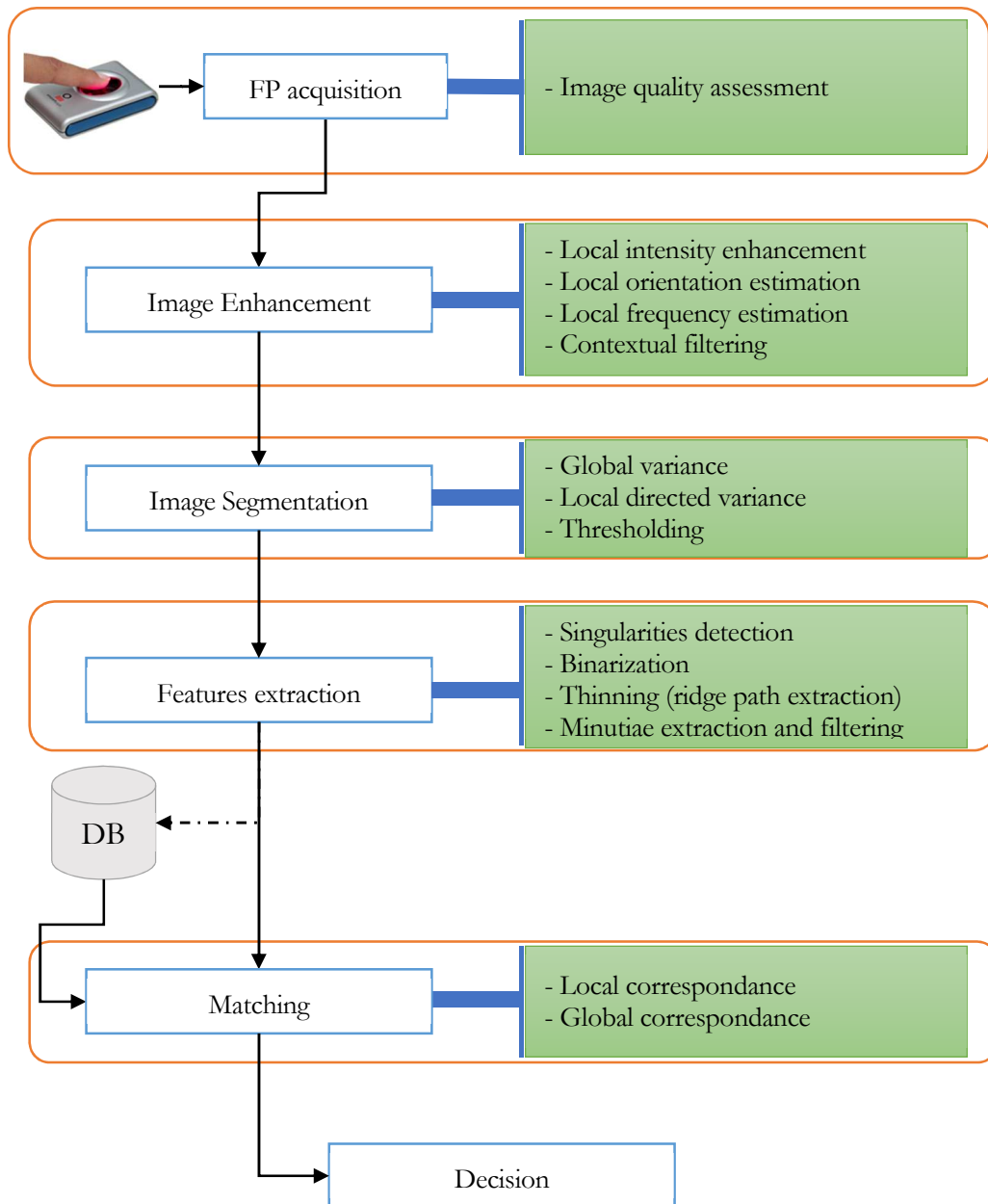


Figure II.5. General process of features-based fingerprint recognition

II.4.2.1 Image acquisition

Basically, there are two manners of acquiring fingerprints:

- 1- **Offline acquisition:** the fingerprint is acquired not directly from the individual's finger, instead, it is digitized from a medium on which the fingerprint is recorded. This is the case of inked fingerprint that is initially rolled on paper using ink. The paper is then acquired using ordinary paper-scanner producing the digitized image. In crime scenes, the fingerprint is found left on some objects, due to the sweat and grease characteristics of the finger. Since it is not visible to the naked eye, specialist adds some chemical products or change light frequencies to make it visible and reproducible on some special adhesives to be captured

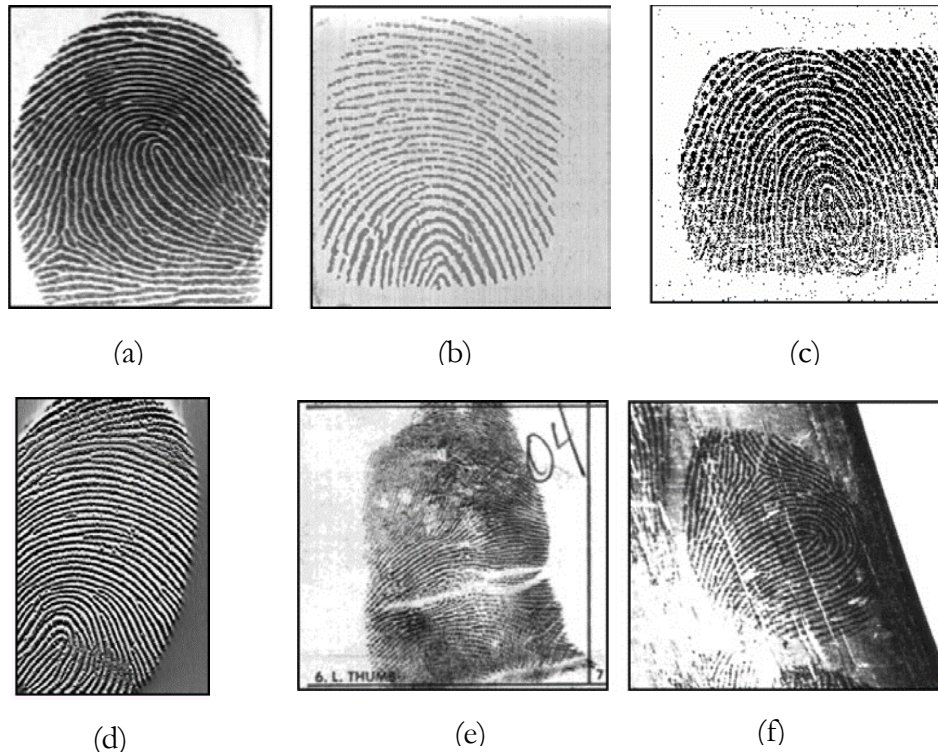


Figure II.6. Some fingerprint images acquired from (a) optical scanner, (b) capacitive scanner, (c) piezoelectric scanner, (d) thermal scanner, (e) inked image and (f) latent image

later by scanners. This type of acquisition is not suitable for real-time systems where response time is mandatory. Fingerprints thus acquired are called “latent images”. Figure II.6-(e and f) show an inked and latent fingerprints.

- 2- Online acquisition: the fingerprint is acquired directly from the subject’s finger. This is achieved using an electronic fingerprint device (fingerprint reader). Live scan is an important property of modern AFIS’s which generally operate in real-time mode. The quality of the captured image is dependent on the technology used by the reader. Nowadays, there are several live-scan fingerprint technologies available that can be either optical readers, solid state readers or ultrasound readers (Krishan et al., 2012). The trend is to ensure good image quality, using small, fast technology with reduced cost. Some fingerprint images acquired from different readers are shown in Figure II.6.

Some readers’ technologies incorporate advanced algorithms to detect the presence of a finger on the surface of the scanner’s glass, the vitality of the finger’s subject, image compression and cryptographic algorithms for a secure communication.

II.4.2.2 Image quality assessment

The performance of the recognition system depends on the quality of the sensed image. A fingerprint with good quality tends to present a high contrast with clear ridge structure, whereas a poor quality fingerprint has low contrast with corrupted ridges.

When acquiring an image, several factors are having a negative impact on the quality of the image. These imperfections can be related to:

- 1- Reader's technology: it is related to the hardware technology and software algorithms embedded in the sensor used to capture the image. Resolution is the most important characteristic of the reader. Basically, most AFISs work on image resolution of 500dpi. Higher resolution, 1000 dpi, is needed in some applications. As shown in Figure II.6, quality of the sensed images differs from one reader to another.
- 2- State of the skin: the surface of the fingertip can be affected by the nature of the subject's occupation (dealing with acids, farmers, construction, etc.) as well as by aging (older people tend to have poor ridge structure than younger).
- 3- Environmental conditions: temperature and humidity have a direct effect on the fingertip surface. They can change the topography of the fingerprint and affect the reflection of the light. A dry fingertip results in low-quality fingerprint image with interrupted ridge structure, whereas a wet fingertip results in a saturated fingerprint with thicker linked ridges (Chikkerur, Cartwright, & Govindaraju, 2007).
- 4- Interoperability of the user: it is related to the manner that the user puts his finger on the scanner. High pressure results in high skin distortions whereas small contact of the skin with the glass surface results in a partial fingerprint.

All these factors may lead the subsequent steps to deal with erroneous features such as false ridge structures that later carry out spurious minutiae.

It is reported that roughly 10% of fingerprints manipulated can be classified as 'poor' images. Generally, a fingerprint image area can be divided into four regions (Hong, Wan, & Jain, 1998):

- 1- Background region: that corresponds to the surface of the scanner that is not covered by the finger. This region doesn't contain any ridge structure.
- 2- Clear region: ridges in such regions are well defined and quite distinguishable. Each ridge is well separated by two valleys and vice versa.
- 3- Recoverable region: ridges are noised with smudges, creases, and small links but their overall structure is still visible.
- 4- Unrecoverable region: the ridge structure is highly affected by noises and it is not visible. Ridges are linked together constituting smudged regions.

Figure II.7 shows two fingerprint images with labeled quality regions. These regions can be automatically classified according to the local contrast, orientation and frequency consistencies. These factors, joined with others, can define a *quality index* associated with a fingerprint image (Krishan et al., 2012).

It is essential to incorporate an enhancement module in any AFIS system. Such algorithms aim to alleviate the effect of the imperfection noises introduced during the acquisition step in order to improve the clarity of the ridges, and capture the maximum 'true' available ridge structure to allow detection of 'genuine' minutiae. Another task of the enhancement algorithms is to mark the unrecoverable regions as being of low quality that must be taken into consideration in the subsequent steps. Once these algorithms are adapted to the nature of the imperfections listed above, the optimal matching performances are soon obtained.

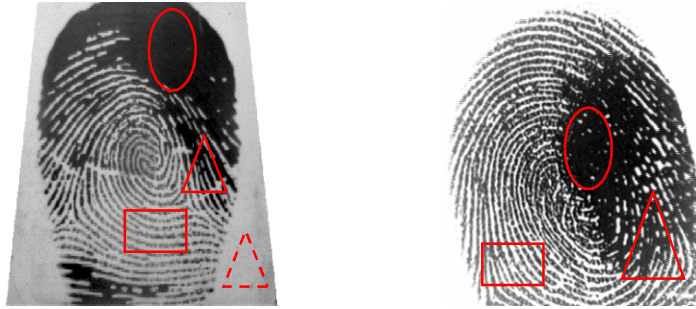


Figure II.7 fingerprint images with marked quality regions: circles for unrecoverable regions, rectangles for good quality regions, continuous triangles for recoverable regions and dashed triangles for background regions

II.4.2.3 Global features estimation

Global features refer to global level-1 characteristics consisting in orientation field, ridge frequency and singular points.

II.4.2.3.1 Orientation field estimation

An important characteristic of a fingerprint image is its orientation (or direction) field (OF) since many operations of fingerprint recognition depend on its accurate estimation.

An orientation can't be associated with a pixel by itself, instead, it is a property defined by its local neighborhood. The local ridge orientation at pixel $p(i,j)$ is defined as the angle θ that the ridge crossing through a small neighborhood forms with the horizontal axis. The angle θ ranges between 0° and π . The coding of all pixels' orientations yields the orientation image (or orientation map). This latter is of great importance in fingerprint recognition since it is implicated in ridge restoration and enhancement, singularities detection, fingerprint classification and matching.

The OF estimation methods proposed in the literature can be classified as being gradient-based approaches, filter-bank based approaches and model-based approaches (Figure II.8). The first approach is reported to be the most popular and the most accurate (Mei, Sun, & Xia, 2009). However, it is still a trade-off between a pixel-wise and block-wise choice. Block-wise OF starts from the assumption that pixels in a local neighborhood tend to share the same orientation. Consequently, block orientation can replace pixels orientations. Although this idea implementation is fast and robust to noise, it produces a low resolution OF. Furthermore, this

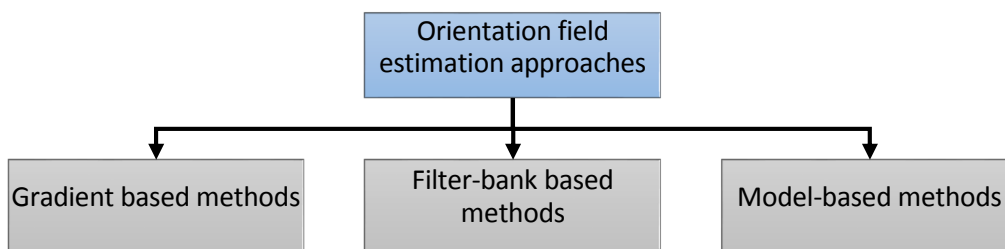


Figure II.8. Orientation field estimation approaches

underlying assumption is not always true since, in case of poor image quality, the obtained OF doesn't reflect the real form of the ridge structure. At the other hand, pixel-wise orientation field (POF) permits to get high resolution version of the OF, however, it is prone to noise and requires high computational time and space.

Gradient based methods rely on the derivation calculation of the input fingerprint image with respect to the two axis to establish the local orientation in a local neighborhood. The orientations are generally obtained by averaging the pixels gradients inside a block. However, since each ridge owns two contours, their gradients are in opposite directions; so, they cancel each other in the averaging result. To deal with this problem, (Kass & Witkin, 1987) proposed to double gradient angles so that an angle α and its opposite $\pi+\alpha$ become respectively 2α and $2\alpha+2\pi$ resulting in the same final value 2α which mathematically represents the squared gradients vector $[V_x(i,j), V_y(i,j)]$.

Most of the gradient-based methods rely on this idea that can be summarized as follows:

- 1- Calculate the horizontal and vertical Gradients G_x and G_y at each pixel $I(i,j)$,

$$\begin{aligned} G_x(i, j) &= \frac{\partial I(i, j)}{\partial x} \\ G_y(i, j) &= \frac{\partial I(i, j)}{\partial y} \end{aligned} \quad \text{II.1}$$

The horizontal Sobel operator used to calculate G_x is: $\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix}$ and the vertical Sobel operator used to calculate G_y is: $\begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$

- 2- Divide the input fingerprint 'I' into non-overlapped blocks of size $W \times W$,
- 3- The relation between the pixel gradients and heir squared gradients is defined by:

$$\begin{aligned} V_x(i, j) &= g^2 \cos 2\alpha = G_{xx}(i, j) - G_{yy}(i, j) \\ V_y(i, j) &= g^2 \sin 2\alpha = 2G_{xy}(i, j) \end{aligned} \quad \text{II.2}$$

where:

$$\begin{aligned} G_{xx}(i, j) &= \sum_{u=i-\frac{w}{2}}^{u=i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{v=j+\frac{w}{2}} G_x(u, v) * G_x(u, v) \\ G_{yy}(i, j) &= \sum_{u=i-\frac{w}{2}}^{u=i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{v=j+\frac{w}{2}} G_y(u, v) * G_y(u, v) \\ G_{xy}(i, j) &= \sum_{u=i-\frac{w}{2}}^{u=i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{v=j+\frac{w}{2}} G_x(u, v) * G_y(u, v) \end{aligned}$$

II.3

4- Calculate the local orientation of each block centered at $p(i,j)$ using this equation:

$$\theta(i,j) = \frac{\pi}{2} + \frac{1}{2} \operatorname{atan2} \left(\frac{V_y(i,j)}{V_x(i,j)} \right) \quad \text{II.4}$$

The value of θ , defined by the equation $\theta(i,j) = \frac{\pi}{2} + \frac{1}{2} \operatorname{atan2} \left(\frac{V_y(i,j)}{V_x(i,j)} \right)$ II.4, is the least square estimate of the dominant block orientation, which means that θ minimizes the sum of the squares of errors.

The quality of the obtained OF is dependent on the input fingerprint quality. The presence of noise, smudges or corrupted ridges has a negative influence on the local estimated orientations. The strength of this latter can be measured by computing their associated coherence. In fact, the ridge orientation typically exhibits small spatial variations between neighborhood pixels which tend to share the same orientations. The orientation coherence of a bloc centered at pixel $p(i,j)$ can be calculated as follows:

$$\operatorname{coh}(i,j) = \frac{\sqrt{(G_{xx}-G_{yy})^2 + 4G_{xy}^2}}{G_{xx}+G_{yy}} \quad \text{II.5}$$

which ranges between 0 and 1. The value 1 indicates an ideal coherence.

To get a high resolution version of the OF using the above method, one can use overlapped windows in such a manner that the step between two consecutive blocks is less than the block size. The full resolution corresponds to a step of 1 pixel which requires high computational time.

The dominant orientation so obtained still contains some inconsistencies. Therefore, most researches use additional regularization steps to get a more smoothed OF. (Hong et al., 1998) used a low-pass filter after converting the resulted orientations into a continuous vector:

$$\begin{aligned} \Phi_x(i,j) &= \cos(2\theta(i,j)) \\ \Phi_y(i,j) &= \sin(2\theta(i,j)) \end{aligned} \quad \text{II.6}$$

Applying averaging filter, or a Gaussian filter, of size 5x5 to both the components Φ_x and Φ_y yields the smoothed components Φ'_x and Φ'_y . The final estimated orientations can be obtained by the following formula:

$$OF(i,j) = \frac{1}{2} \tan^{-1} \left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)} \right) \quad \text{II.7}$$

(S. C. Dass, 2004) proposed a Bayesian approach to smooth the orientation field exploiting the Markov random fields theory. Some a priori models are proposed to enhance the OF.

(Wang, Hu, & Han, 2007) estimated the dominant orientation of a base block from its four overlapping neighborhoods. The best estimate is then selected from the least noise-affected neighborhood according to some reliability measures.

(Chikkerur et al., 2007) has proposed to probabilistically regularize a pre-estimated OF in the frequency domain using the STFT. They considered that the orientation θ is a random variable with probability density function $p(\theta)$. The expected value of θ can be given by

$$\theta = \frac{1}{2} \tan^{-1} \left(\frac{\int_{\theta} p(\theta) \sin(2\theta) d\theta}{\int_{\theta} p(\theta) \cos(2\theta) d\theta} \right) \quad \text{II.8}$$

A subsequent regularization step is introduced using a 3x3 Gaussian kernel averaging.

Another non-gradient based method is proposed by (Govindaraju, Shi, & Schneider, 2003) where the authors used chaincode contours representation that scans the binary image to trace the contours as an array of edge elements. This representation encodes principally the pixels coordinates and slopes in 8 directions. This permits later to estimate the orientation field in blocks of 15x15 pixels.

On the other hand, some global mathematical models are proposed in the literature to represent the coarse orientation estimates. (Barry G Sherlock & Monro, 1993) proposed a mathematical model, called zero-pole model, to represent the global topology of the FP orientation field. Although the zero-pole model can be used to synthesize a fingerprint orientation field or to predict the orientation flow in poor quality images, it can't completely describe a real fingerprint and it needs to know the locations and types of singularities in a ridge pattern in order to adjust the system parameters.

II.4.2.3.2 Ridge frequency estimation

Another intrinsic property of the fingerprint image is its ridges frequency (RF) or density. It deals with the dual alternation of the ridges and valleys in a local neighborhood. The local RF at pixel $[i, j]$, noted $f(i,j)$, is simply the number of ridges per unit length along a hypothetical segment centered at $[i, j]$ and orthogonal to the local ridge orientation θ_{ij} (Maltoni et al., 2009). Similarly to the orientation field image, a RF image is a matrix whose elements $f(i,j)$ determines the ridge frequency of a block centered at the location (i,j) . The RF is also a slowly varying property and hence is computed only once for each non-overlapping block of the image (Chikkerur et al., 2007). RF estimation is sensible to noise, image resolution, occurrence of minutiae and singular regions.

(Hong et al., 1998) proposed a method to calculate the frequency image in the spatial domain using the x-signature. They reported that valid regions frequencies range between 1/31 and 1/25 for 500 dpi images. First, the OF is estimated, then a 32x16 oriented window centered at a pixel $[i,j]$ is defined. The associated x-signature is calculated by accumulating the gray-levels of each column. $f(i,j)$ is then defined as being the average distance between two consecutive peaks. This method is sensitive to noise and lacks reliability in the singular regions and minutiae locations.

(Chikkerur et al., 2007) used the frequency domain to establish the frequency matrix using STFT. They considered that the frequency f is a random variable with probability density function $p(f)$. The expected value of f can be given by

$$f = \int_f p(f) df \quad \text{II.9}$$

The obtained RF is smoothed using a 3x3 Gaussian kernel applied only to the foreground region.

(Carsten Gottschlich, 2012) has further enhanced the (Hong et al., 1998)'s method by introducing curved Gabor filters which locally adapt their shape to the direction of the ridge flow.

(Chua, Wong, & Tan, 2015) modeled a fingerprint image using a 2D sinusoidal function in a local window of size 32x32. The estimated ridge distance is then found using a heuristic

II.4.2.3.3 Singularity detection

Chapter III is dedicated to fingerprint singular points detection where we discuss the importance of singularities in fingerprint recognition. A short state-of-the-art is given and a new method for singular points detection is proposed based on the orientation deviation features.

II.4.2.4 Fingerprint image enhancement algorithms

There are many algorithms proposed in the literature for fingerprint image enhancement. They range from the simplest pixel-wise operations to a complicated contextual filtering. The following is an outline of the commonly used methods to enhance fingerprint images.

Pixel-wise enhancement schemes are generally inherited from the fundamental image processing concepts, such as normalization, histogram equalization, mean and variance normalization, Wiener filtering (Gonzalez, 2009). These operations affect only the pixel itself and don't alter the ridge structure. They are generally used to prepare and pre-adjust an input fingerprint image for further enhancement processes.

Contextual filters are proposed as an alternative to the classical filters that operate on the entire image. Latter filters are suitable for images that are stationary. As the fingerprint has a non-stationary characteristic, any applied filter must adjust its parameters in function of the local context of the ridge structure that can be assumed as a sinusoidal surface. In general, contextual filters are dealing with context formed of local pixel orientation and frequency. They are defined using Fourier transform, Gabor filters, Wavelet transform, etc.

(O'Gorman & Nickerson, 1988) assumed that the local neighborhood frequency is constant for all pixels. They designed a bell-shaped mother filter from which are derived 16 directional-filters. First, the smoothed local ridge orientation is determined at each pixel location. After that, the enhanced image is obtained by convolving each pixel with the filter the most suitable for its local direction.

(B G Sherlock, Monro, & Millard, 1994) argued that local context calculation is prone to noise. To be effective, they convolved the entire image with eight directional filters of full image size using 2D Fast Fourier Transform (2DFFT). The eight inverse FFT, IFFT_i, $i=1..8$, of each resulted directional image is calculated. A pixel $p(x, y)$ in the enhanced image is affected the value of one pixel of the eight pixels $p_i(x, y)$ in IFFT_i, $i= 1..8$, that is closest to its direction.

(Wahab, Chin, & Tan, 1998) proposed a technique that starts by histogram equalization followed by orientation field regularization. It aims to replace a block direction by the most dominant direction in its neighborhood.

The local context used by (Hong et al., 1998) is defined in terms of local orientation and frequency. They convolved the image with a bank of Gabor filters whose parameters are tuned in function of the local context and defined by a sinusoidal plane wave modulated by Gaussian kernel. The algorithm starts by determining the local ridge frequency and orientation of each pixel. Then, a set of preselected filters is created a priori according to a set of orientations and frequencies bins. After that, each pixel is convolved with a filter that is closest to its local direction and local frequency. Thus, the enhanced image is created. Figure II.9-b shows an enhanced image using this technique.

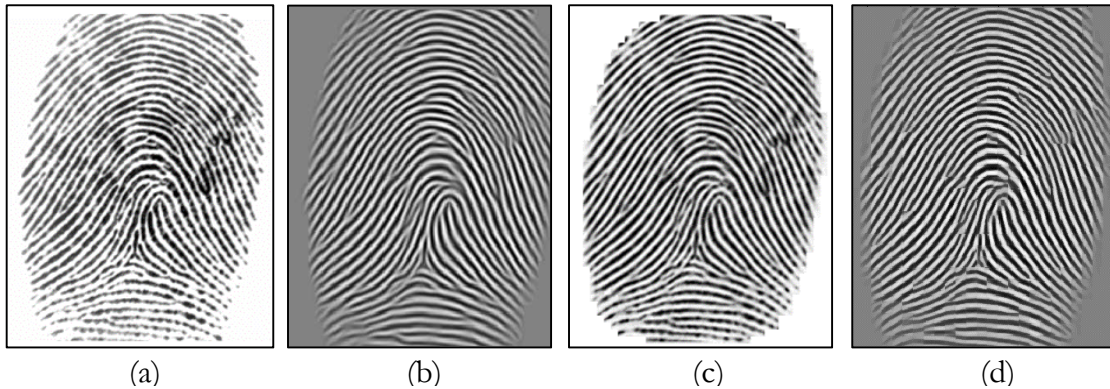


Figure II.9. original image and its enhanced images (a) original image, (b) enhanced image using (Hong et al., 1998) technique, (c) the corresponding enhanced image using (Willis & Myers, 2001) and (d) the corresponding enhanced image using (Chikkerur et al., 2007)

Having noted that Gabor filters are time-consuming since they are image dependent, (Willis & Myers, 2001) proposed a contextual filtering that does not require any prior information such as local ridges orientations and frequencies, instead, they are deduced from its FFT components. In fact, directional information of a specific block is contained in the magnitude of its FFT and the dominant frequency of the block FFT can be assumed to be its ridge frequency. The transform must be calculated on small blocks (32x32) so that these approximations be valid. The obtained FFT is multiplied by its power spectrum raised to some value k (e.g., 1.4). Thereafter, the enhanced image is obtained by applying the IFFT to each block. Figure II.9-c shows an enhanced image using this technique.

(Hsieh, Lai, & Wang, 2003) used a wavelet transform as a multiresolution analysis tool of the global texture and the local orientation and performed normalization followed by a simple directional filtering to eliminate broken ridges.

(Kamei, 2004) proposed two distinct filters in the Fourier domain: a frequency filter corresponding to ridge frequencies and a direction filter corresponding to ridge directions. The power of the images obtained by applying the above filters to the image defines an energy function for selecting features. The enhanced image is the features set that minimizes this function.

(Chikkerur et al., 2007) introduced an approach based on 2D short time Fourier transform (STFT) analysis to enhance the fingerprint image. They divided the image into small overlapped blocks, on each one the STFT (which is rapid and requires small space) is applied. The technique estimates probabilistically all the intrinsic properties of the fingerprints such as the foreground region mask, local ridge orientation as well as local ridge frequency. This technique seems to be more efficient than many others discussed before (Maltoni et al., 2009). Figure II.9-d shows an enhanced image using this technique.

(Khan, Khan, Mahmood, Abbas, & Muhammad, 2010) proposed a principal components analysis (PCA) based technique to enhance fingerprint images. First, the input image is decomposed into directional images to which PCA is applied. The reconstruction of these images yields the enhanced image.

(C Gottschlich & Schoonlieb, 2012) estimated the local orientation of the fingerprint ridge and valley flow and next performed oriented diffusion filtering, followed by a locally adaptive contrast enhancement step.

(Sutthiwichaiorn & Areekul, 2013) described an adaptive boosted spectral filtering algorithm in which they start by extracting the region of interest (ROI) by presegmenting the image. The ROI is analyzed by using an overlapped block-based STFT in the frequency domain that does not rely on preestimated local context. Blocks with lower quality are enhanced iteratively by propagating the good spectra from blocks with good quality.

II.4.2.5 Fingerprint segmentation

As all image processing applications, segmentation is a mandatory problem that must be rigorously resolved. Fingerprint segmentation refers to the process of decomposing a fingerprint image into two disjoint regions: foreground and background. The foreground consists in the useful ridge structure that constitutes the region of interest (ROI) whereas the background represents the region of the reader screen that was not covered by the finger during the acquisition, extended with the unrecoverable regions in which the ridge structure is ill-defined. The process is of great importance to the features-extraction steps since it speeds up the recognition process and avoids the apparition of false ridges that lead to false minutiae.

Segmentation methods can be either pixel-wised or bloc-wised (Yin, Zhu, Yang, Zhang, & Hu, 2007). The classification decision in the former methods affects only the underlying pixel, whereas it affects the whole block in the latter. In both cases, the classification decision is taken based on some established features. Depending on the method, the resulting image can be either a binary image (pixels values are either 1 or 0) or grayscale image where the background pixels are set to zero values.

(Mehtre & Chatterjee, 1989) combined the local orientation histogram with a local gray-scale variance to classify each pixel. In fact, a fingerprint exhibits a low gray levels variance in background regions and high variance in foreground ones. In addition, local orientation histogram presents prominent peaks in ridge structure regions.

(N. K. Ratha, Chen, & Jain, 1995) proposed a bloc-based method relying on the observation that the ridge structure exhibits high gray-levels variance in the direction orthogonal to the dominant direction of a block, whereas it is totally smooth in all directions in the background region.

(Hong et al., 1998) analyzed the shape formed by the local ridge structure using three features: amplitude, frequency and variance to classify each block as being recoverable or unrecoverable. If the number of the recoverable region is less than a threshold, the image is decided of low quality, hence, it must be passed through an enhancement step (presented in the Section II.4.2.3II.4.2.4).

(Bazen & Gerez, 2001) used three-pixel features, being the coherence, the mean and the variance. The three resulted planes was filtered with a Gaussian kernel. An optimal linear classifier, having the low computational complexity, is then trained for the classification per pixel, while morphology is applied as pos-tprocessing to obtain compact clusters and to reduce the number of classification errors.

Similarly, (Klein, Bazen, & Veldhuis, 2002) used four features being the gray mean, variance, gradient consistency and Gabor response, whereas the classification is performed using Hidden Markov Models (HMM) to create connected compact clusters.

(Alonso-Fernandez, Fierrez, & Ortega-Garcia, 2005) proposed to convolve each block with eight Gabor filters tuned to the estimated block frequency and orientation to a certain multiple of $\pi/4$. Foreground blocks have different Gabor responses while background ones tend to have similar values. To avoid border-effect between blocks, they used blocks of size $W \times W$ with an overlapping of $W/2$ pixels. Some additional heuristic constraints have been imposed in order to discard those blocks not suitable for the frequency estimation algorithm.

(Chikkerur et al., 2007) calculated for each block its local energy in the frequency domain. High energies overlap with foreground blocks, hence, thresholding leads to classifying each block. The threshold is automatically determined using Otsu's optimal thresholding technique. The resulting binary image is processed further to retain the largest connected component.

(Cavusoglu & Görgünouglu, 2008) proposed to use a directed mask that serves as a kind of directional low pass filter where the coefficients are obtained from a parabolic curve. The authors report a good execution time however the technique performs badly with oily images.

(Yang, Zhou, Yin, & Yang, 2010) described a K-means based segmentation method using 3-dimensional feature vector consisting of block-wise coherence, mean, and variance. Some posterior morphological operators are applied to enhance the results.

(Das & Mukhopadhyay, 2015) reported a pixel-wise segmentation scheme based on mathematical moments. A global threshold value is calculated from local standard deviations of a set of blocks. The relative local threshold values are derived subsequently to decide whether a pixel belongs to the foreground or background.

(Ferreira, Sequeira, & Rebelo, 2015) uses the fuzzy C-Means algorithm to segment the image. First, a block-wise range-filter is applied on the gray image; thereafter the FCM achieved to binarize the image along with the clusters are merged. Some morphological operations are then applied to establish the final foreground mask.

II.4.2.6 Features extraction

Most of the fingerprint recognition techniques are based on the level-1 features, in particular singular points, and level-2 features consisting in minutiae and ridges paths. These are the most important features that can be extracted from a fingerprint. However, a segmented fingerprint image in its gray-level format is generally not suitable to extract such discriminant features. Instead, most features extraction algorithms go through a process that consists of ridge extraction, followed by ridge thinning and minutiae extraction. Ridge extraction is essentially the step of binarizing the fingerprint image (Bolle, Senior, Ratha, & Pankanti, 2002).

II.4.2.6.1 Binarization

Binarization is the process of converting a segmented fingerprint image S from the grayscale range $[0..255]$ to the binary range $\{0, 1\}$. '1' labels indicate ridges whereas '0' values represent valleys and background. A good binarization method must: (i) improve the clarity of ridge structures of fingerprint images (ii) maintain their integrity, (iii) avoid introduction of spurious

structures or artifacts, and (iv) retain the connectivity of the ridges while maintaining separation between ridges (Govindaraju et al., 2003).

A simple and direct method to do so is to determine a global threshold th and affect the value '0' to all pixels having gray values lower than th and '1' to those higher.

$$B(x, y) = \begin{cases} 1 & \text{if } S(x, y) \geq th \\ 0 & \text{otherwise} \end{cases} \quad \text{II.10}$$

This technique results in a satisfactory binarized image if the original image is of good quality or it has been already enhanced, see Section II.4.2.3II.4.2.4. However, this approach encounters difficulties in the determination of such threshold th especially when the segmented image is characterized by different contrast and intensity regions. An effective solution to these problems is to adjust the threshold in function of the local context of the underlying pixel or block.

(N. K. Ratha et al., 1995) established a local profile along a directed window centered at a pixel $p(i, j)$. It consists of projection of the gray-levels in the direction orthogonal to the pixel's orientation. The obtained profile is smoothed by averaging local cumulated intensities. Pixels showing peaks in the profile are set to '1' along with their two neighboring pixels on each side. The remaining pixels are set to '0'.

Slight different from the (N. K. Ratha et al., 1995)'s method, (Tico, Onnia, & Kuosmanen, 2002) observed that the one-dimensional sequence obtained by collecting gray-level intensities of pixels located on a short segment orthogonal to the local ridge orientation has low and high values corresponding to pixels located respectively on the valleys and the ridges intersected by the segment. Hence, the sign of the second derivative of this sequence can be used to classify each pixel. The obtained binary image doesn't reflect the original ridge width.

(Wu, Shi, & Govindaraju, 2004) used an adaptive binarization method based on Otsu algorithm that clusters pixels into background and foreground.

(Liang, Bishnu, & Asano, 2005) proposed a linear time algorithm to eliminate noise and useless regions, which employs generalized and ordinary morphological operators based on Euclidean distance transform.

(Shaikh, Saeed, & Chaki, 2013) proposes a quantitative evaluation measure (confidence score) to be used for effective benchmarking of different binarization algorithms. The metric has been used to evaluate six different binarization techniques applied on fingerprint images.

(Reddy, Tiwari, Kaushik, & Gupta, 2015) and (Wahab et al., 1998) used a simple dynamic thresholding technique that affects '0' value to all pixels having a gray-level intensity higher than the average intensities in a 16x16 block.

If the input fingerprint image is of poor quality, some further regularization operations are applied to fill holes and eliminate possible spurious ridges, bridges and undesirable artifacts. Generally, mathematical morphology operations (Gonzalez, 2009) are well ready to be used for such purposes. Figure II.12-c shows a binarized segmented image using (N. K. Ratha et al., 1995) method.

II.4.2.6.2 Ridge extraction: thinning

Before undertaking the minutiae extraction step, the binarized fingerprint image has to be thinned. Thinning is the process of extracting ridge structure such that the ridge thickness is

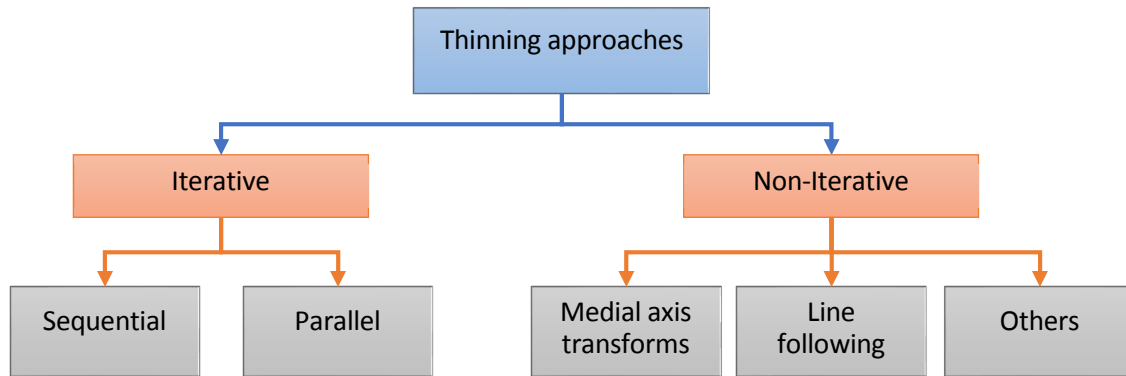


Figure II.10. Fingerprint image thinning approaches

reduced to 1 pixel. (Lam, Lee, & Suen, 1992) have defined four requirements that a good thinning algorithm should meet: 1) the resultant thinned image should be of 1 pixel width with no discontinuities, 2) each ridge should be reduced to its central line, 3) noise should be avoided, and 4) the final image doesn't accept any further thinning process.

Proposed thinning algorithms can be classified into iterative and non-iterative approaches (Lam et al., 1992). The former uses a template where a match in the image implies the deletion of the central pixel. The process is repeated iteratively until no match can be found. Iterative algorithms may be further classified regarding their implementation possibility as i) sequential thinning algorithms, and ii) parallel thinning algorithms as shown in Figure II.10. The non-iterative methods are not a pixel-wised, they produce a median line of the ridge independently of its width in one pass without examining all individual pixels. This approach seems to be faster but generally doesn't give satisfactory results.

(Baruch, 1988) proposed a thinning method based on line path following. A predefined window whose size grows or shrinks in function of the ridge width embraces the ridge. The ridge inside the window is replaced by its central line skeleton.

(Humbe, Gornale, Manza, & Kale, 2007) used mathematical morphology to erode ridges using eight specific structural elements. After thinning, some artifacts may occur such as superfluous spikes, breaks and dots. A subsequent refining step is applied to eliminate such spurious information.

(Golabi, Saadat, Helfroush, & Tashk, 2012) implemented three boxes of matrices tuned to thin ridges according to a specific direction: diagonal, horizontal and vertical directions. A fourth matrix is defined to deal with noise.

(Z. Li, Wang, & Zhang, 2013) has applied a Pulse Coupled Neural Network algorithm that iteratively skeletonizes a binary image by changing the load signals of pulse neurons. A direction-constraining scheme for avoiding fingerprint ridge spikes has been discussed.

(D. Li, Wu, & He, 2014) proposed a non-iterative thinning technique where they used the depth of each pixel to find the deepest points which will be only considered along with its neighboring points to determine the points that can be discarded.

Figure II.12-(d) shows a thinned fingerprint image.

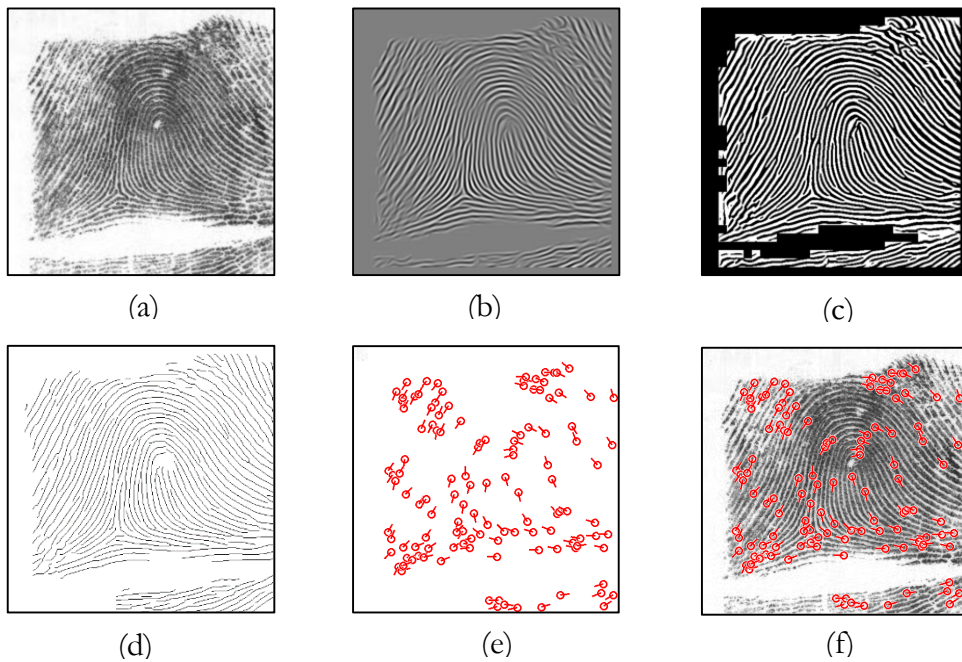


Figure II.12. Results of processing a fingerprint image, (a) original image, (b) enhanced image, (c) segmented and binarized image, (d) thinned image, (e) extracted minutiae, and (f) extracted minutiae superimposed on the original image

II.4.2.6.3 Minutiae extraction and filtering

Once the thinned image is calculated, minutiae extraction process is limited to a simple scan of the thinned image to verify the crossing number associated to each ridge pixel (black pixel). The crossing number associated with a pixel $p(I,j)$, noted $CN(p)$, is defined as being the number of black neighbor pixels. An ending minutia is defined as the pixel having $CN = 1$, whereas a bifurcation minutia is defined to have a CN of 3 (Figure II.11). A fingerprint image with its associated minutiae are shown on the Figure II.12-(e and f)

The location of the underlying pixel defines the 2D coordinates of the minutia. The minutia direction θ is defined as the angle that the ridge associated with the minutia makes with the horizontal axis. It can be simply deduced from the ridge OF value at that pixel, or calculated from the thinned image by selecting a point p at the K^{th} position ($K = 12$) of the minutia ridge (starting from the minutia m) and calculating the angle that the vector \overrightarrow{mp} makes with the horizontal axis.

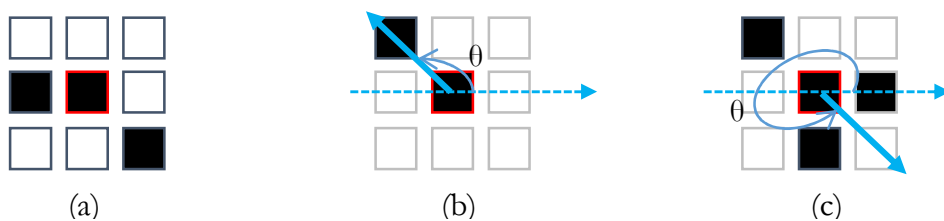


Figure II.11 crossing number configurations of a central pixel, (a) intra-ridge continuity, (b) ending minutia, (c) bifurcation minutia

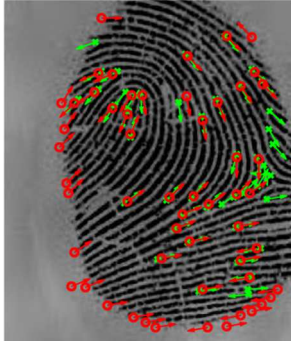


Figure II.13. Spurious and missed minutiae. Minutiae marked with green constitute ground truth. Detected minutiae are marked with red. Some genuine minutiae are missed, whereas most of the detected minutiae are spurious.

Note that the minutiae extraction process can be launched directly on the gray-level image avoiding the binarization-thinning process. (Maio & Maltoni, 1997) have proposed a ridge tracking technique by selecting local maxima gray-scale pixels along one direction. This results in an ϵ -pixel thick polygonal chain that permits to localize minutiae. The authors reported good results compared to the binarized-base techniques. A bit similar approach was undertaken by (Govindaraju et al., 2003) on binarized image as described in Section II.4.2.3.1.

(Anil K Jain, Prabhakar, Hong, & Pankanti, 2000) have exploited the observation that minutia point can be viewed as an anomaly in locally parallel ridges that can be captured with a bank of Gabor filters. An equivalent reasoning is to use the frequency image. Since minutia represents a discontinuity in a ridge, their locations are characterized by frequency transitions.

In (Fronthaler, Kollreider, & Bigun, 2008) parabolic symmetry is added to the local fingerprint model which allow to accurately detect the position and direction of a minutia simultaneously.

Minutiae extraction process reliability depends on the quality of the input image as well as on the reliability of each processing step. Unfortunately, the sequential nature of this process encourages the errors to be propagated. As a result, some genuine minutiae are missed and other detected minutiae are spurious. Missed minutiae are true minutiae that the extraction process was unable to detect, whereas spurious minutiae are false minutiae that do not exist in the input image but the extraction process has considered them as being genuine (see Figure II.13). (Peralta et al., 2014) reported that the number of added minutiae is much greater than the number of missed ones. Consequently, the initial minutiae set must be further processed to exclude spurious minutiae and to recover missed ones which, this task, constitutes the principal task of minutiae filtering methods. The advantages of these filtering methods on identification performance are clear: less time-processing and more matching accuracy.

Minutiae filtering methods can be divided into two approaches (Peralta et al., 2014):

- 1- Structural post-processing methods: these techniques are essentially heuristics based on some structural information of the underlying ridges and minutiae, including among others the length of the ridge, relative minutiae location, holes, bridges, etc. Based on this information, these techniques establish certain rules to discriminate between spurious and genuine minutiae and decide the new structures changes resulting from their removal (see Figure II.14). We find this scheme in (Hung, 1993; Jiang, Yau, & Ser, 2001). A similar technique was used by (F. Zhao & Tang, 2007) where the duality representation between ridges and valleys is exploited to detect such structures. For instance, some rules to detect spurious minutiae can be defined as follows:

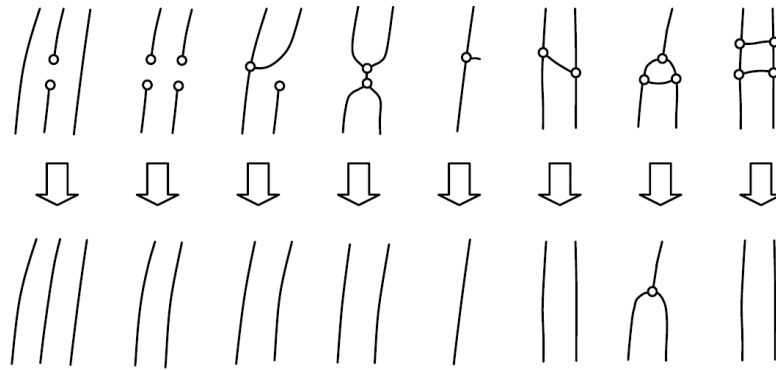


Figure II.14. Some common false minutiae structures and the new structures to which they will be reduced used by (Jiang et al., 2001)

- Existence of a large number of minutiae in a small neighborhood. This is a sign of corrupted region. Most of them must be discarded.
 - Two minutiae that are close to each other having opposite directions. This is a sign of fissured ridge. Both minutiae must be deleted.
 - Minutia at the border of the foreground region. This type of minutiae can be avoided by considering the negative thinned image.
- 2- Filtering based on gray-level: the gray scale levels in the local neighborhood of minutia are used to classify it as being spurious or genuine. (Kumar & Vikram, 2010; Maio & Maltoni, 1997) used neural networks to learn to filter minutiae. (Chikkerur, Govindaraju, Pankanti, Bolle, & Ratha, 2005) described two techniques to filter out spurious minutiae in which the system learns the difference between genuine and spurious minutiae neighborhood. The first approach is based on the response of the minutiae neighborhood to a bank of steerable wedge filters to be used in a special type of neural network to classify minutiae, whereas the second approach is based on the multi-resolution Gabor elementary functions responses to encode minutiae. A Bayesian classifier is then used to classify each minutia.

II.4.2.7 The ISO/IEC 19794-2 (2005) minutia template representation standard

The aim of the ISO/IEC 19794 standards (ISO/IEC19794-2:2005, 2005) is to standardize the biometric data interchange formats in order to guarantee the interoperability between biometric components in particular sensors, storage systems and matchers. Part 2 of these standards is related the concepts and data format representation of fingerprints based on the notion of minutia. It preconizes three data formats: record based, normal and compact format for use in smartcards.

Minutiae data to be saved spreads over 6 bytes: the 2D coordinates (X: 14bits, Y: 14bits), the direction (8bits), type (2bits) and minutia quality (8bits). Optional extended data format for encoding: ridge counts, core and delta locations is possible.

II.4.2.8 Matching

Matching is the most important step in an AFIS. It has received a lot of attention by researchers due to its key role in recognition. The procedure consists of comparing two fingerprints

represented by their templates and returning a similarity score that indicates to which extent the two fingerprints are similar. One template is generally stored in a database, noted T, and the other consists in the input query features, noted Q, that the system has to identify.

Fingerprint matching is not a trivial task, it is very difficult to match two impressions of the same finger and reliably establish the corresponding features because of the following factors (Tian, Zhang, & Cao, 2015):

- 1- Existence of several transformations between the two impressions. Linear transformations consist in translation, rotation and scale which are caused by differential finger placement with respect to the sensor surface during different acquisitions. Non-linear transformations are related to the skin distortions caused by the differential finger pressure exerted by the user during different acquisitions.
- 2- The quality of the impressions might differ between different acquisitions (refer to Section II.4.2.2)
- 3- The feature extraction process may deliver erroneous features and miss genuine features from both impressions.
- 4- There may be small overlapped region between the two impressions (some common features are lost from both impressions)
- 5- Small inter-user and large intra-user variabilities between two impressions could mislead the comparison decision.

A general matching road-map is to bypass all the cited difficulties and determine the best (optimal) alignment that permits a template Q to overlap the template T; this is equivalent to determine the translation, rotation and scale parameters to optimally superimpose the two fingerprints.

The state-of-the-art in fingerprint matching can be divided into three main approaches (Maltoni et al., 2009):

- 1- Correlation-based approach: both templates consist in raw data (pixels) to be compared in terms of gray-levels.
- 2- Minutiae-based methods approach: template features consist in minutiae. The goal is to maximize the number of paring minutiae. This approach inspires its comparison principles from the manner that the expert examiners do in manual matching.
- 3- Non-Minutiae feature-based matching: in low-quality fingerprints, minutiae lose their reliability. In such a case, some non-minutiae features, such as pores, ridge contours, orientation field and frequency map, etc. could be used to consolidate the matching results.

It has been reported by many researches that minutiae-based approach is the most reliable and the most used in automatic fingerprint recognition (Krishan et al., 2012). Subsequent subsections are interesting only in this approach. Further reading about the other approaches can be found in (Maltoni et al., 2009).

II.4.2.8.1 Minutia-based matching principle

Let T consist in M minutiae, $T = \{m_i^t\}_{i=1,M}$, and Q in N minutiae, $Q = \{m_j^q\}_{j=1,N}$; each minutia is principally described in its 2D coordinates (x, y), its direction $\theta \in [0, 2\pi[$ and eventually its type t(0: bifurcation, 1:ending). We suppose, without loss of generality, that $M > N$.

A minutia $m_i^t(x_i^t, y_i^t, \theta_i^t)$ in T is said to be in matching with a minutia $m_j^q(x_j^q, y_j^q, \theta_j^q)$ in Q if:

$$\begin{cases} ED(m_i^t, m_j^q) = \sqrt{(x_i^t - x_j^q)^2 + (y_i^t - y_j^q)^2} \leq th_{ed} \\ \text{and} \\ \lambda(m_i^t, m_j^q) = \min(|\theta_i^t - \theta_j^q|, 2\pi - |\theta_i^t - \theta_j^q|) \leq th_\theta \end{cases} \quad \text{II.11}$$

$ED(.,.)$ represents the Euclidean distance between two points and $\lambda(.,.)$ is their minimal directional difference. The thresholds th_{ed} and th_θ are tolerance boxes introduced to substitute for the deformations caused by the non-linear skin-distortion and displacements errors introduced by the features extraction algorithm.

The alignment of the two fingerprints can be recovered by finding the parameters of the translation Δx and Δy as well as the rotation angle α (scaling factor is supposed to be 1). Since there is a large number of such transformations, the adequate parameters can be determined by transforming the minutiae of Q in the coordinate system of T and selecting those parameters that optimize the distance between T and the transformed Q.

Formally, let $\tilde{Q} = \{\tilde{m}_j^q(\tilde{x}_j^q, \tilde{y}_j^q, \tilde{\theta}_j^q)\}_{j=1,N}$ be the transformed template Q using the parameters Δx , Δy and α .

$$\begin{cases} \begin{bmatrix} \tilde{x}_j^q \\ \tilde{y}_j^q \end{bmatrix} = \begin{bmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} x_j^q \\ y_j^q \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \\ \tilde{\theta}_j^q = \theta_j^q + \alpha \end{cases} \quad \text{II.12}$$

Hence, we define a Boolean function *align* to designate that a minutia m_i^t from T is aligned with a minutia m_j^q from Q:

$$align(m_i^t, \tilde{m}_j^q) = \begin{cases} 1 & \text{if } (ED(m_i^t, \tilde{m}_j^q) \leq th_{ed}) \text{ and } \lambda(m_i^t, \tilde{m}_j^q) \leq th_\theta \\ 0 & \text{otherwise} \end{cases} \quad \text{II.13}$$

The optimal transformation values $\overline{\Delta x}$, $\overline{\Delta y}$, and $\overline{\theta}$ correspond to the parameters that maximize the alignment of the two sets T and \tilde{Q} :

$$\begin{aligned} & \text{Maximize}_{\Delta x, \Delta y, \alpha} (\sum_{i=1}^N align(m_i^t, \tilde{m}_{Im(i)}^q)) \\ & \text{subject to :} \\ & \forall i = 1..M, k = 1..N, i \neq k \Rightarrow Im(i) \neq Im(k) \text{ or } Im(i) = Im(k) = NULL \end{aligned} \quad \text{II.14}$$

where $Im(.)$ is a pairing (mapping) function that associates to each minutia index in T an index in \tilde{Q} (so in Q). The pairing is subject to the conditions that each minutia in T must be paired **at most** with one or no minutiae in Q and vice versa.

The matching problem is not as easy as it just has been viewed, the determination of the optimal parameters $\overline{\Delta x}$, $\overline{\Delta y}$, and $\overline{\theta}$ is a hard problem (Maltoni et al., 2009) that must be undertaken carefully. In fact, once a minutia m_i^t is paired with $m_{Im(i)}^q$ according to a certain transformations does not mean that the two minutiae are true pairs since the decision was taken based only on the minutiae features independently of its local context. Since the relative transformation between two fingerprints is unknown in advance, the correspondence between minutiae is very ambiguous and each minutia of one fingerprint can be matched to any minutiae of the other fingerprint (Feng, 2008). To let the matching be more reliable, additional local information, called minutia descriptor, are added to describe each minutiae based on which the comparison is achieved. Chapter IV gives more details about local-minutia based matching and proposes a short exploration of the common used matching methods.

II.4.3 Performance evaluation

As any biometric identification system, AFIS performance must be subject to be evaluated. The task implies to define some performance criteria as well as fingerprint benchmarks.

The performance criteria are those defined in the Section I.3. Most of them are used in principal fingerprint competitions such as FVC competitions (Cappelli, Ferrara, Franco, & Maltoni, 2007; Maio, Maltoni, Cappelli, Wayman, & Jain, 2002a, 2002b, 2004) based on which fingerprint verification algorithms are ranked.

As for fingerprint benchmarks, there are many public fingerprint databases that can be used to assess the performance of a fingerprint identification system. The most used are the FVC databases.

II.4.3.1 FVC Databases

FVC (Fingerprint Verification Competition) is the largest competition for fingerprint verification algorithms organized by the University of Bologna, Italy, with the conjunction of other American and European universities. It has been organized in 2000, 2002, 2004 and 2006 (Cappelli et al., 2007; Maio et al., 2002a, 2002b, 2004). In every competition, four new fingerprint benchmarks were issued from different scanners technologies and provided to evaluate the candidate fingerprint matching algorithms. Each database has 110 fingers (150 for FVC 2006) and 8 impressions per finger (12 for FVC 2006). Table II.2 resumes some global characteristics of each database.

Table II.2. Some global characteristics of the FVC databases

Competition	Database	Number of impression	Sensor type	Size	Resolution
FVC-2000	DB1	110x8	Optical Sensor	300 × 300	500 dpi
	DB2	110x8	Capacitive Sensor	256 × 364	500 dpi
	DB3	110x8	Optical Sensor	448 × 478	500 dpi
	DB4	110x8	Synthetic Generator	240 x 320	≈ 500 dpi
FVC-2002	DB1	110x8	Optical Sensor	388 × 374	500 dpi
	DB2	110x8	Optical Sensor	296 × 560	569 dpi
	DB3	110x8	Capacitive Sensor	300 × 300	500 dpi

	DB4	110x8	SFinGe v3.0	288 x 384	≈ 500 dpi
FVC-2004	DB1	110x8	Optical Sensor	640 × 480	500 dpi
	DB2	110x8	Optical Sensor	328 × 364	500 dpi
	DB3	110x8	Thermal sweeping	300 × 480	512 dpi
	DB4	110x8	SFinGe v3.0	288x 384	≈ 500 dpi
FVC-2006	DB1	150x12	Electric Field sensor	96 x 96	250 dpi
	DB2	150x12	Optical Sensor	400 x 560	569 dpi
	DB3	150x12	Thermal sweeping Sensor	400 x 500	500 dpi
	DB4	150x12	SFinGe v3.0	288 x 384	≈ 500 dpi

Other databases benchmarks exist such as the NIST databases (NIST_DB, n.d.) and Michigan State University (MSU) Database (Anil K Jain, Prabhakar, & Ross, 1999),

II.5 Conclusion

Although fingerprint has been known for centuries, its scientific use goes back to the beginning of the 20th century. The automation of the fingerprint recognition started in the early of 1970s. Fingerprint is, and it will remain, the most used modality in individual identification due to its acceptability, maturity as well as to its inexpensive cost technology.

A fingerprint can be analyzed at three levels, level-1 depicts the global characteristics inherent to the orientation pattern of the ridge structure, this latter can be viewed to have a sinusoidal form so frequencies. The ridge friction tends to have a global shape determined by special points called singular points. Fingerprints can be classified according to their shapes into five prominent classes. Level-2 refers to local characteristics exhibited by the ridge path. Special discontinuities in the ridge path, called minutiae, are the most important traits based on which individuals can be identified. The ridge path itself is the second local characteristic that guarantees the individuality. Level-3 features are related to finer details brought by fingerprints at a higher resolution. These consist in pores and ridge contours that are sources of individuality once they are reliably detected.

Studies on fingerprint individuality are limited and the issue is still open; some questions are still being asked especially about the sufficient number of features (minutiae for example) to decide for the perfect matching.

Automatic fingerprint identification system intelligence is generally inspired from the manner that human experts manipulate latent fingerprints. Since their creation, they have been widely used in many applications especially where security is of major concerns.

Fingerprint identification system is mainly a minutiae-based process that goes through acquisition, enhancement, segmentation, features extraction and matching steps. Although the literature is abundant in each stage, and AFIS systems do quite well, still some concerns need further improvements.

In the next chapter, we will get into an important issue in fingerprint features extraction concerning singularities detection where we propose an efficient detection algorithm based on orientation deviations features.

Chapter III.

Fingerprint singular points detection

Traditionally, expert examiners used singular points locations (cores and deltas) to visually classify and align fingerprints. The automation of such process to accurately locate singular points in reasonable time is an important factor in fingerprint recognition systems.

In this chapter, we describe an accurate algorithm to detect singular points (SP) in fingerprint images.

This chapter is organized as follows: Section III.1 gives the Henry-based definition of singular points. In Section III.2, some challenging tasks related to SP detection are highlighted to give thereafter a short state-of-the-art in SP detection. The proposed singular point detection algorithm scheme is described in details in Section III.3. Experimental results and comparative studies are given in Section III.4.

III.1 Singular points

Fingerprint is the most reliable identification biometric modality. As an image, a fingerprint (FP) is an oriented texture pattern determined by interleaved ridges and valleys. At the global level view, ridges often run smoothly in parallel but show one or more regions where they assume distinctive shapes characterized by high curvature (Maltoni, Maio, Jain, & Prabhakar, 2009) called singular regions (SR). At the local level, the ridge pattern presents local discontinuities caused by sudden broken ridges or merged ridges called minutiae points. Minutiae points are very distinctive features and therefore they are suitable for person identification while the singular regions information is used as auxiliary features to fingerprint pre-alignment. Their importance appears particularly in fingerprint classification and database information retrieval.

Singular regions are characterized by special points, called singular points (SPs), where the curvature is higher than normal and the direction of the ridge changes rapidly. There are two types of SPs. The first is core point, and is defined as the topmost point of the innermost curving ridge. The second is delta point, and is at the center of a triangular region, where three different ridge flows meet (E. R. Henry, 1990). For fingerprints that do not contain core or delta points (such as arch-type fingerprints), the SP is usually associated with the point of maximum ridge line curvature (Maltoni et al., 2009). The number of singular points in a full fingerprint varies from 1 to 4. Figure III.1 illustrates a typical fingerprint with one core and one delta point.

Singular points have been efficiently exploited in fingerprint modelling (Barry G Sherlock & Monro, 1993), classification (Cappelli, Lumini, Maio, & Maltoni, 1999; L. Wang & Dai, 2007), identification (Jain, Prabhakar, Hong, & Pankanti, 1999) and template securing (Belguchchi,

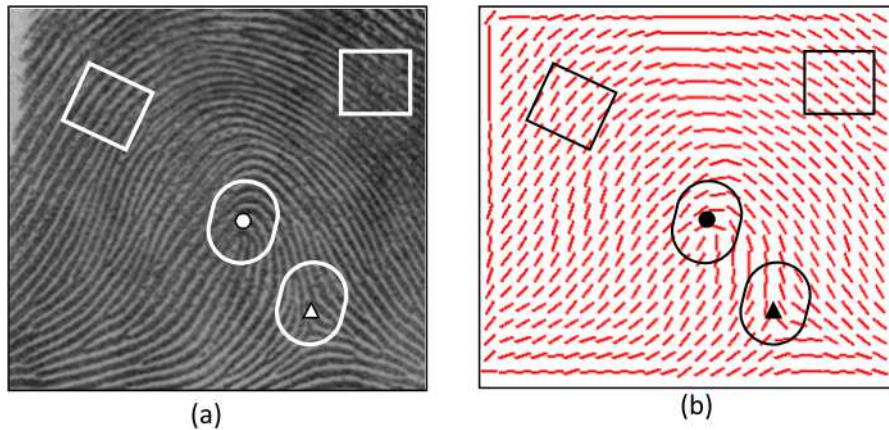


Figure III.1. Fingerprint ridge pattern with marked singular regions and singular points. (a) Core point marked with circle; delta point marked with triangle. (b) The associated estimated orientation field showing samples of singular and normal regions: normal-region sample marked with rectangles manifesting smooth parallel pattern in particular direction. The variation of the orientation field is very low; Singular regions marked with ovals showing inconsistent oriented pattern. The variation of the orientation field is very high.

Cherrier, Rosenberger, & Ait-Aoudia, 2013; Das, Karthik, & Chandra Garai, 2012; Quan, Fei, Anni, & Feifei, 2008).

III.2 Singular points detection: challenges & algorithms

It is essential to accurately determine singular points locations within small bounding boxes. However, the design of such detection algorithm encounters many challenging problems such as:

- 1- Poor quality of the acquired image due to noise and some corrupted regions.
- 2- Limited size of the acquired image resulting in partial or total absence of singularities.
- 3- Rotation of the FP image.
- 4- Location of SP at border of the fingerprint area.
- 5- Computational cost.

Most of the proposed methods to detect singular points in fingerprint images are based on the orientation field (OF) (Maltoni et al., 2009). They can be roughly classified into two approaches: local-pattern analysis or global-pattern analysis (Figure III.2).

The local-pattern analysis based approach exploits some topological properties manifested by the singular points in the OF at a local level of a pixel. This is possible using the local directional histogram (Srinivasan & Murthy, 1992), the Poincaré index (PI) (Jain, Prabhakar, Hong, & Pankanti, 2000; Klein, Bazen, & Veldhuis, 2002), the orientation consistency (Zacharias & Lal, 2013) or the shape of the directional pattern around the singular points (Park, Lee, Smith, & Park, 2006).

The global-pattern based approaches start from the fact that the overall pattern of the ridge-valley is heavily influenced by the existing singularities. Many works exploit this idea including

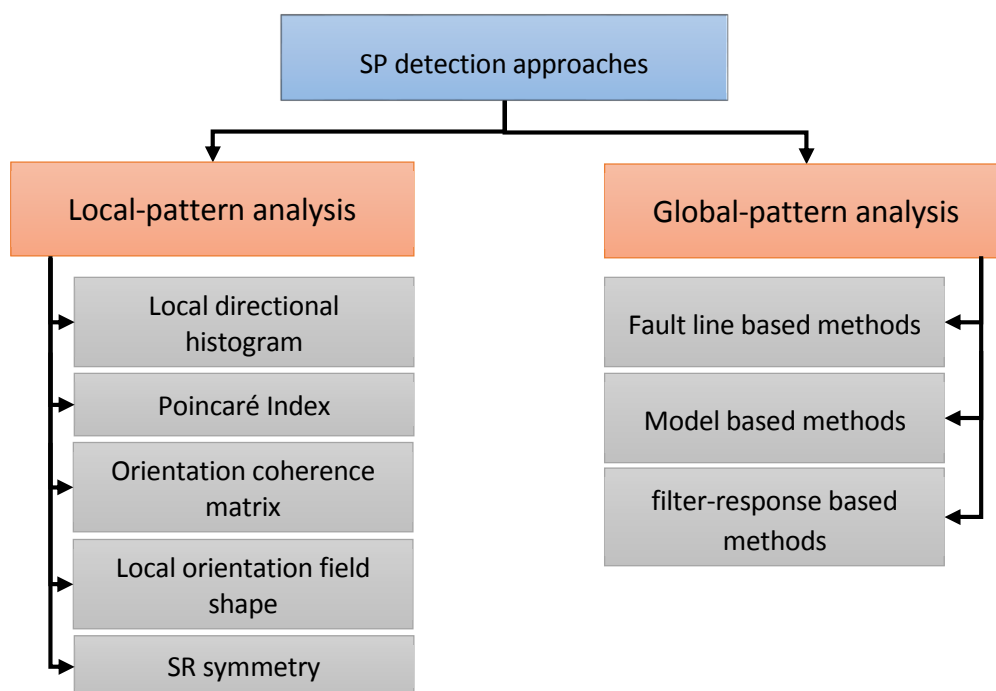


Figure III.2. Orientation field estimation approaches

the fault-line based methods (Cappelli et al., 1999) (Huang, Liu, & Hung, 2007), model-based methods (Barry G Sherlock & Monro, 1993) and filter-response based methods (Weng, Yin, & Yang, 2011).

(Srinivasan & Murthy, 1992) is one work based on local-pattern analysis. It uses a local directional histogram of the orientation field to detect some structural features. Thus, singular points are characterized by locations where the histogram does not show a clear prominent peak.

Poincaré index (PI) is the most dominant technique in this field. It relies on the fact that the difference accumulation of the gradual orientations over a closed curve has special values for singular and normal points. The PI based methods have the advantage of being simple, robust to image rotation and can obtain the type of each detected singular point. However, besides having problem when the SP is near the border, PI based-methods are very sensitive to noise and behave badly when images have poor quality generating a high false alarm rate. (Bazen & Gerez, 2002) proposed an improved version of the PI involving the Green's theorem, while (J. Wang, Olsen, & Busch, 2014) used a series of pattern-based filters to eliminate false singularities. Usually, the PI is applied as a post-processing step to filter out some spurious SPs from a candidate singular points set (Cappelli et al., 1999; Kekre & Bharadi, 2010; Weng et al., 2011).

(Cappelli et al., 1999) used the coherence metric, which is a measure that indicates how well the orientations in a neighborhood are pointing in the same direction, to distinguish between singular and normal regions characterized by low and high coherence values respectively. Some problems appear when the fingerprint contains singularities close to each other.

A similar work was proposed by (Zacharias & Lal, 2013) using an enhanced consistency metric.

(Park et al., 2006) examined the shape of the directional field at a local neighborhood of a pixel to check if it verifies predefined rules established for each singular point type. This method has

the advantage to detect all types of singular point with their locations and orientations but it is sensitive to noise and partial fingerprints.

Symmetry of the pattern structure exhibited by the singular regions has been exploited by (Nilsson & Bigun, 2002) in multi-resolution representation of the complex orientation field on which they applied two tuned filters. Thresholding the response of the filters determines the SP locations. Being robust to noise, this method is threshold-dependent; lower thresholds rise spurious SP candidates. This method has been more enhanced by (Chikkerur & Ratha, 2005).

On the other hand, global-pattern based methods are slight different from the above-described methods. For example fault line based methods try to partition the OF into homogenous orientation regions. (Cappelli et al., 1999; Huang et al., 2007) showed that the inner boundaries of these regions (called fault lines) coincide with the singularities locations. They converge to the core point and diverge from delta-point. Being dependent on the segmentation method applied, these methods find more difficulties when a partial fingerprint is submitted.

(B G Sherlock, Monro, & Millard, 1994) proposed a mathematical model, called zero-pole model, to represent the global topology of the FP orientation field. Singularities can be detected using adequate parameters. Although, the zero-pole model can be used to synthesize a fingerprint orientation field, it can't completely describe a real fingerprint. This model has been exploited by (Weng et al., 2011; Zhou & Gu, 2004) in combination with the Hough transform and Poincaré-Index to extract singular points.

III.3 Proposed Method

Hereafter, we describe an efficient method to extract singular points. It is based on the calculation of the Orientation-Deviation (OD) feature which describes more completely the topological structure surrounding a pixel. This feature has discriminant properties for each singular point type as well as for normal points. Thus, singularities are defined as locations where the orientation field energy, calculated over their OD-based features, is high provided that they satisfy the OD-based properties.

The proposed algorithm has the ability to detect accurately the classical singularities (core and delta) as well as the arch-type SP. It is more robust to noise, less sensitive to partial fingerprint and location of singularities at borders. The experimental results and the comparative study conducted on the public database FVC2002 DB1 and DB2 (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002) show that our method is more reliable, with better false alarm rate and detection rate, than many works in the literature known to be efficient in detecting singularities.

This work has two main merits:

- (1) Proposition of the OD-based feature that manifests topological properties highly correlated with underlying point type.
- (2) Extension of the Poincaré index to be defined on the OD space as a pair of two values that can detect singularities with their types.

III.3.1 Principle

The ridge flow in a fingerprint determines an oriented textured image that can be divided into two distinct regions: (1) regions characterized by pseudo-parallel ridge pattern determining

smooth texture, oriented at a particular direction called normal regions (NRs). The orientation field (OF) in such regions manifests usually low spatial variation; (2) regions with condensed ridge pattern with anisotropic texture directions called singular regions (SRs). Singular points are located inside SRs and characterized by pixel locations where the spatial variation of the OF, over local neighborhood, is higher than normal (see Figure III.1). This observation can be exploited to design an efficient SP detection algorithm that goes upon three main steps: (1) design an efficient pixel-wise feature that can robustly capture the OF structure details surrounding a pixel; (2) propose a good metric that efficiently measures the OF variations at a pixel based on its extracted features, and (3) accurately detect SPs with correct information (genuine SPs, types and orientations). Figure 2 shows the flowchart of the proposed algorithm. The following subsections give more details about each step.

III.3.2 Orientation field estimation

Most of the available SP detection methods are based on the orientation field (OF). Their performances depend on its accurate calculation. The OF estimation methods proposed in the literature are discussed in Section II.4.2.3.1. Gradient-based approach is reported to be the most used and the most efficient. However, it is still a trade-off between a pixel-wise and block-wise choice. Pixel-wise orientation field (POF) permits more accurate SP detection location but it is sensitive to noise, thus, cannot avoid false detections. Block-wise OF generates less spurious detections with low computational cost but the detected SPs are generally shifted from their real positions and lacks reliability in detecting close singularities.

In this work, we implement a modified version of the method described in (Ratha, Chen, & Jain, 1995), which is a block-wise OF. This method captures reliably the dominant direction of the ridge flow over a pre-defined sized block and performs an acceptable directional-variance based

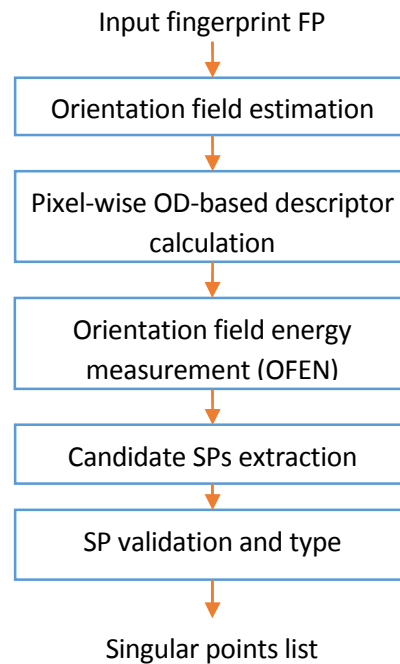


Figure III.3. The flowchart of the proposed method

segmentation. First, the input image is denoised using a Gaussian filter $g(0, \delta_g)$. After that, the gradient of the resulted fingerprint is calculated using a Sobel operator that permits estimating the local orientation of each block, of size $W \times W$. Since this estimation is prone to noise, the calculated OF is converted to a continuous vector field, by doubling the orientation, to be smoothed after by a low-pass filter yielding the final OF (Hong, Wan, & Jain, 1998). Finally, the input image is segmented by calculating the grey-level variance δ^2 in a direction orthogonal to the orientation field in each block. Only the blocs having a variance greater than a threshold δ_{th} are retained as foreground.

To make a compromise between the pixel-wise orientation field and the block-wise orientation field in term of computation cost and accuracy, we choose the block size W to be equal to the average ridge width τ .

III.3.3 Pixel-wise Orientation deviations based descriptor

We propose to describe a pixel in the input image by implying the information brought by the orientation field surrounding its location as indicated in (Tico & Kuosmanen, 2003). Formally, let $p(x, y)$ be a pixel in the segmented image at location (x, y) with orientation θ_p . The descriptor of p consists of a set of sampling points taken from circumferences of a set of circles centered at p with different radius. Let L indicates the number of circles C_1, C_2, \dots, C_L with respective radii r_1, r_2, \dots, r_L . Each circle C_i comprises K_i sampling points $p_{i,1}, p_{i,2}, \dots, p_{i,K_i}$ equally distributed on its circumference (Figure III.4). Taking the pixel p as origin and its direction as the positive direction of x axis, the starting point $p_{i,1}$ is located on the x axis. Let $\theta_{i,j}$ ($i = 1..L, j = 1..K_i$) designate the orientation values corresponding to each sampling point $p_{i,j}$. We define the orientation deviation (OD) of the sampling point $p_{i,j}$ with respect to p , denoted $\Theta_{i,j}$, as follows :

$$\Theta_{i,j} = \begin{cases} \theta_{i,j} - \theta_p - \pi & \text{if } (\theta_{i,j} - \theta_p) \geq \pi / 2 \\ \theta_{i,j} - \theta_p + \pi & \text{if } (\theta_{i,j} - \theta_p) < -\pi / 2 \\ \theta_{i,j} - \theta_p & \text{otherwise} \end{cases} \quad \text{III.1}$$

The OD-feature measures how much the associated sampling point differs in orientation with its central point. Thus, the set of all the OD-features of all the sampling points can be organized to describe more completely the neighborhood structure of p . This set constitutes the descriptor of p , denoted $D(p)$, as indicated by the Eq. (III.2).

$$D(p) = \left\{ \left\{ \Theta_{i,j} \right\}_{j=1}^{K_i} \right\}_{i=1}^L \quad \text{III.2}$$

The OD-based descriptor characterizes the pixel location with respect to the fingerprint pattern by capturing the spatial arrangement of pixels orientations in its local pattern. It is important to note that the presented descriptor is defined on the input image at the pixel-level. This property offsets the bias generated by the bloc-wised nature of the OF and, thus, ensures high accuracy detection of the SPs. Furthermore, the OD based descriptor presents some advanced topological properties; some of them are presented in the Section III.3.4.3. The most useful one consists in its intra-pattern distinctive information that can classify each pixel in the input FP as belonging to an NR or SR region. The next subsection confirms this claim by analyzing the OD-feature distribution.

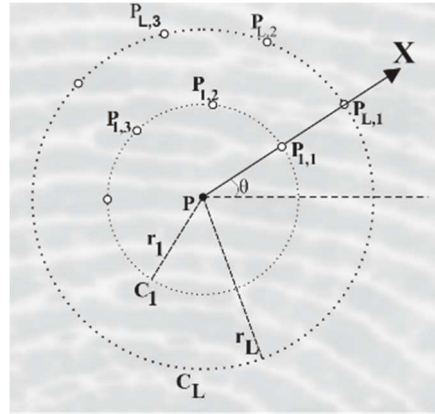


Figure III.4 Pixel-wise orientation-deviation based descriptor

III.3.3.1 Orientation deviation distribution analysis

Figure III.5 shows the empirical distribution of the absolute values of orientation deviations, $|\Theta_{ij}|$, in both NR and SR classes. The test has been established by selecting 100 fingerprints from the public database FVC2002 db1 (one impression for each finger). Each fingerprint contains one or more singularities (core, delta and arch-type SP). First, inside each fingerprint we located manually the singular points and some other points that belong to normal regions. Then, the descriptor in Eq. III.2 was calculated for each identified point.

The plots point out that the OD distribution is highly correlated with the underlying class. In fact, the histogram of the orientation deviations in the NR (Figure III.5) shows that more than 97,3% of the sampling points converge to small values in the interval $[0.. \pi/9]$ with higher density near 0° which is consistent with the fact that the local pattern in the NR class exhibits low orientation field variations. On the other hand, the histogram of SR region shows that more than 82,36% of the sampling points have higher values lying outside the interval $[0^\circ.. \pi/9]$ distributed, almost uniformly, over all possible values in the interval $[0^\circ, \pi/2[$. This indicates higher spatial variations of the orientation field in the SR class.

Based on these behaviors of the OD-feature distribution, the defined descriptor can constitute a robust feature to classify each pixel p as belonging to one of the two classes NR or SR provided that a good orientation field variation measure has been defined over $D(p)$.

III.3.4 Singular point detection

The singular points detection process can be summarized in the following steps:

- i) Each pixel is assigned an energy value that measures the local spatial variations of the OF around its local neighborhood, derived from its OD-based descriptor,
- ii) Classify each pixel as belonging to NR or SR regions. Pixels with high energy values constitute singular regions.
- iii) Candidate singular points are indicated with pixel locations where the energy function manifests local maxima.

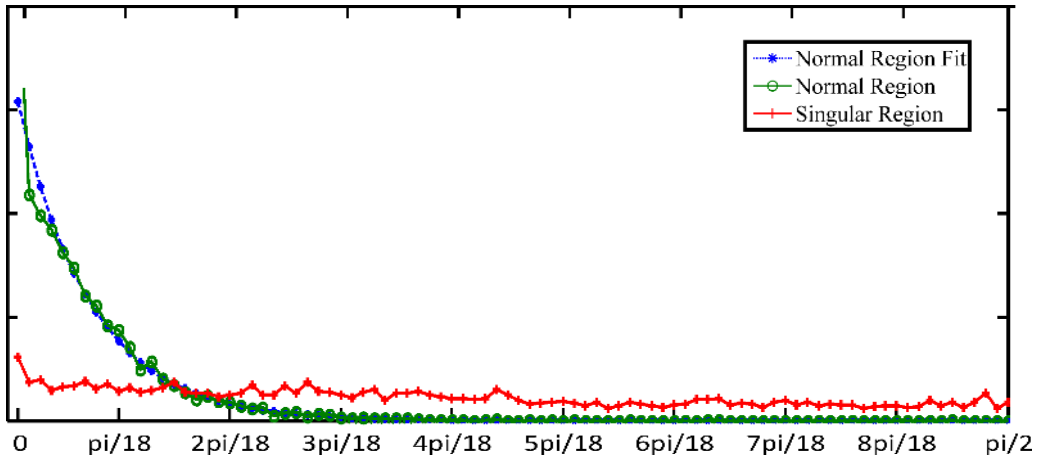


Figure III.5. Orientation deviations distribution in both normal and singular region.

- iv) Filter out spurious SPs and keep genuine ones with their information (location, direction and type).

The following sub-sections give more details about each step.

III.3.4.1 Orientation field energy measure

We define the orientation field energy measure associated to a pixel p (called $OFEN(p)$) as a function that measures the degree of variation of all attributes of its OD-descriptor $D(p)$ as an indicator of the spatial variation of the orientation field surrounding the pixel p .

The determination of such a function is not as obvious as it seems. It must provide a high convergence values among pixels in the same class and clear dispersion between different classes. One could think of using the mean of absolute values of $D(p)$ (or their variances). But, this kind of functions can penalize votes of some strong values in SR since they can be easily compensated by many votes of weaker values in NR. So, we need a function that emphasizes the contribution of the orientation deviations values as more as their votes are stronger. One proposition is to write $OFEN(p)$ as

$$OFEN(p) = \frac{1}{K} \prod_{i=1}^L \prod_{j=1}^{K_i} f(\Theta_{i,j}) \quad \text{III.3}$$

Where $f(\Theta)$ is a function that evaluates the contribution of the orientation deviations Θ , and K is the total length of the descriptor $D(p)$.

A suitable choice of the function f can be derived from the distribution of OD in NR which seems to be an exponential distribution as a best fit. The χ^2 goodness-of-fit is 35.77 (for 25 data bins) with a significance level of 5% for the exponential hypothesis (see Figure III.5)). So we can set

$$f(\Theta) = \frac{1}{\mu} \exp(-|\Theta|/\mu) \quad \text{III.4}$$

Where μ is the OD mean. So, we need to inverse the function f to let the energy be higher when the OD values, $|\Theta|$, are higher.

$$OFEN(p) = \frac{1}{K} \prod_{i=1}^L \prod_{j=1}^{K_i} \mu \exp\left(\left|\Theta_{i,j}\right|/\mu\right) \quad \text{III.5}$$

K is the total number of sampling points. The formula in (5) can be simplified as follows:

$$OFEN(p) = \frac{\mu^K}{K} \exp\left(\frac{1}{\mu} \sum_{i=1}^L \sum_{j=1}^{K_i} \left|\Theta_{i,j}\right|\right) \quad \text{III.6}$$

Since the factor (μ^K/K) is a constant and has no influence on the pixel classification, it can be omitted. The final energy function is:

$$OFEN(p) = \exp\left(\frac{1}{\mu} \sum_{i=1}^L \sum_{j=1}^{K_i} \left|\Theta_{i,j}\right|\right) \quad \text{III.7}$$

By computing the OF energy measure at each pixel, the input fingerprint image can be represented by an equivalent image, called orientation field energy map (OFEM). The resulting image is a direct interpretation of the distribution of the OF variation in the local neighborhood of each pixel in the input fingerprint. Figure III.6 shows the OFEM image of a whorl fingerprint with double core and double delta. The darkened red indicates high energy regions. As the Figure III.6 shows; the chosen energy function has improved the selectivity of the proposed descriptor so that the two regions (NR and SR) are clearly separated. Based on these results, we can locate candidate singular points.

III.3.4.2 Candidate singular points localization

Based on the analysis for the OFEM image, three important properties can be pointed out:

- 1- The energy response is low for normal area pixels, corresponding to low OF variation, and very high at singular regions pixels, corresponding to high OF variation (indicated respectively with blue and red colors in Figure III.6).
- 2- At the singular regions, the energy response is a monotonically increasing function that reflects the gradual transition of the variation of the OF from NR pixels to SR pixels. The closer the distance is to SP, the higher is the energy. The SP location is consistent with the point with local maximum where the energy function exhibits prominent peak. This gradual transition is interpreted by a cone that covers the entire SR with summit at the SP location (Figure III.6-d).
- (3) Noisy and corrupted regions can cause local maxima by generating peaks indicating spurious SPs (Figure III.6-e). However, these peaks are sudden changes in the energy function and don't obey to the gradual transition rule.

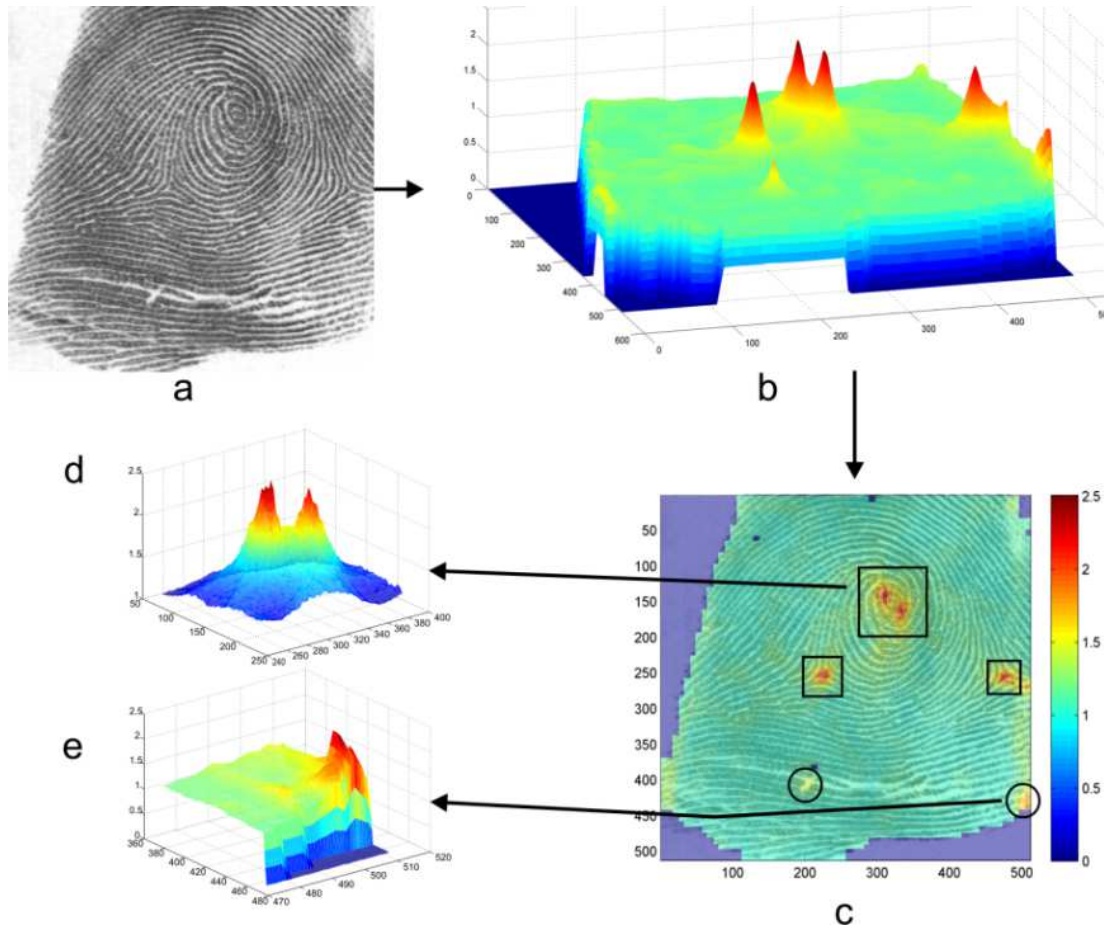


Figure III.6 Orientation field energy map of a whorl fingerprint. (a) Original image, (b) orientation field energy map (OFEM) in 3D view, (c) the corresponding 2D view of the OFEM superimposed on the original image. Candidate singular regions are labelled with rectangles (true) and circles (spurious) (d) the gradual transition tendency of the energy in true double-core region, (e) the tendency of the energy in a spurious singular region.

Based on these notes, candidate singular points can be located by isolating candidate singular regions (CSRs) using global and local thresholding technique (Gonzalez, 2009) on the TEMP image. Thus, a pixel p belongs to a CSR if its energy response is greater than a global threshold T_g as indicated by the equation (III.8).

$$\text{CSR} = \{ p(x,y) / \text{OFEN}(p) > T_g \} \quad \text{III.8}$$

T_g can be adaptively determined in such a way that an isolated CSR constitutes the upper part of its associated cone.

$$T_g = \max (\alpha * \max_{p \in I} (\text{TEXT}(p)), E_{NR}) \quad \text{III.9}$$

where I is the input fingerprint, α is a threshold factor that belongs to $]0..1[$ and E_{NR} is a selected threshold corresponding to the max value that a normal region pixel energy can, empirically, attain. This value permits to exclude the partial fingerprint containing no singularities. It can be obtained by substituting all the Θ_{ij} in the Eq. III.7 by the maximum OD value that a normal region pixel can attain which is $\pi/9$ as discussed in the Section III.3.3.1.

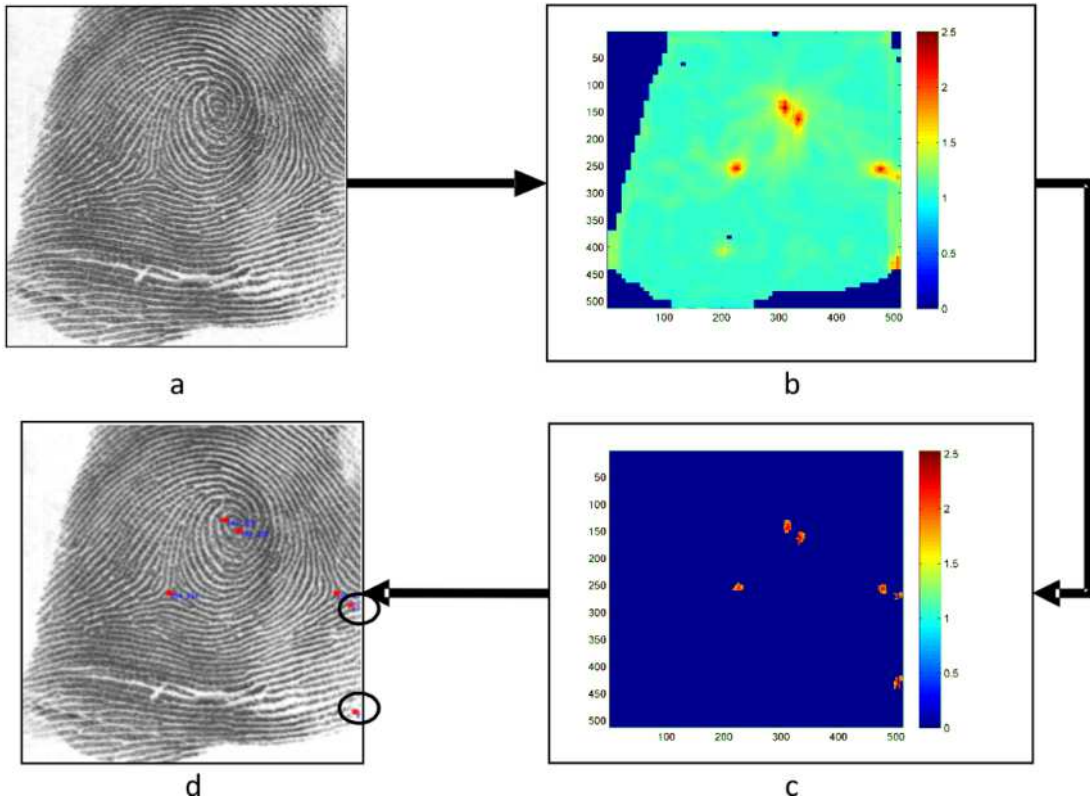


Figure III.7 Candidate singular points extracted by global and local thresholding. (a) Original image, (b) corresponding energy map, (c) detected candidate singular regions after thresholding, (d) final candidate singular points superimposed on the original image; the encircled ones are spurious.

$$E_{NR} = \exp\left(\frac{-K * \pi / 9}{\mu}\right) \quad \text{III.10}$$

Consequently, a candidate singular point (CSP) location can be determined directly as the pixel p in the associated CSR with local maximum energy.

$$\text{CSP}(x,y) = \operatorname{argmax}_{p \in \text{CSR}}(\text{OFEN}(p)) \quad \text{III.11}$$

Figure III.7 shows the candidate singular points detected in the fingerprint of Figure III.6 among which two points are spurious. They will be removed by analyzing some topological properties of each detected SP.

III.3.4.3 Singular points validation and type extraction

In an input FP with accepted quality, the localization of SPs is straightforward with no spurious points. However, the presence of noisy and corrupted regions could generate some spurious points despite of the anti-noise capability of the presented descriptor and the thresholding scheme applied. In addition, the type of the extracted SPs is not yet known. Thus, two important advanced properties of the OD based descriptor are introduced in the subsequent sections that permit to eliminate spurious points and get the type of each valid SP.

III.3.4.3.1 OD-based descriptor profile

As mentioned above, the proposed descriptor represents completely the local structure surrounding a pixel p . Our experiments show that the arrangement of the OD features in $D(p)$ is highly correlated with the topological structure of p , that is, whether p is a core point, delta point, arch-type singular point or a pixel with no singularities (normal or spurious singular points). Figure III.8 shows some fingerprint portions with labelled singular points and their respective OD-based descriptor profiles plots. Each descriptors is calculated over 4 circles ($L = 4$). The plots clearly indicate that the tendency of each profile depends heavily on the pixel type. Moreover, the profile is, almost, a regular symmetric shape for each singular point which is consistent with the idea in (Nilsson & Bigun, 2002; Park et al., 2006).

The profile characteristics for each type can be summarized as follows:

- The core point profile has almost monotonically decreasing values with ‘arctangent’ function-like shape (Figure III.8-a).
- The delta point profile has monotonically increasing values with ‘tangent’ function-like shape (Figure III.8-b).
- The arch-type SP has a combination of the two precedent profiles with decreasing values (the first half values) then increasing values (the second half values) having the ‘cosine’ function-like shape (Figure III.8-c).
- The normal point has almost a linear profile with values near the zero (Figure III.8-d).
- The spurious singular points don’t have any regular shape (Figure III.8-e).

The announced properties lose reliability as the size of the descriptor (number of circles L) increases. This can be interpreted by the fact that more non-singular patterns are included in the SP features as its size increases. Thus, the descriptor size must be carefully chosen. In addition to that, noise near valid singular points locations could change a little the profile shape, but the rules remain valid and still clear difference between true and spurious singular points exist.

Note that there is no issue of determining the starting point of the OD-based descriptor profile when the fingerprint is rotated. It coincides always with the starting point of the OD-descriptor which is invariant to rotation.

III.3.4.3.2 Extended Poincaré Index

The classical Poincaré Index (PI) method, which is defined over the OF, has some special values in the singular regions. We extend the PI to be defined on the OD space rather than on the orientation field. Thus, we define the Extended Poincaré Index for a point $p(x,y)$ along the circle C_i of the descriptor $D(p)$ as a pair of two values :

$$EPI(p) = (\Delta^+(p), \Delta^-(p)) \quad \text{III.12}$$

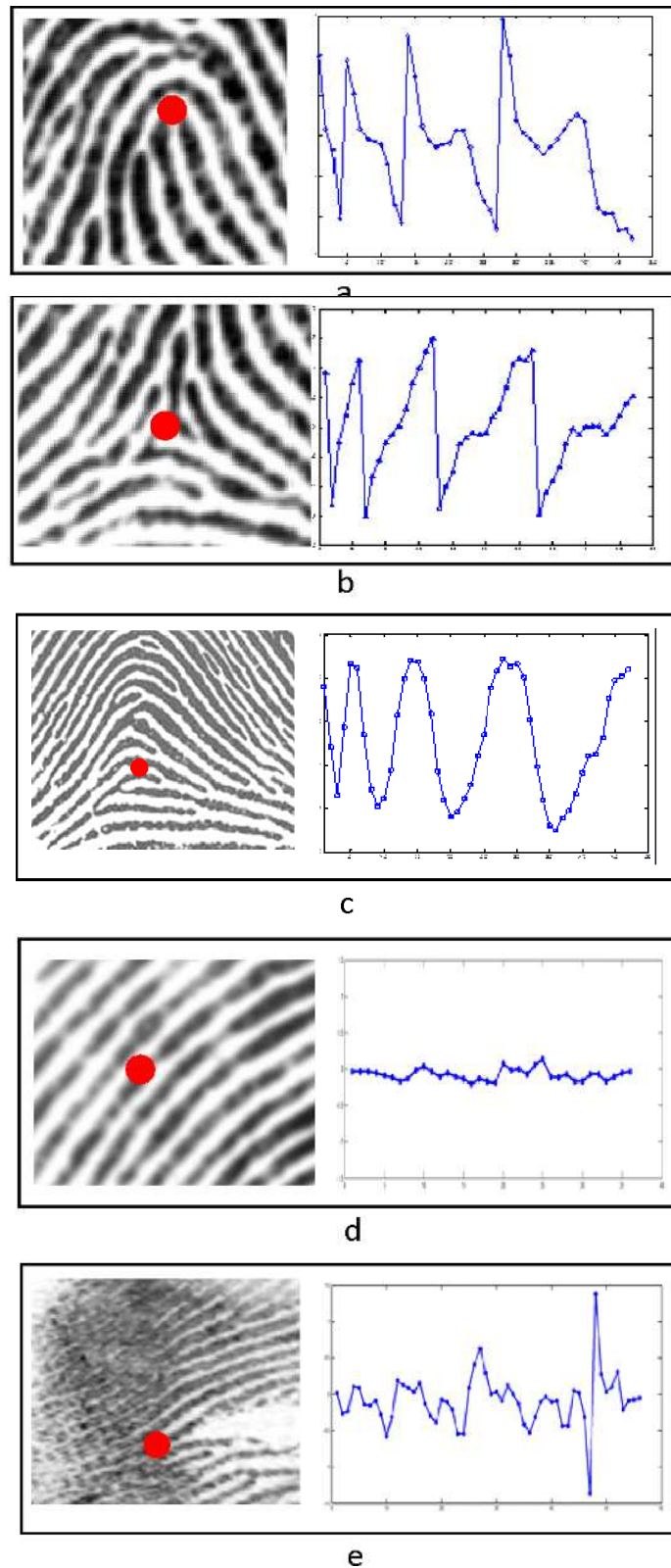


Figure III.8 Labeled singular, normal and spurious points on some partial fingerprints and their OD-based descriptor profiles. All the descriptors are calculated over 4 circles. (a) True core point, (b) true delta point, (c) arch-type point, (d) normal point, (e) spurious delta point.

where $\Delta^+(p)$ (respectively $\Delta^-(p)$) represents the accumulation of the positive (respectively

negative) differences of the adjacent orientation deviations (DOD) in C_i .

$$\Delta^+(p) = \frac{1}{\pi} \sum_{j=1}^{K_i} DOD^+(j) \quad \text{III.13}$$

$$\Delta^-(p) = \frac{1}{\pi} \sum_{j=1}^{K_i} DOD^-(j) \quad \text{III.14}$$

where

$$DOD^+(j) = \begin{cases} \delta(j) & \text{if } 0 \leq \delta(j) < \pi/2 \\ \delta(j) + \pi & \text{if } \delta(j) \leq -\pi/2 \\ 0 & \text{otherwise} \end{cases} \quad \text{III.15}$$

and

$$DOD^-(j) = \begin{cases} \delta(j) & \text{if } -\pi/2 < \delta(j) < 0 \\ \delta(j) - \pi & \text{if } \delta(j) > \pi/2 \\ 0 & \text{otherwise} \end{cases} \quad \text{III.16}$$

with

$$\delta(j) = \Theta_{i,(j+1) \bmod K_i} - \Theta_{i,j} \quad \text{III.17}$$

The values that the pair Δ^+ and Δ^- of the EPI function can assume depend on the type of the underlying:

- If $\text{EPI}(p) = (1,0)$ then p is a possible delta point.
- If $\text{EPI}(p) = (0,-1)$ then p is a possible core point
- Otherwise, p is a normal pixel and the sum of the pair Δ^+ and Δ^- is null.

Note that the sum $(\Delta^+ + \Delta^-)$, most used in the PI literature^{16,18}, is a general condition than the above announced values which are more strict and permit also to detect arch-type singular point.

Figure III.9 shows the application of the EPI function on the fingerprint of Figure III.6. The function is calculated over the circle C_1 with radius equal to 10 pixels. Both the attributes Δ^+ and Δ^- are plotted separately on the Figure III.9 besides the resulting singularities superimposed on the original image. Blue color on Figure III.9-a indicates candidate core points and red color indicates candidate delta points. Since the resolution of the OD space reaches the pixel unit, the resulted singular points sets constitute condensed clustered pixels for each singular region. The size of each cluster depends on the radius of the circle C_i and whether it includes true or spurious singular point. Usually, the clustered regions are well separated and each one contains at most one true candidate SP to which the whole cluster must be reduced. Note that the proposed EPI has eliminated one spurious singular points detected in the Figure III.7, but,

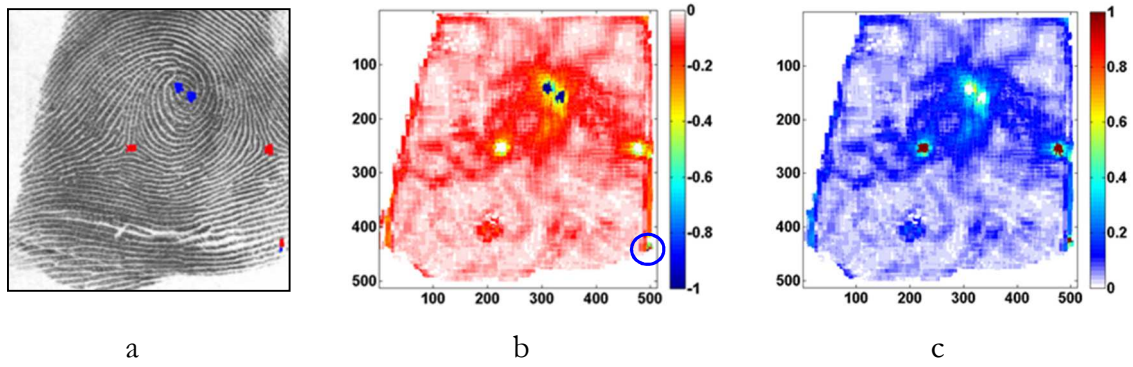


Figure III.9 Candidate singular points detection using the extended Poincaré Index. (a) Resulting singular points superimposed on the original image, blue colour indicates core points and red colour indicates delta points, (b) the Δ^- attribute plot which is responsible for detecting the core points, (c) the Δ^+ attribute plot which is responsible for detecting the delta points.

unfortunately, it has introduced another spurious point (encircled with blue circle in Figure III.9-b) which didn't exist before.

III.3.5 SP detection algorithm description

The combination of the concepts presented previously allow us to formulate an accurate algorithm to detect singular points in a given input fingerprint I . The main steps are summarized as follows:

1. Apply a Gaussian filter $g(0, \delta^2)$ to the input image I .
2. Estimate the orientation field OF , at each pixel and get the segmented image G as discussed in Section III.3.2. The block size is W .
3. Compute the OD based descriptor $D(p)$ for each pixel p in the segmented image G .
4. Compute the orientation field energy map $OFEM$ as indicated by the Eq. (III.7)
5. Apply a **global** thresholding to the energy map. Let S_1 be the resulted set of pixels; $S_1 = \{p(x,y) \in G / OFEM(p) > T_g\}$. S_1 indicates the energy-based candidate singular points list.
6. Extract the second candidate singular points list, S_2 , by calculating the EPI at each pixel in the segmented image G . $S_2 = \{p(x,y) \in G / EPI(p) = (1,0) \text{ or } (0, -1)\}$
7. Calculate the final candidate singular points, S , by intersecting the energy-based and the EPI-based singular points sets; $S = S_1 \cap S_2$. S is a set of clusters of pixels determining candidate singular regions (CSRs).
8. For each cluster C in S
 - a. Get the point $p^*(x,y)$ with local maximum energy in C .
 - b. If the descriptor $D(p^*)$ contains a value which is consecutively repeated M times or more then eliminate p from S and continue from 8 (see the Section III.4.1).
 - c. Verify the incremental transition rule of the energy in the local neighborhood of p^* . If it doesn't verify this rule, eliminate p^* from S and continue from 8.
 - d. Get the type t^* of p^* ($t^* = -1$ for a CORE or 1 for a DELTA point)
 - e. Verify the descriptor profile tendency of p^* according to its type t^* . If it doesn't verify this rule, eliminate p^* from S and continue from 8.

9. For each point p in S
 - a. Get the orientation of p from OF.

The algorithm output is the set S of all candidate singular points with their full information (2D coordinates, type and orientation).

III.4 Experimental results

We use the public database FVC2002 DB1 and DB2¹⁹ to test the proposed algorithm. Both databases contain 800 fingerprints (100 fingers with 8 impressions for each one).

To obtain ground truth, all singular points were manually labelled as triplets (x_0, y_0, t_0) ; where x_0 and y_0 are the coordinates of the singular point and t_0 is its type. A detected SP (x, y, t) is accepted as true SP if $|x-x_0| < W$ and $|y-y_0| < W$ and $t=t_0$, otherwise it is a miss detection. So we define the detection rate as the ratio of truly detected SPs to all ground truth SPs. The ratio of the number of falsely detected SPs to the number of all ground truth defines the false alarm rate. A fingerprint is decided to be truly detected if all its SPs are truly detected and no spurious SP found.

The experiments are conducted following the proposed algorithm in the Section III.3.5 which is implemented in C# and evaluated on a PC with an Intel core i3 processor and 3GB RAM running windows 7. The parameters used are listed in Table 1. Note that window size W and the average inter-ridge distance τ values are given according to the resolution of the FVC2002 DB1 and DB2 fingerprints. In general case, assume that R is the resolution of the fingerprint image in dpi. The average inter-ridge distance value τ in millimeter is estimated as equal to 0.463 mm/ridge according to some studies (Stoney, 1988), this makes τ equal in pixels to $[0.463 \cdot R / 25.4]$ which gives $\tau = 0.018 \cdot R$. The windows size is generally chosen to be a little less than the τ value, so $W = 4 \cdot \tau / 5$.

Table III.1 parameters used in our algorithm

Parameter	Meaning	Value
δ_g	Standard deviation of the Gaussian filter	1.4
μ	OD mean	5.08
W	Segmentation block size	8
δ^2	Segmentation grey level variance threshold	100
α	Threshold factor	2/3
M	Maximum number of consecutively repeated value in an OD-descriptor	3
τ	Average inter-ridge distance	10

III.4.1 OD-Descriptor implementation discussion

The OD-Descriptor is implemented such that two consecutive circles are separated by at least one ridge ore one valley.

$$\begin{cases} R_1 = \tau \\ R_{i+1} - R_i = \tau; i = 1..L-1 \end{cases} \quad \text{III.18}$$

The number of sampling points on each circle also obeys to this rule. That is, the distance between two consecutive sampling points on the circle C_i is equal to τ . Thus, the number of sampling points in the circle C_i , noted N_i , is:

$$N_i = [i*2\pi] \quad (1)$$

where $[.]$ denotes the integer part function. This choice is very important in a manner that it doesn't allow many consecutive equal values in the same circle around a SP. Such characteristic can enormously help to filter out some spurious singularities. Furthermore, each circle can be viewed as to be tuned to capture information at a given curvature scale. This idea substitutes reliably the multiresolution techniques implemented in most works such as (Weng et al., 2011) and gives more flexibility to accurately locate SPs.

III.4.2 The effect of the OD-descriptor size

The first set of experiments has been conducted to evaluate the effect of the descriptor size (number of circles L) on the detection rate. We varied the size of the descriptor from 1 to 4, and for each case we establish the resulted detection rate for both databases. Figure III.10 summarizes the results. From these results, we can conclude that increasing the descriptor size value has an adverse effect on the detection rate. Best results are obtained for less values especially for $L = 2$. This can be interpreted as follows: as the descriptor size increases, more non-singular patterns will be included in the descriptor of each singular point. This gives chance to other CSPs to maximize their energy and to be real concurrent to the genuine SPs. In addition to that, the extension of the descriptor to other non-singular patterns decreases the robustness of the two announced properties which can generates more spurious singular points.

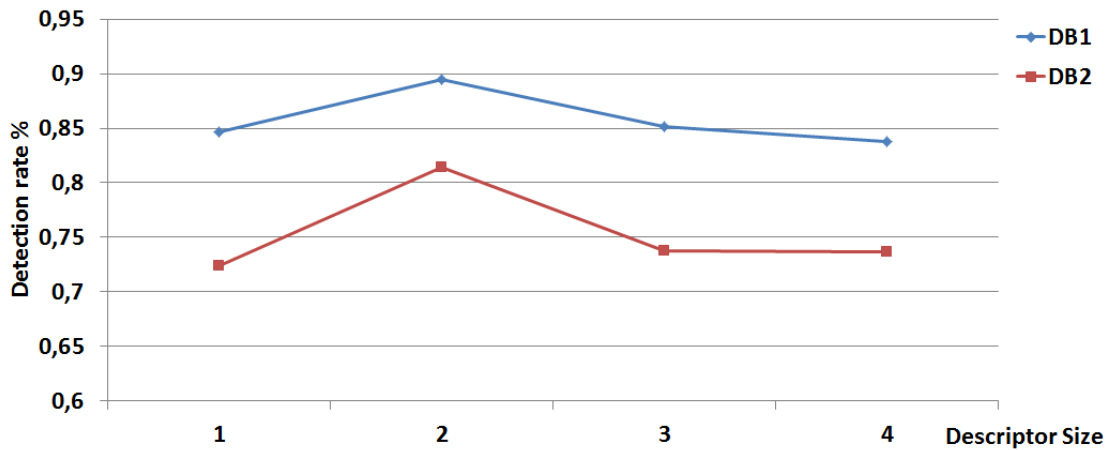


Figure III.10 The detection rate evolution on the FVC databases DB1 and DB2 in function of the descriptor size.

III.4.3 Time performance evaluation

To evaluate the time performance of our algorithm, we have divided it into five stages. Each stage contains several steps. Table III.2 summarizes the average execution time obtained for each

stage by applying the algorithm on the database FVC2002 DB1 using the value $L=2$ for the OD-descriptor size. It should be noted that the size of each fingerprint image in the FVC2002 DB1 is 388×374 pixels. As it can be seen from the results, the average execution time is 0.881 seconds. The most time-consuming stages (almost 50% of the average execution time) are the orientation field estimation, which involves many image processing steps, and the OD-based descriptor calculation which involves points sampling process.

III.4.4 Comparative study

The second set of experiments gives a comparative study with three works reported to give best results namely (Weng et al., 2011), (Zhou & Gu, 2004) and (Chikkerur & Ratha, 2005). Both the first methods are enhanced versions of the PI method. The comparison results on both databases FVC2002 DB1 and DB2 are listed in Table III.3 and Table III.4 respectively. From these results, we can conclude that our method performs better on both databases in terms of all false alarm rates. This means that our method generates less number of spurious singular points. The detection rate on both databases is also better than the others, however the detection rates for the core point on the database DB2 is less. This means that our method fails a little to detect some core points especially when the input fingerprint is of low quality.

III.4.5 Singular point for arch-type fingerprint

As known, arch-type fingerprint doesn't obey to the Henry rule in defining core and delta points. Thus, it doesn't contain any singular point. However, determining a reference point for this type of fingerprints is of great utility in fingerprint recognition, especially for identification and classification. In such a case, the Arch-type SP is usually associated with the point of maximum ridge line curvature. Consequently, this point coincides with location with global maximum energy. Moreover, our experiments confirm that the positive attribute of the EPI function, Δ^+ , knows also its global maximum at the same location. Note that the EPI function attributes at each pixel of an arch-type fingerprint are related by the equation: $\Delta^+ + \Delta^- = 0$. To handle this type of fingerprints, the proposed algorithm must be modified, at step 6, as follows:

- Extract the second candidate singular points list S_2 by calculating the EPI at each pixel in the segmented image G . $S_2 = \{ p(x,y) \in G / \text{EPI}(p) = (1,0) \text{ or } (0, -1) \}$
- If(S_2 is empty) then $S_2 = \{ p(x,y) / \Delta^+ > \alpha * \max(\Delta^+) \}$

Table III.2 Execution times for different stages in the algorithm

Stage	Steps	Time in seconds
Orientation field estimation	1 to 2	0,257
OD-based descriptor calculation	3	0,233
Energy based Candidate SPs detection	4 to 5	0,202
EPI based candidate SPs detection	6	0,189
SPs validation and types extraction	7 to 9	0,018

Table III.3 The comparative results between some proposed SP detection algorithms on FVC2002 DB1

		Proposed	(Weng et al., 2011)	(Zhou & Gu, 2004)	(Chikkerur & Ratha, 2005)
Singular points (cores + Delta)	Detection rate	95.092	96,4	96.10	95.06
	False alarm rate	3.370	4.39	4.30	7.25
Cores	Detection rate	95.634	96.85	95.78	95.89
	False alarm rate	2.599	3.14	2.27	6.93
Deltas	Detection rate	93.797	94.01	96.98	92.75
	False alarm rate	5.211	7.63	9.97	8.16
Fingerprints	Correct rate	89.500	89.13	88.88	85.13

Table III.4 The comparative results between some proposed SP detection algorithms on FVC2002 DB2

		Proposed	(Weng et al., 2011)	(Zhou & Gu, 2004)	(Chikkerur & Ratha, 2005)
Singular points (cores + Delta)	Detection rate	90.277	94.57	94.51	93.46
	False alarm rate	5.535	9.67	9.60	17.33
Cores	Detection rate	90.147	96.23	95.95	93.23
	False alarm rate	4.298	8.60	8.45	13.87
Deltas	Detection rate	90.601	90.51	90.88	94.20
	False alarm rate	8.616	12.31	12.54	28.62
Fingerprints	Correct rate	81.375	81.50	81.25	73.25

Table III.5 performance comparison between some selected SP detection methods

	Performance criteria				
	Robustness to noise	Partial FP image sensitivity	Location of SP at border sensitivity	Arch-based SP detection capability	Computational cost
Poincaré Index	low	low	low	Not capable	low
(Nilsson & Bigun, 2002)	high	low	low	Not capable	medium
(Park et al., 2006)	low	high	low	capable	low
(Zacharias & Lal, 2013)	medium	low	low	Not capable	medium
(Zhou & Gu, 2004)	high	low	low	Not capable	high
Proposed method	medium	high	high	capable	Medium

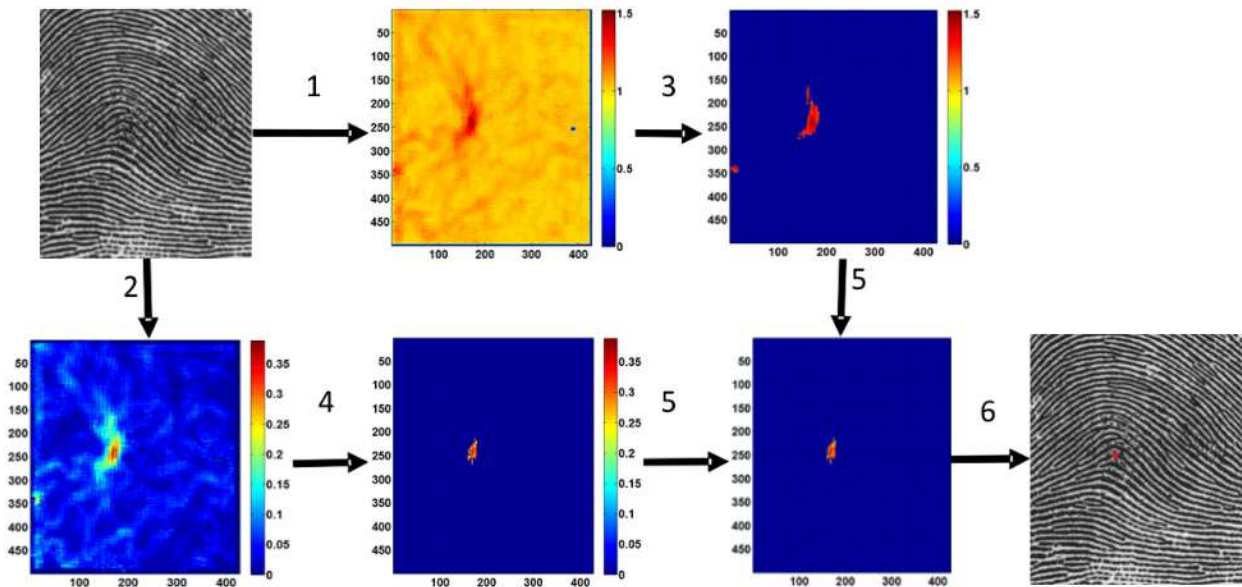


Figure III.11 Arch-type singular point detection flow chart. (1) Compute the OFEM map, (2) compute the positive attribute $\Delta+$, (3) OFEM global thresholding (4) $\Delta+$ global thresholding, (5) pixel intersection between the two images, (6) local energy thresholding that gives the final singular point.

Figure III.11 resumes the arch-type singular point detection process.

III.4.6 Special cases

Figure III.12 show some special and delicate cases of fingerprints where our method successfully and accurately detects singularities that most of the state-of-the-art methods fail to do. These include:

- Singularities are close to each other like in whorl type (Figure III.12-a) and tented-arch type (Figure III.12-b) fingerprints. Both these fingerprint types have a complex ridge pattern containing two singularities; the whorl type contains two cores and the tented-arch type contains one core and one delta. Most of the proposed algorithms fail to detect both singularities especially when they are close to each other. As shown by the Figure III.12, our algorithm has successfully detected both singularities in each case.
- Partial fingerprints with no singularities (Figure III.12-c) or with singularities located at borders (Figure III.12-d and e).
- Fingerprint with low quality (Figure III.12-f).

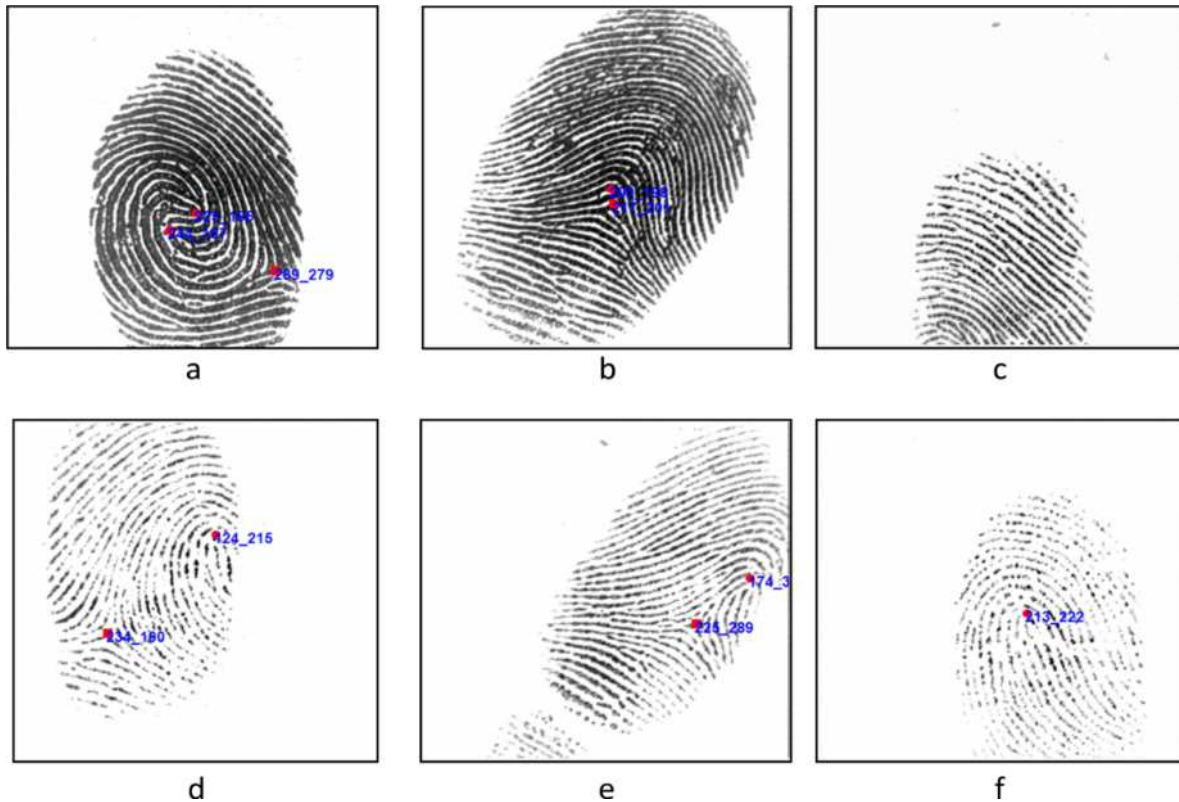


Figure III.12 some difficult cases to deal in which the algorithm was able to detect the singularities. (a) and (b) singularities are close to each other, (a) whorl fingerprint, (b) tented arch fingerprint, (c) partial fingerprint with no singularities, (d) and (e) core point localized at border, (f) fingerprint with low quality.

III.5 Conclusion

In this chapter, a fingerprint singular point detection method based on the calculation of the variation of the orientation field is described. Initially, a pixel-wise descriptor based on the orientation deviation features is designed to gather some topological information in the local orientation field of each pixel. These information are able to classify each pixel as belonging to normal or singular region. The classification is performed based on the local orientation field energy. Candidate singular points are defined as locations where the energy function exhibits local prominent peak. Thus, the list of candidate singular points is obtained by applying a global and local thresholding method. Spurious singular points are further eliminated by analyzing some topological properties manifested by the pixel descriptor; in particular, the tendency of the descriptor profile which is dependent to the type of the underlying pixel. A second refining step relies on the extension of the classical Poincaré Index to be defined on the orientation deviation space as a pair of two attributes. Each attributes has a special value for each normal and singular point type. Experiments have shown the accuracy of our algorithm especially in minimizing the false alarm rate.

Chapter IV

Fingerprint matching using a dynamic minutia descriptor

Most minutiae-based matching techniques use local static descriptor to emphasize their discrimination power between ambiguous minutiae features. Although the improvements shown by these methods, still some challenging problems limit their performance in particular the presence of spurious minutiae and the missing of genuine minutiae. The added/missed minutiae problem misleads the matching algorithm and complicates the correspondence decision. A general countermeasure of most existing matching algorithms is to add a global matching consolidation step that results in augmented time complexity.

In this chapter, a dynamic minutiae-based descriptor is described. Its particularity resides in its ability to adjust a minutia features according to the correspondent minutia context in the second print.

The minutiae of the input fingerprint are arranged to get a global stable geometric structure called minutiae-based polysegment structure (MPS). This latter permits to detect added/missed minutia once compared to another MPS structure. Whenever the matching algorithm detects an added minutia in an MPS, it inserts a virtual minutia in the second to update the minutia descriptor context and, hence, let propagating the similarity. This increases the chance to maximize the number of genuine paired minutiae. Furthermore, the MPS structure reduces enormously the minutiae space to be tested; the matching algorithm complexity is near $O(n \log(n))$. Experiments of the proposed algorithm are conducted on the public database FVC2002.

IV.1 Local minutia descriptor

Fingerprints have been routinely used in the forensics community for over one hundred years and automatic fingerprint identification systems (AFIS) were first installed almost fifty years back (Maltoni, Maio, Jain, & Prabhakar, 2009).

The performance of an AFIS depends largely on the matching method being conducted that can be coarsely classified as being minutiae-based or correlation-based matching. In general, it has been observed that the former class methods are the most well-known, widely used and perform better than correlation-based ones (Maltoni et al., 2009). In this chapter, we principally focus on this class.

The Minutiae matching task is to establish a correspondence between two fingerprints represented by their respective minutiae lists. However, based only on traditional attributes of

minutia (2D-coordinates (x , y), direction θ and type (bifurcation or ridge ending)), the correspondence between minutiae is very ambiguous due to the nature of the problem being essentially a point pattern matching problem which can be affected by serious difficulties such as the rotation, translation and distortion of the fingerprints. Consequently, many minutiae-based AFIS enrich the minutia attributes with additional rotation and translation invariant features by implying some other minutiae in its neighborhood to form so-called “local descriptor”.

Local minutia descriptors can be classified into nearest neighbor-based and fixed radius-based (Maltoni et al., 2009). The first class describes a minutia in function of its k -nearest minutiae information in terms of Euclidian distance (Bengueddoudj, Akrouf, Belhadj, & Nada, 2013; Jiang & Yau, 2000) and/or angles (Jea & Govindaraju, 2005; Kwon, Yun, Kim, & Lee, 2006). In the second class, a central minutia is described in function of all minutiae that lie in a distance less or equal than a radius R . (Cappelli, Ferrara, & Maltoni, 2010; Feng, 2008; Ratha, Bolle, Pandit, & Vaish, 2000). The common features used in both approaches are: distances, ridge-count, directions and radial angles of the central minutia relative to each one in the local structure. Thus, the matching process between two prints is generally achieved in two steps 1) Local matching step that allows to determine minutiae pairs that share similar local descriptor features (match locally), 2) Consolidation step that aligns globally the two prints according to some selected minutiae pairs and gets the maximum matching score.

IV.2 Issues around matching using local minutia descriptor

Local-descriptor based methods have brought many desirable improvements in particular local deformation tolerance, high discriminability between minutiae features and significant matching performances. However, there are a number of challenging issues that need to be addressed in order to boost the performances, including: the static nature of the descriptor, the presence of spurious minutiae and the missing of genuine ones besides the high computational complexity constitute challenging problems that are paid, unfortunately, little attention by the literature. The following subsections discuss in more details the influence of these problems on the local descriptor performances and review some proposed solutions.

IV.2.1 The unstable static descriptor problem

Most minutiae-based matching methods use a non-static descriptor. A minutia descriptor is said to be static if its feature elements are pre-established, based on local neighborhood structure, before the matching step and their values are kept unchangeable during all the matching process time. Furthermore, the same descriptor with the same values is used as a reference against any issued minutiae descriptor given for matching. However; the local structure on which the descriptor is based is not stable when some minutiae are missed from one print to another even if they are from the same finger. Indeed, due to many reasons especially noise and the conditions of acquiring the fingerprint; the minutiae extraction algorithm may deliver erroneous minutiae. That is, it may add spurious minutiae that do not exist initially in the reference print or, inversely, miss genuine minutiae that exist initially in the reference print. Moreover, there may be only a small overlapping region between the two prints such that several minutiae are missed in both instances.

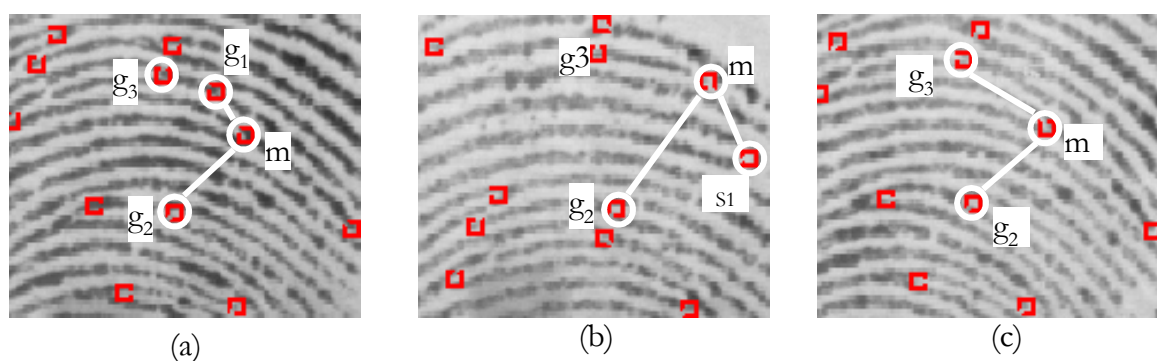


Figure IV.1. The effect of added/missed minutiae on the structure of a 2-Neighbors-based minutia descriptor. (a), (b) and (c) are partial fingerprints of the same finger from FVC2002 database with labelled minutiae. (a) Reference descriptor of minutia *m* consisting in *g1* and *g2*; (b) the descriptor of '*m*' has changed, it consists in *g2* and *s1*. The error is due to spurious minutia *s1* that has replaced *g1*; (c) The minutia *g1* is missed, the descriptor has been changed to comprise this time *g2* and *g3*.

Figure IV.1 illustrates the effect of the added/missed minutiae problem on the stability of a minutia descriptor along three partial fingerprints of the same finger. For instance, any spurious minutia '*s*' added in the neighborhood of a central minutia '*m*' can exclude a genuine minutia '*g*' from the local structure by force of the relation “nearest neighbor” (Figure IV.1-b). On the other hand, any missed genuine minutia in the neighborhood of *m* will be replaced by another minutia that doesn't really belong to the structure of '*m*' (Figure IV.1-c). Thus, the established descriptor, in both cases, is based on a local structure different from that of the reference descriptor and it is unreliable to be matched with. This incompatibility leads to encourage the false matching cases and can deliver some inconsistent minutiae pairs.

IV.2.2 The search-space size problem

Most of the local-minutiae based descriptor matching methods present a high matching complexity time which is due principally to two reasons: i) given two prints template *T* and query *Q*, both of *N* minutiae in average (Usually *N* is between 30 and 60). The local matching step has to do an exhaustive test to cover all the minutiae descriptors set in *Q* for each minutia in *T* (so N^2 comparisons) to identify a set of best matching minutiae pairs *P*, ii) due to the effect of the erroneous minutiae, the local matching step may deliver false matched pairs or generates pairs that share common minutiae. As a consequence, an additional consolidation step is necessary to refine the local results and extend them to a global level. This can be achieved by aligning the two prints according to each minutiae pair in *P*. Finally, the minutiae pair that maximizes the global score is retained to generate the final paired-minutiae list. This step involves a time cost equivalent to $O(kN^2)$ at least where *k* is the size of *P*.

IV.2.3 Some proposed solutions

To deal with these problems, some authors design their descriptor to be independent with respect to any minutia detected in the fingerprint by employing non-minutia information. (Tico &

Kuosmanen, 2003) used local field orientation information taken at a set of sampling points around a central minutia to build its descriptor. A similar approach was proposed by (Feng, 2008; Qi & Wang, 2005) combined with minutiae descriptor. Since they cannot neglect the erroneous minutia problem, a greedy matching algorithm is used followed by a light consolidation step. The final global alignment is obtained by aligning the two minutiae lists according to the minutiae pair that maximizes the similarity function during the local matching step. Unfortunately, this is not always the reliable minutiae pair to be selected.

Other works exploited the computational geometry to model the fingerprint as global minutiae-based structures that are more stable to erroneous minutiae problem. (Deng & Huo, 2005) used Delaunay triangulation structure to interconnect minutiae. Thus, any added/missed minutia will have only a local limited effect on the neighborhood of a minutia which is delimited by the Delaunay triangles. Having only $O(N)$ triangles, N is the number of minutiae, the search space is enormously reduced. Other similar geometrical structures are also used, such as nested convex polygons (Khazaei & Mohades, 2007) .

An interesting method was proposed by (Das, Karthik, & Chandra Garai, 2012) that is capable to detect any added/missed minutiae. It relies on the Minimum Distance Graph (MDG) structure originating from the core point. A two-phase approach is achieved to find a match between a pair of MDG: first, three successive matched edges must be found based only on their distances. Second, the rest of both the graphs are subdivided into two sub-graphs which are again matched together. The authors reported good performances. However, the method has some drawbacks as well: the MDG structure is less stable for matching; any erroneous minutia can have global effects on the graph since it can turn away its partial or total path (see Figure IV.2).

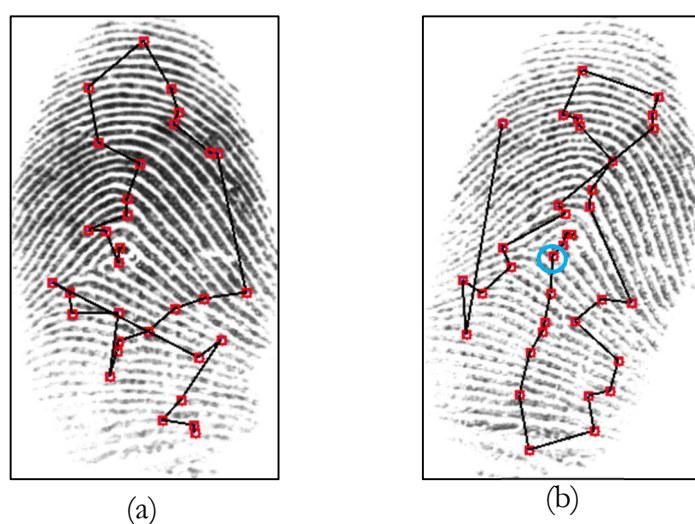


Figure IV.2. Two fingerprints from the same finger with their respective MDGs. The occurrence of the minutiae surrounded with a circle in (b) has totally inverted the MDG_b according to MDG_a. The two MDGs are falsely unmatched

All the previous methods don't attack directly the problem of erroneous minutiae; they rather try to reduce its effect by constructing more complicated descriptors and/or consuming more time.

We strongly believe that the problem doesn't reside in the occurrence of erroneous minutiae since we can't avoid the missing of genuine minutiae and the presence of spurious minutiae even if we use an efficient minutiae extraction algorithm, it rather resides in the classical matching scheme that most minutiae-based matching algorithm use. This scheme is based on a static minutiae-descriptor that doesn't tolerate added or missed minutiae.

We propose in this work to modify the classical correspondence scheme, which is based on a static descriptor, to deal with a dynamic minutia-descriptor that can change its features as the matching process progresses. Such a descriptor is more flexible towards added or missed minutiae. The proposed matching algorithm models the spatial distribution of minutiae in both fingerprints as a shape called Minutiae-based Polysegments Shape (MPS) originating from the core point. Based on a non-static descriptor, the correspondence scheme is achieved with a kind of shape pattern matching algorithm between the two MPS. It starts from the assumption that the two MPS are similar and try to synchronize adaptively one shape according to the second. Whenever a missed minutia is detected in an MPS, the proposed matching algorithm injects a new virtual minutia in the second to reconstruct compatible structures in both prints and, thus, let propagating the synchronization. At the end of the algorithm, both the prints exhibit the same spatial shape allowing us to calculate the matching score.

The proposed approach has two merits, it introduces the concepts of a dynamic descriptor and virtual minutia, and presents a matching algorithm with reduced complexity time equal to $O(n \cdot \log n)$.

The proposed method goes through three main steps: 1) minutiae features extraction and core point detection, 2) Minutiae Polysegment Structure construction and 3) the matching step yielding the matching score.

Subsequent sections give more details about this process.

IV.3 Minutiae features extraction and core point detection

IV.3.1 Minutiae features extraction

As stated in Section II.4.2.6.3, there exist principally two approaches for minutiae extraction methods: direct approach that extracts minutiae directly from the greyscale image (Maio & Maltoni, 1997), and the indirect approach that follows the scheme based on the enhancement, binarization and thinning (Hong, Wan, & Jain, 1998). The former is fast but can miss genuine minutiae whereas the latter is slow but can add spurious minutiae. We have implemented the main steps of (Ratha, Chen, & Jain, 1995) method. The final result is a list of minutiae $\{m_i\}_{i=1..N}$ having the following features: $m_i(x_i, y_i, \theta_i)$ where x_i, y_i are minutia location coordinates and θ_i is its orientation.

IV.3.2 Core point detection

The core point is the most top point on the most inner ridge. Chapter III gives a comprehensive state-of-the-art in fingerprint singular points detection algorithms. We use the algorithm

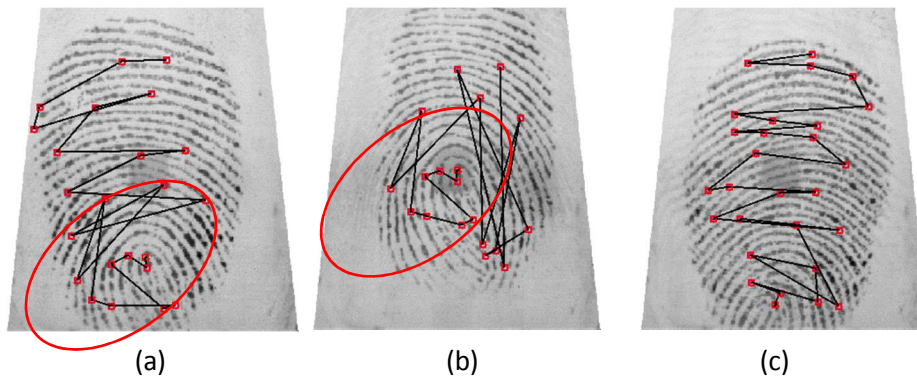


Figure IV.3 Some fingerprints with their associated MPS structures. (a) and (b) are impressions of the same finger. Their MPS structures look similar but influenced by the added/missed minutiae. (c) A fingerprint from another finger, its MPS is totally different.

proposed in that chapter to detect the core point. If the input fingerprint doesn't contain any core-point, we extract the most inner point in the ridge structure with the high curvature.

IV.3.3 Minutiae-based Polysegment structure construction

The spatial distribution of minutiae in a fingerprint is represented as a global structure resulted by connecting one minutia to another in a manner to construct a well-formed shape called Minutiae Polysegment Structure (MPS). This global geometric representation stores most topological information about the minutiae distribution and still maintains the uniqueness of a fingerprint. Formally, after the above features extraction step, a fingerprint FP is transformed to a set S of $(N+1)$ points, one core point + N minutiae.

$$S = \{C(x_0, y_0, \theta_0)\} \cup \{m_i(x_i, y_i, \theta_i), i = 1..N\}.$$

The Minutiae Polysegment Shape defined over the set S is a special directed graph $G(S,E)$ whose nodes correspond to the points of S , and with two nodes m_i and m_j connected by a directed arc if the minutia m_j is the following nearest minutia to the core point after the minutia m_i . Consequently, MPS is a one-path broken line originated from the core point. As a data structure, it is a FIFO queue initialized with the core point C , and the minutiae points are then queued according to their distance to C . The sort function is done using a fast sort algorithm (Sedgewick, 2002). Figure IV.3 gives examples of fingerprint images and their respective MPS.

IV.3.3.1 MPS structure properties

As it has just been defined, the MPS structure has some important characteristics that make it more suitable for matching:

- 1- It is invariant with respect to global transformations of the fingerprint such as translation and rotation.
- 2- It determines a forbidden region $FR(m_i, m_{i+1})$ between two successive nodes m_i and m_{i+1} , within which no node m_k may lie. It results from the intersection of two disks centered at

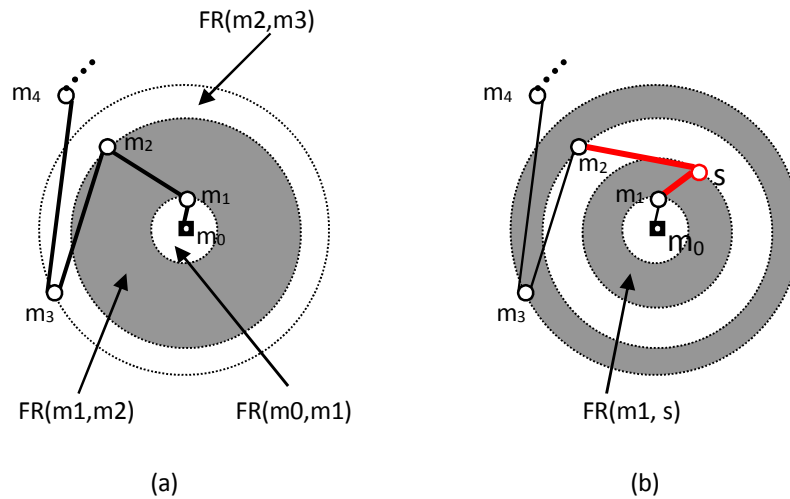


Figure IV.4. The effect of added/missed minutiae on the MPS structure.
 (a) Reference MPS, (b) the resulted MPS when a new incoming minutia 's' is inserted in (a).

the core point C with respective radius $d(C, m_i)$ and $d(C, m_{i+1})$ (see Figure IV.4). Where $d(.,.)$ is the Euclidean distance between two nodes.

- 3- More stable to added/missed minutiae: inserting or removing a minutia have only a local effect on the MPS. Figure IV.4 illustrates the effect of inserting a new minutia on an initial MPS. In fact, when a new minutia m_p is inserted in an MPS, it will lie, according to its distance to the core point C , in the forbidden region $FR(m_i, m_j)$ of two consecutive nodes m_i and m_j . So, the MPS will be simply enriched with two segments (m_i, m_p) and (m_p, m_j) that lie both into $FR(m_i, m_j)$. The rest of the MPS remains unchangeable.

These characteristics are fundamental for the following matching step since they permit to detect any added (missed) minutiae between two prints and, therefore, establish a robust and fast matching algorithm.

Throughout the rest of this paper, we use the terms node and minutia interchangeably. The minutia attributes (x, y, θ) are used with its correspondent node.

IV.3.4 The Proposed Matching Algorithm

Given two fingerprints represented, each one, with its equivalent MPS; the matching algorithm starts from the assumption that the two prints look similar with respect to their MPS structures. It tries to adjust adaptively the irregular local contexts of one shape according to the second shape by inserting virtual nodes whenever it detects missed ones. This idea is consolidated by our experiments confirming that if the prints come from the same finger, they will tend to share similar sub-graphs with minor differences caused by the missed minutiae between them (see Figure IV.3). Whereas shapes obtained from different prints tend to be more different.

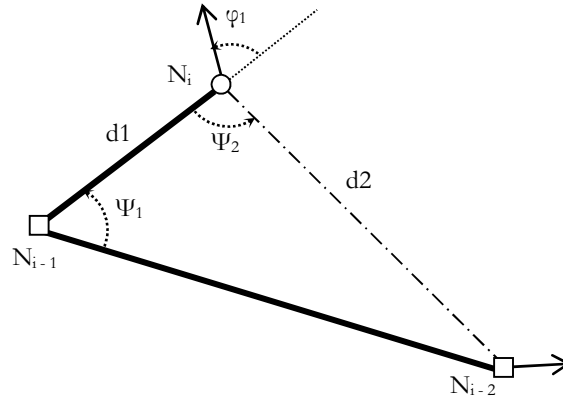


Figure IV.5. A minutia-node descriptor structure N_i consisted of its 2-predecessors nodes N_{i-1} and N_{i-2} .

IV.3.4.1 Minutiae node Descriptor

Based on the structure of the MPS defined in Section IV.3.3, each minutia-node N_i is affected a descriptor similar to that in (Jiang & Yau, 2000) but used here in a dynamic version. It describes the spatial relationships and geometric attributes of the minutiae node N_i with its predecessor nodes in the MPS structure. The feature elements of this descriptor are defined by the distances, directions and radial angles of N_i relative to each of its k -predecessor minutiae nodes in the MPS structure. In the case of $k = 2$, it is defined by (see Figure IV.5):

$$D_{N_i} = (d_1, d_2, \psi_1, \psi_2, \varphi_1) \quad (IV.1)$$

Where $d_1 = d(N_i, N_{i-1})$, $d_2 = d(N_i, N_{i-2})$, ψ_1 and ψ_2 are the angles ($[0, 2\pi]$) in the counterclockwise sense between the two vectors $(\overrightarrow{N_{i-1}N_{i-2}}, \overrightarrow{N_{i-1}N_i})$ and $(\overrightarrow{N_iN_{i-1}}, \overrightarrow{N_iN_{i-2}})$ respectively. Finally, φ_1 is the angle ($[0, 2\pi]$) in the counterclockwise sense between the vector $\overrightarrow{N_{i-1}N_i}$ and the direction axis of the node N_i . It's obvious that the proposed structure is invariant with respect to global transformations.

It's worth noting that a minutiae descriptor must be adaptive to reflect the dynamic changes between fingerprints acquired from the same finger and even from different fingers. In contrast to other minutia-based approaches, the proposed minutia descriptor is not established before the matching algorithm; it is rather calculated during the matching step. In fact, since the MPS structure is subject to be modified by the proposed matching algorithm, as it will be described in the next subsection, the context of a minutiae N_i (that is N_{i-1} and N_{i-2}) is susceptible to be changed. It takes total stability when the matching process is about to examine the underlying node.

The comparison between two minutia-node descriptors D_i and D_j is based on a similarity level S defined as:

$$S(D_i, D_j) = \begin{cases} \frac{Th - |D_i - D_j|}{Th} & \text{if } |D_i - D_j| < th \\ 0 & \text{otherwise} \end{cases} \quad (IV.2)$$

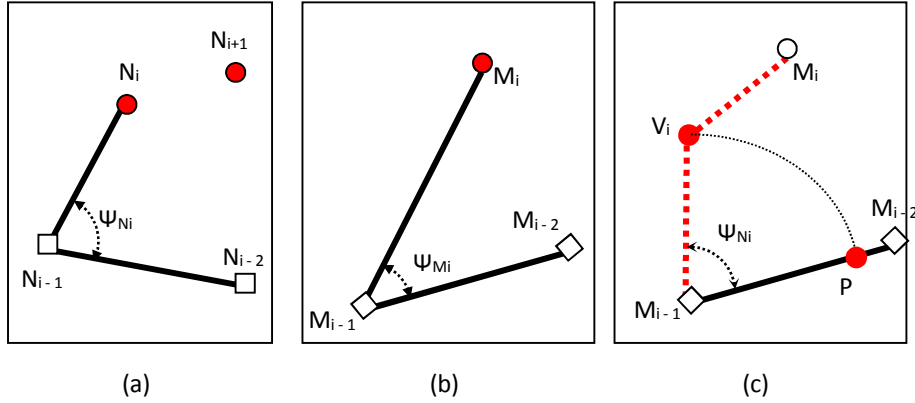


Figure IV.6. Matching of two dynamic descriptors. (a) descriptor of the template node N_i , (b) descriptor of the query node M_i . (c) The new descriptor obtained by adapting (b) to the local context of N_i in (a)

Note that the nodes N_i and M_i are unmatchable and N_{i+1} can match with M_i but its context prevents to be so because N_i is missed in (b). This latter must be adapted by inserting a virtual minutia V_i in the context of M_i to obtain an new descriptor as shown in (c). Now N_{i+1} matches well with N_{i+1}

Where $|D_i - D_j|$ is the Euclidean distance between the two descriptors and th is a threshold vector allowing some tolerance towards deformations. $th = (th_d, th_d, th_\psi, th_\psi, th_\phi)$.

The similarity score verifies the relation $0 < S(D_i, D_j) < 1$.

IV.3.4.2 MPS-Based matching algorithm

Let T and Q denote the template and the query fingerprints with their respective minutiae polysegment structures MPS_T and MPS_Q .

$MPS_T = [N_i; i=1 \dots N]$ Queue of $(N+1)$ minutiae nodes.

$MPS_Q = [M_i; i=1 \dots M]$ Queue of $(M+1)$ minutiae nodes.

Let N_0 and M_0 be the origin nodes of MPS_T and MPS_Q respectively (which constitute the core points of template and query fingerprints respectively). These two nodes are supposed matched pairs. Then, the MPS-based matching process has to compare each node in the MPS_T with exactly its corresponding node in MPS_Q that shares the same index.

Let N_i and M_i two nodes at the index i from MPS_T and MPS_Q respectively. We have two cases:

- The two nodes match with respect to their local descriptors (see next subsection); we mark (N_i, M_i) as real paired minutiae and we go on to examine the next nodes at the index $i+1$ (N_{i+1} and M_{i+1}).
- The two nodes don't match; we conclude that one node corresponds to a missed node in the opposite MPS (see Figure IV.6). To detect which one is missed, we compare the Euclidean distances of each node to its MPS origin (i.e. $d(N_0, N_i)$ and $d(M_0, M_i)$). The node with minimum distance indicates the missed one (see Figure IV.6). We proceed then to insert

a virtual node V_i in the MPS that corresponds to the absent node. The MPS with missed node is called '*destination MPS*', where the MPS with added node is called '*source MPS*'.

Without loss of generality, we suppose hereafter that MPS_T constitutes the source MPS and MPS_Q the destination MPS.

The virtual node V_i has to be inserted in the adequate position so that it reflects the same topological context in the source MPS and conserves the topological context in the destination MPS. That is, it must verify the following conditions:

- 1- Displacement condition : $d(N_{i-1}, N_i) = d(M_{i-1}, V)$
- 2- Rotation condition : $\Psi_{N_i} = \angle N_{i-2} N_{i-1} N_i = \angle M_{i-2} M_{i-1} V$

Consequently, the 2D coordinates of V are:

$$\begin{pmatrix} X_v \\ Y_v \end{pmatrix} = \begin{pmatrix} \cos(\psi_{N_i}) & -\sin(\psi_{N_i}) \\ \sin(\psi_{N_i}) & \cos(\psi_{N_i}) \end{pmatrix} \begin{pmatrix} X_p - X_{M_{i-1}} \\ Y_p - Y_{M_{i-1}} \end{pmatrix} + \begin{pmatrix} X_{M_{i-1}} \\ Y_{M_{i-1}} \end{pmatrix} \quad (IV.3)$$

Where x_p and y_p are the 2D coordinates of the point P resulting from the translation of M_{i-1} towards M_{i-2} with a vector length equal to $d(N_{i-1}, N_i)$ (see Figure IV.6). The pair (N_i, V) is marked as virtual paired minutiae.

The next step is to examine the next node in MPS_T , which is N_{i+1} , with the current node M_i in MPS_Q . The algorithm finishes when one of the two MPS is totally explored.

It is worth noting that the descriptor of the node M_i was defined initially in terms of the two nodes (M_{i-1} and M_{i-2}). But after the detection of the missed node in MPS_Q that should correspond to N_i which is restored with V , the new descriptor of the node M_i will be redefined in terms of (V and M_{i-2}). Consequently, the proposed descriptor is dynamic having the ability to adjust its values according to the corresponding context in the opposite fingerprint. Moreover, thanks to the insertion of V ; the node N_{i+1} in the Figure IV.6 has more chance to be matched with M_i which will maximize the number of pairing minutiae.

Figure IV.7 shows matching results of two genuine fingerprints and their initial and final MPS structures.

IV.3.4.3 Global matching score computation

At the end of the matching process, both MPS_T and MPS_Q are extended with additional virtual nodes such that each node in MPS_T has its correspondent in MPS_Q . So, we distinguish two kinds of pairs of nodes:

- 1- Real Paired nodes: two nodes (N_i, M_i) are called real paired nodes if N_i matches M_i and both N_i and M_i are real minutia-nodes.
- 2- Virtual Paired nodes: two nodes (N_i, M_i) are called virtual paired nodes if N_i corresponds to M_i and one of them is a real minutia-node and the other is a virtual node.

Let note the number of real paired nodes with RPN and the number of virtual paired nodes with VPN. Let Z be the new size of MPS_T (or MPS_Q), we can write:

$$RPN = Z - VPN \quad (IV.4)$$

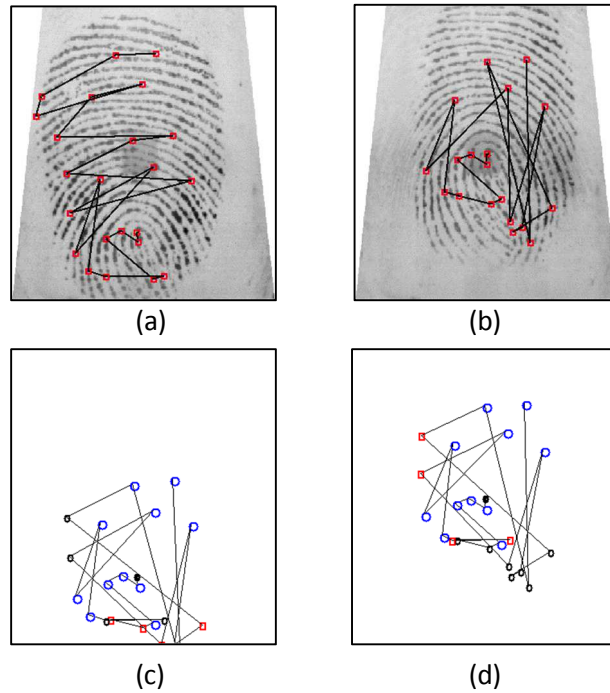


Figure IV.7. Matching results of genuine fingerprints pair. (a) and (b) two fingerprints with their respective MPS; (c) and (d) the final adapted MPSs. Big blue circles are paired nodes whereas squares designate virtual nodes. Note the total similarity between the final MPSs.

RPN increases in case of genuine pairs and decreases in case of impostor pairs, whereas VPN goes inversely. The value of Z is limited by the interval $[\min(M,N), M+N]$. So, one can define the global score as:

$$score = \frac{2 * RPN}{M + N} \quad (IV.5)$$

The Score function tends to be near 1 in case of perfect matching and it is near 0 in case of a total mismatch. A global threshold 'Th_g' between 1 and 0 must be defined in order to decide whether two prints match or not.

IV.4 Complexity analysis and Experimental results

IV.4.1 Complexity analysis

Our matching algorithm goes through two main stages. The first is the MPS construction stage which involves a quick sort algorithm that runs in $O(N \log(N))$ for both prints. The second stage is the MPS-based matching scheme which compares each node in the template MPS with its corresponding node that shares the same index in the query MPS. However, this comparison can involve the process of virtual minutia insertion. In the worst case, which is the case of impostor fingerprint pair, all the nodes of the template MPS could be inserted in the query MPS and inversely. So, the number of nodes examined is $N+M$. Thus, the second stage runs at worse in $O(2N)$. Consequently, the complexity associated with our matching algorithm is $\sim O(N \log(N))$.

The proposed algorithm is very fast compared with some known matching algorithms (see Table IV.1)

IV.4.2 Experimental Results

The fig. 6 shows the results of testing our algorithm on a genuine fingerprint pair from the FVC2002 DB2 database.

Table IV.1 Complexity of the proposed algorithm with some known matching algorithms

Algorithm	Total complexity
(Tico & Kuosmanen, 2003)	$O(kN^2)$
(Das et al., 2012)	$O(N^2)$
(Jain, Hong, & Bolle, 1997)	$O(N^3)$
(Feng, 2008)	$O(N^2)$
Our algorithm	$O(N \log(N))$

Table IV.2 Performance indicators of the proposed algorithm

EER(%)	FMR100(%)	FMR1000(%)	ZeroFmr(%)
22,420	60,000	78,571	86,905

For the evaluation of our algorithm, we have used FVC2004 DB2-A database (Maio, Maltoni, Cappelli, Wayman, & Jain, 2004) consisting of 100 fingers with 8 prints for each one, so a total of 800 fingerprints. The performance indicators, specified in this competition, of our algorithm are summarized in Table IV.2. The parameters used for 'th' are equal to $(12, 12, \pi/6, \pi/6, \pi/8)$. The evolution of the FMR and FNMR in function of threshold Th_g is illustrated by Figure IV.8. The algorithm performs well in case of good fingerprints where the core point is well located. However, if one fingerprint presents bad quality or doesn't contain a core point at all the performance will significantly decrease.

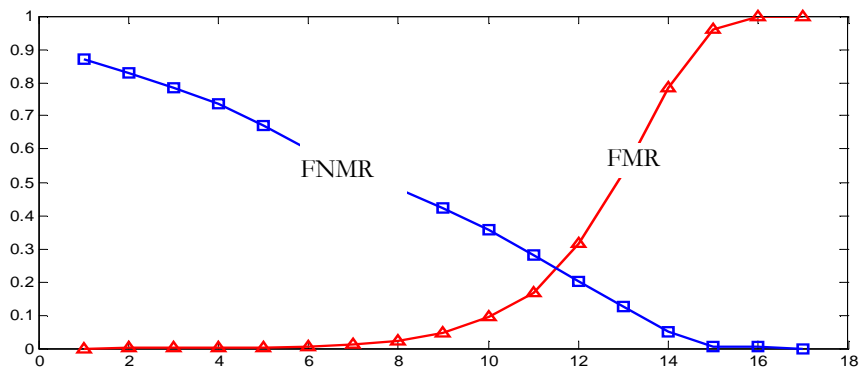


Figure IV.8 Evolution of the FMR and FNMR

IV.5 Conclusion

A fast minutiae-based matching algorithm is proposed in this work. Instead of using the classical correspondence scheme based on a static descriptor which is very vulnerable to erroneous (added/missed) minutiae, the proposed algorithm uses a dynamic descriptor that has the ability to auto adjust its context according to the reference context. This is achieved using the proposed minutiae polysegment structure MPS that allows the matching process to detect any added or missed minutiae between two prints to proceed, later, with virtual minutiae insertion. The algorithm presents a reduced time complexity equivalent to $O(n \cdot \log(n))$. Experimental results on FVC2004 show acceptable performance improvement. However, since it is singular-point dependent algorithm, it performs badly when the print doesn't contain core point or this last one is misdetected. In addition to that, it is sensitive to large skin distortions.

The algorithm can be improved by incorporating an effective deformation scheme to handle high distortions.

Chapter V

Remote fingerprint-based authentication and non-repudiation services for mobile learning systems

Although AFISs are deployed in all areas, they operate locally. That is, both the acquisition and the matching steps as well as identity decision are achieved locally. The proliferation of e-services implies that the user must be identified remotely. The state-of-the-art of the biometrics-based remote authentication is not well established, this latter does not yet exploit the full potentiality of biometrics and still rely on password-based authentication schemes wrapped around PKI infrastructure. Some desired advanced services such as non-repudiation can't be guaranteed.

In this chapter, we discuss a novel fingerprint-based strategy that provides a remote authentication, communication and non-repudiation scheme applied for mobile learning using recent advances in cancelable biometrics. The proposed scheme covers all the learning system steps starting by subscription, communication and assessments.

Although, the proposed algorithm is dealing with mobile learning context, it can be considered as being a general framework to ensure fingerprint-based remote authentication.

V.1 Mobile learning

The recent advances made in mobile technologies have enriched the mobile devices with increasing capabilities. Today's smartphones are characterized by large screens, powerful graphics cards, high computing power processors and a variety of sensors (Figure V.1). It follows that the suitable use of the mobile devices is not limited to voice communication and games; it extends across a large general-purpose applications set such as geo-localization, internet shopping, augmented reality (FitzGerald et al., 2013) and education.

V.1.1 Definition

Mobile learning is the adaptation of education resources and services to the context of the “*current learners*” using the “*ambient technologies*”. In fact, many efforts are made to satisfy the education purposes of current users known to be highly mobile and usually attached to internet via their mobile devices having not enough, or not suitable, time to assist a presential classroom but motivated to learn. This situation imposes the design of new strategies to develop and present

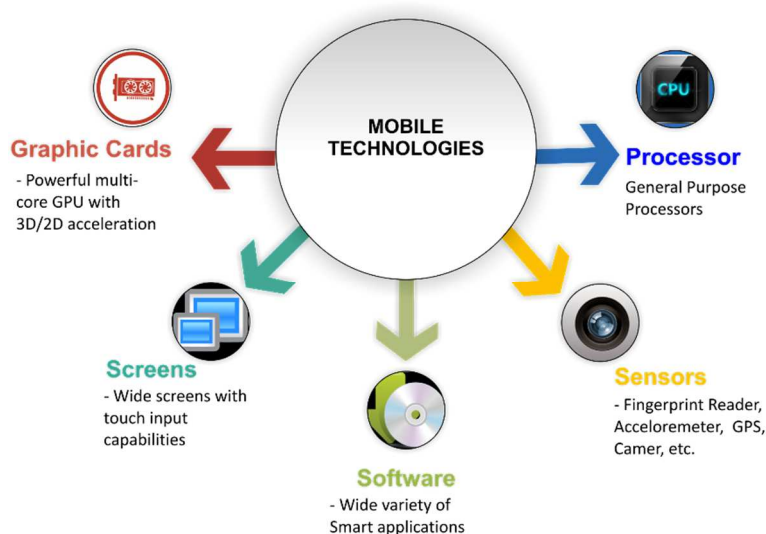


Figure V.1 Recent mobile technology capabilities

courses and related materials that provide better conditions for learning anywhere and at any time.

V.1.2 Current security concerns

Actual m-learning advances have paid little attention to some security issues threatening both the learner and the system privacy. (Kambourakis, 2013) has nicely identified eight challenges relative to the security and privacy of m-learning systems, among which we cite the most critical ones: (1) system and data security and privacy, (2) learner privacy, (3) mobile device related issues and (4) content filtering.

In fact, learners are supposed to access services and consume learning resources using their mobile devices. Some of them can be stored on the mobile or shared with others. At the system point of view, resource access must be granted at any time to genuine users only who must be efficiently authenticated and controlled. At the learner side, contents received must not be harmful to the learner. Serious concerns revolved around the misuse of the mobile devices in case of loose or manipulation by people other than the owner. Therefore, educational institutions, educators, and individual learners may be deeply concerned about the growing threats to data security and privacy (Kambourakis, 2013). Another important issue that should be considered in such systems is related to the non-repudiation. This latter indicates how much the learner and the system are sure of their identities, one relative to the other, when they are transmitting information, one as a the genuine transmitter and the other as a the genuine receiver.

V.1.3 Related works

The state-of-the-art in mobile-learning dealing with security and privacy of both the learning-system and the learner is heavily inherited from the e-learning contexts and the network communication background (Kambourakis, 2013). It is based generally on the classical secret-based methods (passwords, tokens or PKI) (de Medeiros Gualberto & Zorzo, 2010; El-Khatib,

Korba, Xu, & Yee, 2003; Ugray, 2009) which are not strongly suitable in this context. It is commonly known that the issues encountered in m-learning systems are quite different from those known in m-learning since the implication of the mobile devices can reveal more private data and requires far more challenges (Udell & Woodill, 2014).

Some other, but unfortunately few, interesting methods exploit the fact that the recent mobiles are reach in multiples sensors that can be used to securely identify the users using their biometric traits.

In (Kambourakis & Damopoulos, 2013) the authors introduce a dynamic signature-based scheme to ensure a post-authentication and non-repudiation in the m-learning systems. The authors report that the proposed scheme can correctly classify users' signatures in an amount of 95%.

The work in (Adibi, 2010) discusses a multimedia-enriched interactive non-repudiation system involved in a m-learning environment to track users accessing the learning materials and control the identity of the examination attendees.

In (Kambourakis, Damopoulos, Papamartzivanos, & Pavlidakis, 2014) the authors exposed a touchscreen-based key-stroke scheme for identifying users. The reported Equal Error Rate (EER) of 12% indicates low identification precision. The same modality was investigated in (Flori & Kowalski, 2010) to continually identify users in online examination.

(Alotaibi, 2010) proposed a fingerprint-based scheme to ensure that no unauthorized individuals are cheating to give an e-exam.

Other commercial solutions, such as Apple TouchID and Samsung Galaxy S5, propose a built-in fingerprint reader to implement a secure fingerprint-based mobile unlock. Combined with operating system SDK, this solution allows also to identify mobile owner in internet shopping and, so, in mobile learning.

Biometric-based solutions for security and privacy preservation in mobile learning seem to be more promising. However, biometric data are vulnerable. Once a biometric system is compromised, biometric traits are definitively lost and cannot be renewed. As a consequence, the user can be tracked everywhere. In this work, we propose to use recent advances in cancelable fingerprint identification system to propose a strategy to secure communication in mobile learning systems. The proposed scheme offers both secure authentication and non-repudiation services.

The next section introduces some cancelable biometric notions, focusing on fingerprint, after which we present in details our proposed scheme.

V.2 Cancelable biometrics

Biometric authentication is based on comparison of input biometric data against a stored features-template. If this last one is compromised, it can help to reconstruct a fake biometric data to be illegally exploited. Once compromised, the subject's biometrics are definitively lost and cannot be renewed. The success of the authentication system depends heavily on the security of the stored template.

Cancelable biometrics stands for techniques that aim to apply some intentional distortions to the original biometric data to protect the stored template (Maltoni, Maio, Jain, & Prabhakar, 2009). The transformed template is then stored instead of the original ones. More formally, let B the original template features, F the transform function and P the parameters-vector used to generate the transformed template features B_p .

$$B_p = F(B, P) \tag{1}$$

The transformation function F must fulfill three requirements:

- 1- It must preserve acceptable identification accuracy in the transformed domain,
- 2- it must be not invertible to ensure that the original template cannot be recovered back, so F^{-1} does not exist or it is computationally hard to revert it, and
- 3- it allows regenerating new templates if the transformed one is compromised. This new generated template should not match with the compromised one, neither with the original template, to prevent user tracking.

For instance, changing the parameters-vector P , permits a cancelable fingerprint system to generate a multiplicity of non-matchable transformed fingerprint-features based on one original fingerprint. Consequently, users can submit different fingerprint-features, by simply changing the parameters-vector values, to each application system they are concerned with to ensure security independence between applications.

Many algorithms have been proposed to protect fingerprint template. (Ratha, Connell, & Bolle, 2001) were the first who have introduced the notion of cancellable biometrics. They outlined the major weak links in automated biometric systems and they proposed some solutions that have been taken up and elaborated in (Ratha, Chikkerur, Connell, & Bolle, 2007). There, the authors proposed to disorder the minutiae in the 2D space by changing their positions with respect to the singular points locations using three non-invertible functions: Cartesian, polar, and functional surface folding. The authors confirmed that the third function gives best results than the others.

(Lee, Choi, Toh, Lee, & Kim, 2007) proposed an alignment-free cancelable fingerprint templates based on invariant orientation information of a minutia derived from its orientation and its local neighboring regions. The obtained invariant information are moved slightly in distance and orientation using two changing functions as a key for translation and rotation to form the protected template.

(Ahmad, Hu, & Wang, 2011) modified the polar transformation version of (Ratha et al., 2007) to be independent of the global features (core-point) based registration. Instead, a minutia-based polar coordinate system is constructed based on which a local template is generated for each minutiae regarding the others. The template is then rotated, translated and scaled using some parameters as a key to impose a many-to-one transformation.

(Das, Karthik, & Chandra Garai, 2012) described an alignment-free fingerprint hashing algorithm based on minimum distance graphs (MDG). Their protection algorithm is a minutiae-based transformation whose principle is to hide minutiae locations and to exhibit distances between two closest minutiae. The hash graph is generated by connecting each minutia to its closest one

starting from the core-point. To make the template cancellable, they applied the (Lee et al., 2007) shifting scheme.

(Belguechi, Cherrier, Rosenberger, & Ait-Aoudia, 2013a, 2013b) proposed to apply the BioHashing method proposed by (Jin, Ling, & Goh, 2004) to the well-known fingercode in (Jain, Prabhakar, Hong, & Pankanti, 2000) combined with a local minutia descriptor to generate their protected template. These algorithms are enhanced versions of that proposed by the authors in (Belguechi, Rosenberger Christopher, & Samy Ait-Aoudia, 2010). The authors reported good security and matching accuracy performance. To ensure more security in case of key leakage, the obtained protected template is embedded in a smartcard. A cancelable Match on Card (MoC) system is proposed. The notable thing in this work is the rigorous evaluation framework they used to validate their securing scheme.

(Moujahdi, Bebis, Ghouzali, & Rziza, 2014) proposed a minutiae-based representation structure called fingerprint shell to construct their protected template. First, the minutiae are ordered according to their distances to each singular point. A random value is added to the distances list to form the user specific-key. The distances are used to construct several contiguous right angle triangles.

(Prasad & Santhosh Kumar, 2014) generated a protected template by construction of M rectangles with different orientations around each minutia and the calculation of the invariant local relations. A fixed length bit string is then generated which converted into complex vector by applying DFT. To make the template cancellable, the obtained vector is transformed using a specific-user key.

V.3 Fingerprint-based authentication scheme for mobile learning

As modern smartphones are equipped with a built-in fingerprint reader, the proposed method uses the fingerprint modality to secure communication in mobile learning. Other modalities such as voice or face can be also used in this method.

We propose to endow the learning system with an Authentication Authority (AA) that is responsible to authenticate learners, based on their fingerprints, when they request access to the system. Since users does not necessarily trust the AA, their identities must not be used in plain form as authentication data. AA implements the cancelable fingerprint algorithm described by (Ratha et al., 2007) to protect minutiae-based template. It proposes to change the minutiae positions using a one-to-many transformation matrix to get a new transformed template. All transformed fingerprint-based identities of the learners are stocked in a database. So, even if the database is compromised the original fingerprint template cannot be revealed.

The proposed scheme goes through all the learning process steps: (i) subscription (ii) resources access, and (iii) assessment process (Figure V.3).

V.3.1 Subscription

The learner is obliged to subscribe to get authorization to access resources. The subscription step permits the AA to *learn* the identity of the learner. The subscription interface (SI) asks the user to introduce a username that will be sent to AA to be validated. AA generates randomly a transform matrix P associated to the received username and sends it back to SI. The SI asks the user to

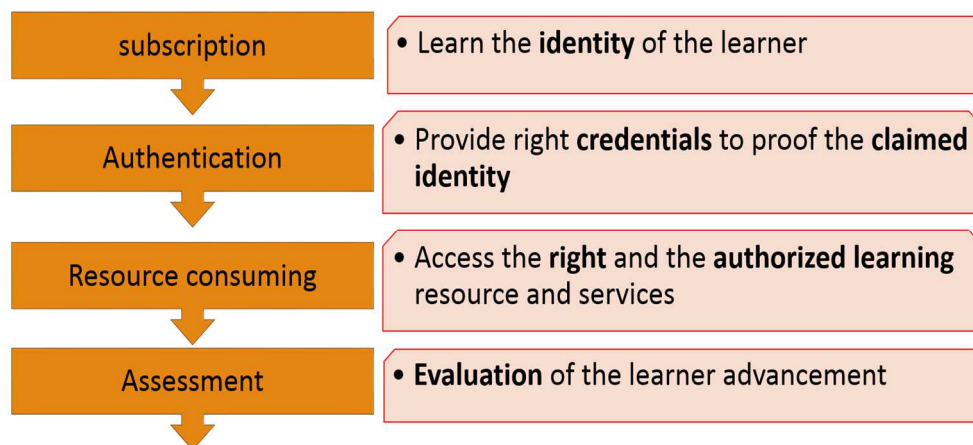


Figure V.2 The learning Process

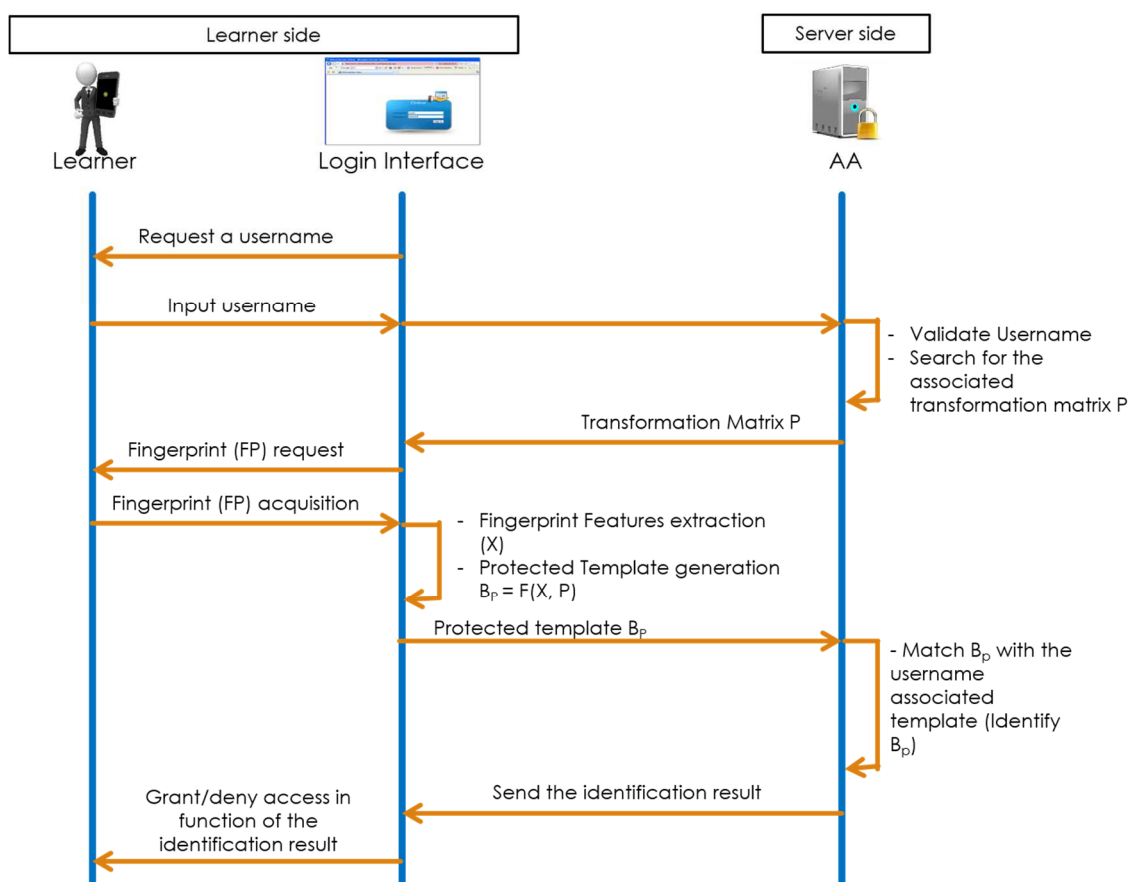


Figure V.3 The subscription process

introduce his fingerprint. This last one is acquired and treated locally after which is transformed using the received matrix P . The resulted transformed template B_p is sent to the AA using a secure encryption algorithm such as RSA or blowfish algorithm. AA, when receiving the template B_p associates it to the username account and confirms the reception of the template.

It is worth noting that this operation must be run at the client side to ensure security issues of the acquired fingerprint. Moreover, all communication must be secured using a secure encryption algorithm.

The same scheme is followed when the user wants to generate a new identifier template H_{p1} . This implies that the subscription interface allows the user to regenerate a new protected template provided that he is already authenticated using the old template B_p as indicated in the next subsection. The process of subscription is indicated in Figure V.3.

V.3.2 Resources access

In this step, the learner is intended to access learning resources. The learner must be authenticated as a genuine user. The login interface (LiI) asks the user to introduce his username, which will be sent to AA. This last validates the existence of the received username and extracts the associated transformation matrix P that will be sent to LiI. This latter inquires the user to introduce his fingerprint, which will be transformed into a protected transformed template using the same algorithm as in subscription step applied to the received parameter P .

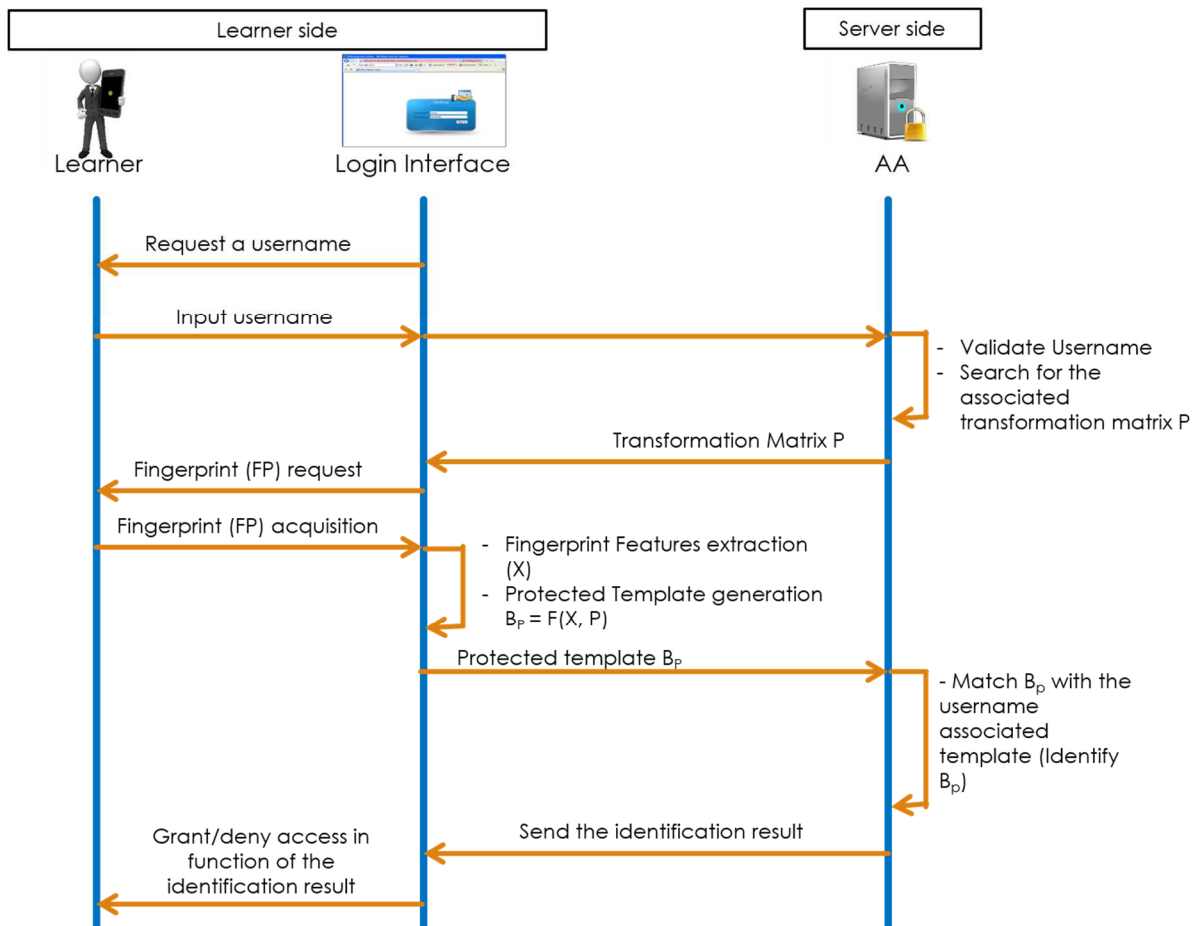


Figure V.4 The authentication process

The resulted template B_p will be sent to AA. At the reception, AA shall identify the user in the database by launching a matching process between B_p as a query template and the stored template associated to the user. The user is granted the access in function of the identification results. The process of accessing resources is indicated in Figure V.4.

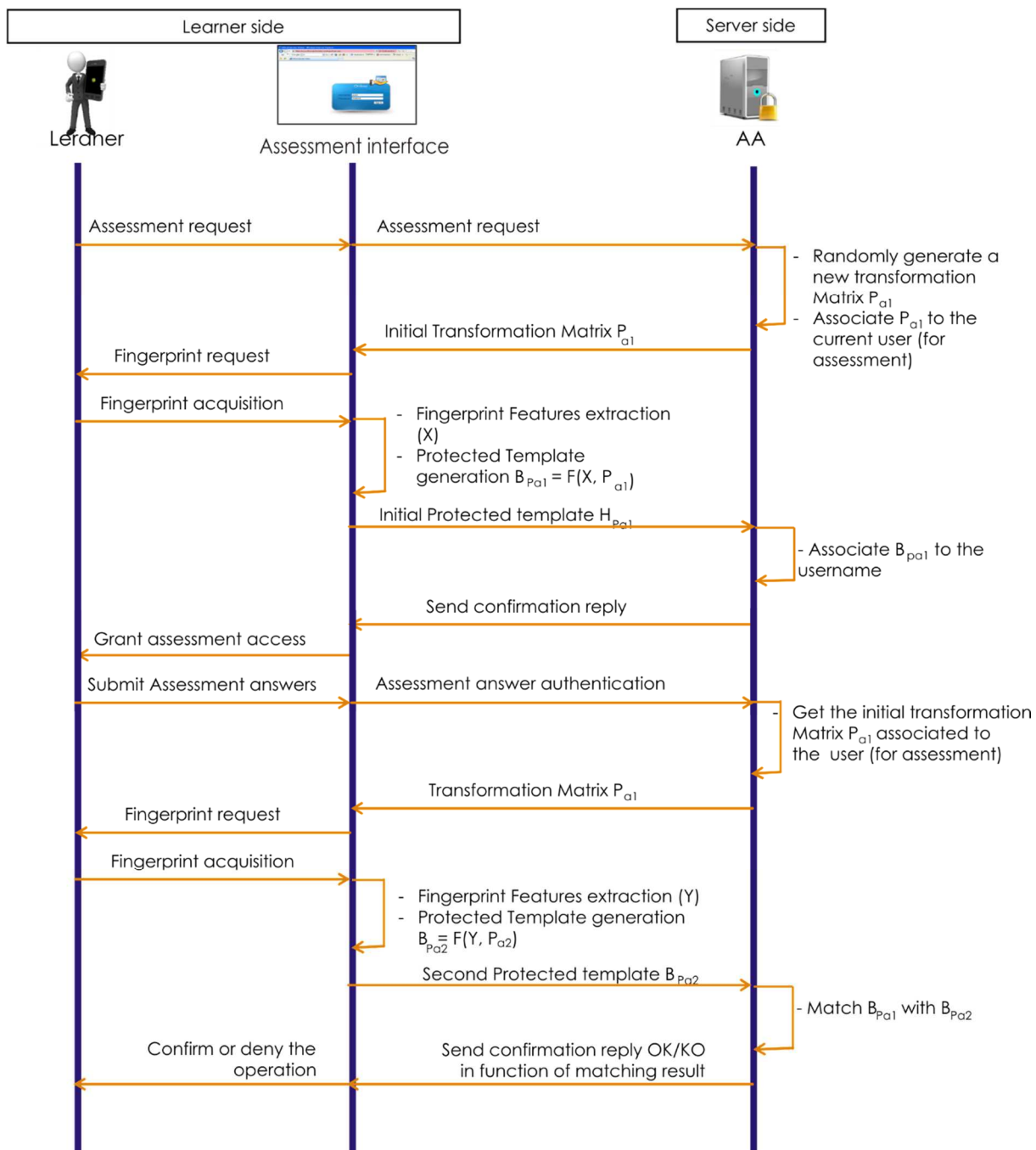


Figure V.5 The assessment process

V.3.3 Assessment process

The assessment process requires a non-repudiation service to ensure that the submitter of the assessment answers is the same learner who was already authenticated to perform the assessment process. In addition to that, the learning system cannot deny the user submission of its assessment answers. The process of non-repudiation is indicated in Figure V.5.

When asking for an assessment, the learner must be logged in first as described in the previous subsection. Once logged in, the learner requests an exercise, the assessment interface (AI) sends the username to AA. This latter randomly generates a new temporary transformation matrix P_{a1} , associates it to the username and sends it back to AI. AI asks the user to authenticate secondly and generates a new protected template B_{pa1} , using the same fingerprint cancelable algorithm applied to the matrix P_{a1} , that will be sent to AA. This last one stores B_{pa1} associated with its username.

When submitting the assessment answers, the logged in learner has to provide a transformed template that matches B_{pa1} in order to complete the submission process. This ensures that the person who initially asked for the assessment is the same person who is submitting the answers. At the reception of the assessment answers, the system replies by a confirmation message.

The above process can be repeated for each exercise constituting the assessment.

V.4 Conclusion

In this chapter, we have discussed a fingerprint-based scheme to provide a solution to some security and privacy issues in mobile-learning systems using recent advances in cancelable fingerprint systems. The proposed scheme ensures security in all learning process, particularly in subscription, resources accessing and assessment process. Secure authentication and non-repudiation services are proposed. The system can be further developed to be applied in a real mobile learning case-study based on online labs.

One principal merit of the proposed scheme is that can be viewed as a general framework to secure remote resources.

Conclusion

Biometric identification systems are proposed as a more secure alternative to classical authentication systems based on knowledge or tokens. Behavioral and/or physiological characteristics, unique to each person, are collected to build the biometric data used in identification. Fingerprint, as a leading biometric identification modality since centuries, is widely adopted in many identification systems thanks to its trade-off between other modalities in terms of acceptability, accuracy, security and low-cost technology. It largely enhanced their security aspects.

In this thesis, we were particularly interested in minutiae-based automated fingerprint identification systems. Although, these systems are now of mature technologies, some challenging issues need further improvements.

In this thesis, we have basically focused on three main problems:

- 1- Singularity detection: We have developed an efficient algorithm to detect singular points in fingerprint images. Our idea is based on the observation that the orientation field (OF) at the regions containing singular points has high variation whereas in the other regions it is smooth. Thus, a pixel-wise descriptor, that comprises orientation-deviation based features, is proposed to measure the OF variation in the local neighborhood of a pixel which we call OF energy. Candidate singular points are characterized by locations where the OF energy function has local gradual maxima. Furthermore, the orientation-deviation based descriptor exhibits some advanced topological properties, in particular, the descriptor profile tendency, which are highly correlated with the singularity type. These properties are used to filter out some spurious detected singular points. A second refining step based on an extended Poincaré Index is then applied to keep only genuine singular points with their information. The proposed algorithm has the ability to detect accurately the classical singularities as well as the arch-type defined singularity. Experiments conducted over the public databases FVC2002 db1 and db2 confirm its accuracy and reliability with reduced False Alarm Rate in comparing to other proposed methods.
- 2- Effect of the added/missed minutiae on the matching algorithm: added or missed minutiae have a direct influence on the stability of the local minutiae descriptor and, so, on its matching power. In this thesis, we have considered the presence of spurious minutiae and the absence of genuine ones as an inevitable problem even with reliable minutiae extraction algorithm and the subsequent enhancement techniques applied. Hence, rather to invest more in enhancement, that can add more spurious minutiae, it is wisely preferable to consider it as true minutia. Thus, we have proposed an adaptive minutia descriptor that can change its features as the matching process evolves in comparison. A stable geometric structure is proposed that permits to detect any added minutiae between two fingerprint impressions. Once an added minutia is detected in an impression it is directly inserted in the structure of the second that permits to update the minutiae descriptor features. This strategy can be

viewed as being a general framework in which other algorithms can be integrated to handle the added missed minutiae problem.

- 3- Remote fingerprint authentication: we have presented a fingerprint-based remote authentication scheme to secure access to remote resources. Although the proposed algorithm is designed to mobile-learning systems, it can be easily adapted to any distributed systems where resources are accessed remotely, in particular, cloud-based ones. The algorithm predicts an authentication authority that is responsible for user authentication. Since the user doesn't trust the underlying infrastructure to provide his fingerprint in plain form as a mean of authentication, the system uses a transformed version of the user fingerprint to be sent to AA. This achieved by exploiting recent advances in cancellable fingerprints that permit to create distorted fingerprint features from an original fingerprint using some parameters along with the matching accuracy is preserved. Inherited from the fingerprint characteristics, a non-repudiation service is rigorously established in the proposed algorithm.

The present work is still extensible to many researches:

- Classification of fingerprints databases based on the proposed orientation deviation descriptor. This helps a lot to accelerate the automated fingerprint identification applied to large scale databases.
- Integrate and evaluate the proposed adaptive descriptor into a matching framework with along many state-the-art algorithms.
- Propose a template securing algorithm to enhance the privacy of fingerprint data stored in databases.
- Generalize the proposed remote authentication service based on fingerprints and propose a working implementation design.

Bibliography

- Adibi, S. (2010). A remote interactive non-repudiation multimedia-based m-learning system. *Telematics and Informatics*, 27(4), 377–393.
- Ahmad, T., Hu, J., & Wang, S. (2011). Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition*, 44(10-11), 2555–2564. <http://doi.org/10.1016/j.patcog.2011.03.015>
- Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. (2005). An enhanced gabor filter-based segmentation algorithm for fingerprint recognition systems. In *Proc. IEEE Intl. Symposium on Image and Signal Processing and Analysis, ISPA, Spec. Sess on. Signal Image Processing for Biometrics, IEEE Press, Zagreb (Croatia), September 2005* (pp. 239–244).
- Alotaibi, S. (2010). Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment. *The 4th Saudi International Conference*.
- Baruch, O. (1988). Line thinning by line following. *Pattern Recognition Letters*, 8(4), 271–276.
- Bazen, A. M., & Gerez, S. H. (2001). Segmentation of fingerprint images. In *Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2001)* (Vol. 276280).
- Bazen, A. M., & Gerez, S. H. (2002). Systematic methods for the computation of the directional fields and singular points of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(7), 905–919.
- Belguechi, R., Cherrier, E., Rosenberger, C., & Ait-Aoudia, S. (2013a). An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates. *Computers and Security*, 39(PART B), 325–339. <http://doi.org/10.1016/j.cose.2013.08.009>
- Belguechi, R., Cherrier, E., Rosenberger, C., & Ait-Aoudia, S. (2013b). Operational bio-hash to preserve privacy of fingerprint minutiae templates. *IET Biometrics*, 2(2), 76–84.
- Belguechi, R., Rosenberger Christopher, & Samy Ait-Aoudia. (2010). Biohashing for Securing Minutiae Template. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (pp. 1168–1171). <http://doi.org/10.1109/ICPR.2010.292>
- Belhadj, F., Ait-Aoudia, S., & Akrouf, S. (2015). Secure Fingerprint-based authentication and non-repudiation services for mobile learning systems. In *Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on* (pp. 200–204). <http://doi.org/10.1109/IMCTL.2015.7359586>
- Belhadj, F., Akrouf, S., Harous, S., & Ait-Aoudia, S. (2015). Efficient fingerprint singular points detection algorithm using orientation-deviation features. *Journal of Electronic Imaging*, 24(3), 033016. <http://doi.org/10.1117/1.JEI.24.3.033016>
- Bengueddoudj, A., Akrouf, S., Belhadj, F., & Nada, D. (2013). Improving fingerprint minutiae matching using local and global structures. In *8th International Workshop on Systems, Signal Processing and Their Applications, WoSSPA 2013* (pp. 279–282). <http://doi.org/10.1109/WoSSPA.2013.6602376>
- Bolle, R. M., Senior, A. W., Ratha, N. K., & Pankanti, S. (2002). Fingerprint minutiae: A constructive definition. In *Biometric Authentication* (pp. 58–66). Springer.
- Bosworth, S., Kabay, M. E., & Whyne, E. (2014). *Computer security handbook* (Six editio). y John Wiley & Sons, Inc., Hoboken, New Jersey.
- Campisi, P. (2013). *Security and Privacy in Biometrics*. Springer-Verlag London. <http://doi.org/10.1007/978-1-4471-5230-9>

- Cappelli, R., Ferrara, M., Franco, A., & Maltoni, D. (2007). Fingerprint verification competition 2006. *Biometric Technology Today*, 15(7), 7–9.
- Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 32(12), 2128–2141.
- Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. (1999). Fingerprint classification by directional image partitioning. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 21(5), 402–421.
- Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. (2007). Fingerprint Image Reconstruction from Standard Templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(9), 1489–1503. <http://doi.org/10.1109/TPAMI.2007.1087>
- Cavusouglu, A., & Görgünouglu, S. (2008). A fast fingerprint image enhancement algorithm using a parabolic mask. *Computers & Electrical Engineering*, 34(3), 250–256.
- Chen, J., & Moon, Y.-S. (2007). A minutiae-based fingerprint individuality model. In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on* (pp. 1–7).
- Chen, J., & Moon, Y.-S. (2008). The statistical modelling of fingerprint minutiae distribution with implications for fingerprint individuality studies. In *Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on* (pp. 1–7). <http://doi.org/10.1109/CVPR.2008.4587399>
- Chen, Y., & Jain, A. (2009). Beyond Minutiae: A Fingerprint Individuality Model with Pattern, Ridge and Pore Features. In M. Tistarelli & M. Nixon (Eds.), *Advances in Biometrics SE - 54* (Vol. 5558, pp. 523–533). Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-01793-3_54
- Chikkerur, S., Cartwright, A. N., & Govindaraju, V. (2007). Fingerprint enhancement using STFT analysis. *Pattern Recognition*, 40(1), 198–211.
- Chikkerur, S., Govindaraju, V., Pankanti, S., Bolle, R., & Ratha, N. (2005). Novel approaches for minutiae verification in fingerprint images. In *Application of Computer Vision, 2005. WACV/MOTIONS'05 Volume 1. Seventh IEEE Workshops on* (Vol. 1, pp. 111–116).
- Chikkerur, S., & Ratha, N. (2005). Impact of singular point detection on fingerprint matching performance. In *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on* (pp. 207–212).
- Chua, S. C., Wong, E. K., & Tan, A. W. C. (2015). Fingerprint Ridge Distance Estimation: A Mathematical Modeling. *International Journal of Computer Applications*, 126(15).
- Daluz, H. M. (2014). *Fundamentals of Fingerprint Analysis*. Taylor & Francis. Retrieved from <https://books.google.dz/books?id=p4xqBAAAQBAJ>
- Das, D., & Mukhopadhyay, S. (2015). A Pixel Based Segmentation Scheme for Fingerprint Images. In *Information Systems Design and Intelligent Applications* (pp. 439–448). Springer.
- Das, P., Karthik, K., & Chandra Garai, B. (2012). A Robust Alignment-free Fingerprint Hashing Algorithm Based on Minimum Distance Graphs. *Pattern Recogn.*, 45(9), 3373–3388. <http://doi.org/10.1016/j.patcog.2012.02.022>
- Dass, S. (2014). Individuality of Fingerprints: A Review. In S. Z. Li & A. K. Jain (Eds.), *Encyclopedia of Biometrics SE - 58-2* (pp. 741–751). Springer US. http://doi.org/10.1007/978-3-642-27733-7_58-2
- Dass, S. C. (2004). Markov random field models for directional field and singularity extraction in fingerprint images. *Image Processing, IEEE Transactions on*, 13(10), 1358–1367.
- de Medeiros Gualberto, T., & Zorzo, S. D. (2010). Service for secure and protected applications in Collaborative Learning Environments. In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on* (pp. 2419–2426).
- Deng, H., & Huo, Q. (2005). Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching. In *Audio-and Video-Based Biometric Person Authentication* (pp. 270–278).

- E. R. Henry. (1990). *Classification and Uses of Finger Prints*. Routledge, London.
- El-Khatib, K., Korba, L., Xu, Y., & Yee, G. (2003). Privacy and Security in E-Learning. *International Journal of Distance Education Technologies*, 1(4), 1–19.
- Feng, J. (2008). Combining minutiae descriptors for fingerprint matching. *Pattern Recognition*, 41(1), 342–352. <http://doi.org/http://dx.doi.org/10.1016/j.patcog.2007.04.016>
- Ferreira, P. M., Sequeira, A. F., & Rebelo, A. (2015). A Fuzzy C-Means Algorithm for Fingerprint Segmentation. In *Pattern Recognition and Image Analysis* (pp. 245–252). Springer.
- FitzGerald, E., Ferguson, R., Adams, A., Gaved, M., Mor, Y., & Thomas, R. (2013). Augmented reality and mobile learning: the state of the art. *International Journal of Mobile and Blended Learning*, 5(4), 43–58.
- Flior, E., & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on* (pp. 488–492).
- Fournier, N. A., & Ross, A. H. (2015). Sex, Ancestral, and pattern type variation of fingerprint minutiae: A forensic perspective on anthropological dermatoglyphics. *American Journal of Physical Anthropology*.
- Fronthaler, H., Kollreider, K., & Bigun, J. (2008). Local features for enhancement and minutiae extraction in fingerprints. *Image Processing, IEEE Transactions on*, 17(3), 354–363.
- Golabi, S., Saadat, S., Helfroush, M. S., & Tashk, A. (2012). A novel thinning algorithm with fingerprint minutiae extraction capability. *International Journal of Computer Theory and Engineering*, 4(4), 514–517.
- Gonzalez, R. C. (2009). *Digital image processing*. Pearson Education India.
- Gottschlich, C. (2012). Curved-region-based ridge frequency estimation and curved Gabor filters for fingerprint image enhancement. *Image Processing, IEEE Transactions on*, 21(4), 2220–2227.
- Gottschlich, C., & Schoonlieb, C.-B. (2012). Oriented diffusion filtering for enhancing low-quality fingerprint images. *Biometrics, IET*, 1(2), 105–113. <http://doi.org/10.1049/iet-bmt.2012.0003>
- Govindaraju, V., Shi, Z., & Schneider, J. (2003). Feature extraction using a chaincoded contour representation of fingerprint images. In *Audio-and Video-Based Biometric Person Authentication* (pp. 268–275).
- Harrell, E., & Langton, L. (2015). Victims of identity theft, 2014. *U.S. Department of Justice*.
- Henry, E. R. (1905). *Classification and uses of finger prints*. HM Stationery Office.
- Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint Image Enhancement: Algorithm and Performance Evaluation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 20(8), 777–789. <http://doi.org/10.1109/34.709565>
- Hsieh, C.-T., Lai, E., & Wang, Y.-C. (2003). An effective algorithm for fingerprint image enhancement based on wavelet transform. *Pattern Recognition*, 36(2), 303–312.
- Huang, C.-Y., Liu, L., & Hung, D. C. D. (2007). Fingerprint analysis and singular point detection. *Pattern Recognition Letters*, 28(15), 1937–1945.
- Humbe, V., Gornale, S. S., Manza, R., & Kale, K. V. (2007). Mathematical morphology approach for genuine fingerprint feature extraction. *Int. Journal of Computer Science and Security (IJCSS)*, 1, 53–59.
- Hung, D. C. D. (1993). Enhancement and feature purification of fingerprint images. *Pattern Recognition*, 26(11), 1661–1671.
- ICAO. (2015). Machine Readable Travel Documents. Retrieved December 18, 2015, from <http://www.icao.int/publications/pages/publication.aspx?docnum=9303>
- ISO/IEC19794-2:2005. (2005). *Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data* (2nd Editio).
- ISO/IEC2382-37. (2012). Information technology — Vocabulary — Part 37: Biometrics.
- Jain, A., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(4), 302–314.

- Jain, A. K., Chen, Y., & Demirkus, M. (2007). Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(1), 15–27. <http://doi.org/10.1109/TPAMI.2007.250596>
- Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*. Springer Science & Business Media.
- Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (1999). FingerCode: a filterbank for fingerprint representation and matching. In *Computer Vision and Pattern Recognition, 1999. IEEE Computer Society Conference on*. (Vol. 2).
- Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *Image Processing, IEEE Transactions on*, 9(5), 846–859.
- Jain, A. K., Prabhakar, S., & Ross, A. (1999). Fingerprint matching: Data acquisition and performance evaluation. *Dept. of Computer Science, Michigan State Univ., East Lansing, Tech. Rep. MSU-CPS-99--14*.
- Jea, T.-Y., & Govindaraju, V. (2005). A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10), 1672–1684.
- Jiang, X., & Yau, W.-Y. (2000). Fingerprint minutiae matching based on the local and global structures. In *Pattern recognition, 2000. Proceedings. 15th international conference on* (Vol. 2, pp. 1038–1041).
- Jiang, X., Yau, W.-Y., & Ser, W. (2001). Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge. *Pattern Recognition*, 34(5), 999–1013.
- Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11), 2245–2255. <http://doi.org/http://dx.doi.org/10.1016/j.patcog.2004.04.011>
- John, V. R. (2003). *Identity theft*. Upper Saddle River, NJ Prentice Hall PTR.
- Journal Officiel, Arrêté du Aouel Safar 1433 correspondant au 26 décembre 2011. (2011). *Journal Officiel de La République Algérienne Démocratique et Populaire*, 26–29.
- Kambourakis, G. (2013). Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *International Journal of U-and E-Service, Science and Technology*, 6(3), 67–84.
- Kambourakis, G., & Damopoulos, D. (2013). A competent post-authentication and non-repudiation biometric-based scheme for m-learning. In *Proceedings of the 10th LASTED International Conference on Web-based Education (WBE 2013)*, ACTA Press: Innsbruck, Austria.
- Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2014). Introducing touchstroke: keystroke-based authentication system for smartphones. *Security and Communication Networks*.
- Kamei, T. (2004). Image Filter Design for Fingerprint Enhancement. In N. Ratha & R. Bolle (Eds.), *Automatic Fingerprint Recognition Systems SE - 6* (pp. 113–126). Springer New York. http://doi.org/10.1007/0-387-21685-5_6
- Kass, M., & Witkin, A. (1987). Analyzing oriented patterns. *Computer Vision, Graphics, and Image Processing*, 37(3), 362–385.
- Kekre, H. B., & Bharadi, V. A. (2010). Fingerprint core point detection algorithm using orientation field based multiple features. *International Journal of Computer Applications (0975-8887) Volume*.
- Khan, M. A., Khan, A., Mahmood, T., Abbas, M., & Muhammad, N. (2010). Fingerprint image enhancement using Principal Component Analysis (PCA) filters. In *Information and Emerging Technologies (ICIET), 2010 International Conference on* (pp. 1–6). <http://doi.org/10.1109/ICIET.2010.5625686>
- Khazaee, H., & Mohades, A. (2007). A novel fingerprint matching and classification schema based on nested convex polygons. *International Journal of Mathematics and Computer in Simulation*.
- Klein, S., Bazen, A., & Veldhuis, R. (2002). Fingerprint image segmentation based on hidden Markov models. In *Proceedings of 13th Annual Workshop on Circuits, Systems and Signal Processing* (pp. 310–318).
- Krishan, K., Kanchan, T., & Bumrah, G. S. (2012). The Fingerprint Sourcebook. *Journal of Forensic and Legal*

- Medicine*, 19(3), 182–183. <http://doi.org/10.1016/j.jflm.2011.12.018>
- Kumar, R., & Vikram, B. R. D. (2010). Fingerprint matching using multi-dimensional ANN. *Engineering Applications of Artificial Intelligence*, 23(2), 222–228.
- Kwon, D., Yun, I. D., Kim, D. H., & Lee, S. U. (2006). Fingerprint matching method using minutiae clustering and warping. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on* (Vol. 4, pp. 525–528).
- Lam, L., Lee, S.-W., & Suen, C. Y. (1992). Thinning methodologies—a comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 14(9), 869–885.
- Lee, C., Choi, J. Y., Toh, K. A., Lee, S., & Kim, J. (2007). Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 37(4), 980–992. <http://doi.org/10.1109/TSMCB.2007.896999>
- Lee, H. C., Ramotowski, R., & Gaensslen, R. E. (2001). *Advances in Fingerprint Technology, Second Edition*. CRC Press. Retrieved from <https://books.google.dz/books?id=xFnMBQAAQBAJ>
- Lee, V. M. (2015). Fraud Reduction, Applications. In S. Li & A. Jain (Eds.), *Encyclopedia of Biometrics SE - 909* (pp. 735–739). Springer US. http://doi.org/10.1007/978-1-4899-7488-4_909
- Li, D., Wu, X., & He, X. (2014). Depth-based thinning: A new non-iterative skeletonization algorithm for 2D digital images. In *Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on* (pp. 1193–1197). <http://doi.org/10.1109/ICIEA.2014.6931347>
- Li, Z., Wang, R., & Zhang, Z. (2013). Modified Binary Image Thinning Using Template-Based PCNN. In W. Lu, G. Cai, W. Liu, & W. Xing (Eds.), *Proceedings of the 2012 International Conference on Information Technology and Software Engineering SE - 77* (Vol. 212, pp. 731–740). Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-34531-9_77
- Liang, X., Bishnu, A., & Asano, T. (2005). A near-linear time algorithm for binarization of fingerprint images using distance transform. In *Combinatorial Image Analysis* (pp. 197–208). Springer.
- Maio, D., & Maltoni, D. (1997). Direct gray-scale minutiae detection in fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(1), 27–40.
- Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002a). FVC2000: Fingerprint verification competition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(3), 402–412.
- Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002b). FVC2002: Second Fingerprint Verification Competition. In *Proceedings of the 16th International Conference on Pattern Recognition (ICPR'02) Volume 3 - Volume 3* (p. 30811–). Washington, DC, USA: IEEE Computer Society. Retrieved from <http://dl.acm.org/citation.cfm?id=839291.842963>
- Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004). FVC2004: Third Fingerprint Verification Competition.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition* (2nd ed.). Springer Publishing Company, Incorporated. <http://doi.org/10.1007/978-1-84882-254-2>
- Mehetre, B. M., & Chatterjee, B. (1989). Segmentation of fingerprint images—a composite method. *Pattern Recognition*, 22(4), 381–385. [http://doi.org/10.1016/0031-3203\(89\)90047-2](http://doi.org/10.1016/0031-3203(89)90047-2)
- Mei, Y., Sun, H., & Xia, D. (2009). A gradient-based combined method for the computation of fingerprints' orientation field. *Image and Vision Computing*, 27(8), 1169–1177.
- Miller, A. (2015). *Current and Future Uses of Biometric Data and Technologies*.
- Moujahdi, C., Bebis, G., Ghouzali, S., & Rziza, M. (2014). Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognition Letters*, 45(1), 189–196. <http://doi.org/10.1016/j.patrec.2014.04.001>
- Nagar, A., Choi, H., & Jain, A. K. (2012). Evidential value of automated latent fingerprint comparison: an empirical approach. *Information Forensics and Security, IEEE Transactions on*, 7(6), 1752–1765.

- Nanavati, S., Thieme, M., Raj, N., & Nanavati, R. (2002). *Biometrics: Identity Verification in a Networked World*. New York, NY, USA: John Wiley & Sons, Inc.
- Newton, D. E. (2008). *DNA evidence and forensic science*. New York: Facts On File. Retrieved from <http://site.ebrary.com/id/10315335>
- Nilsson, K., & Bigun, J. (2002). Complex filters applied to fingerprint images detecting prominent symmetry points used for alignment. In *Biometric authentication* (pp. 39–47). Springer.
- NIST_DB. (n.d.). Biometric Special Databases and Software from the Image Groupe - http://www.nist.gov/itl/iad/ig/special_dbases.cfm. Retrieved January 16, 2016, from http://www.nist.gov/itl/iad/ig/special_dbases.cfm
- O’Gorman, L., & Nickerson, J. V. (1988). Matched filter design for fingerprint image enhancement. In *Acoustics, Speech, and Signal Processing, 1988. ICASSP-88., 1988 International Conference on* (pp. 916–919).
- Pankanti, S., Prabhakar, S., & Jain, A. K. (2002). On the individuality of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(8), 1010–1025.
- Park, C.-H., Lee, J.-J., Smith, M. J. T., & Park, K.-H. (2006). Singular point detection by shape analysis of directional fields in fingerprints. *Pattern Recognition*, 39(5), 839–855.
- Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable Biometrics: A review. *Signal Processing Magazine, IEEE*, 32(5), 54–65. <http://doi.org/10.1109/MSP.2015.2434151>
- Peralta, D., Galar, M., Triguero, I., Miguel-Hurtado, O., Benitez, J. M., & Herrera, F. (2014). Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms. *Engineering Applications of Artificial Intelligence*, 32, 37–53.
- Prasad, M. V. N. K., & Santhosh Kumar, C. (2014). Fingerprint template protection using multiline neighboring relation. *Expert Systems with Applications*, 41(14), 6114–6122. <http://doi.org/10.1016/j.eswa.2014.04.020>
- Qi, J., & Wang, Y. (2005). A robust fingerprint matching method. *Pattern Recognition*, 38(10), 1665–1671.
- Quan, F. Q. F., Fei, S. F. S., Anni, C. A. C., & Feifei, Z. F. Z. (2008). Cracking Cancelable Fingerprint Template of Ratha. *2008 International Symposium on Computer Science and Computational Technology*, 2, 572–575. <http://doi.org/10.1109/ISCST.2008.226>
- Ratha, N. K., Bolle, R. M., Pandit, V. D., & Vaish, V. (2000). Robust fingerprint authentication using local structural similarity. In *Applications of Computer Vision, 2000, Fifth IEEE Workshop on*. (pp. 29–34).
- Ratha, N. K., Chen, S., & Jain, A. K. (1995). Adaptive flow orientation-based feature extraction in fingerprint images. *Pattern Recognition*, 28(11), 1657–1672.
- Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating Cancelable Fingerprint Templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4), 561–572. <http://doi.org/10.1109/TPAMI.2007.1004>
- Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634. <http://doi.org/10.1147/sj.403.0614>
- Rattani, A., Chen, C., & Ross, A. (2014). Evaluation of Texture Descriptors for Automated Gender Estimation from Fingerprints. In *Computer Vision-ECCV 2014 Workshops* (pp. 764–777).
- Reddy, Y. P., Tiwari, K., Kaushik, V. D., & Gupta, P. (2015). An Efficient Fingerprint Minutiae Detection Algorithm. In *Security in Computing and Communications* (pp. 186–194). Springer.
- Schuckers, M. E. (2010). *Computational Methods in Biometric Authentication: Statistical Methods for Performance Evaluation*. Springer Science & Business Media.
- Sedgewick, R. (2002). *Algorithms in Java, Parts 1-4*. Addison-Wesley Professional.
- Shaikh, S., Saeed, K., & Chaki, N. (2013). Performance Benchmarking of Different Binarization Techniques for Fingerprint-Based Biometric Authentication. In R. Burduk, K. Jackowski, M. Kurzynski, M.

- Wozniak, & A. Zolnierak (Eds.), *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013 SE - 23* (Vol. 226, pp. 237–246). Springer International Publishing. http://doi.org/10.1007/978-3-319-00969-8_23
- Sherlock, B. G., & Monro, D. M. (1993). A model for interpreting fingerprint topology. *Pattern Recognition*, 26(7), 1047–1055.
- Sherlock, B. G., Monro, D. M., & Millard, K. (1994). Fingerprint enhancement by directional Fourier filtering. In *Vision, Image and Signal Processing, IEE Proceedings-* (Vol. 141, pp. 87–94).
- Srinivasan, V. S., & Murthy, N. N. (1992). Detection of singular points in fingerprint images. *Pattern Recognition*, 25(2), 139–153.
- Stoney, D. A. (1988). Distribution of epidermal ridge minutiae. *American Journal of Physical Anthropology*, 77(3), 367–376.
- Su, C., & Srihari, S. N. (2008). Generative models for fingerprint individuality using ridge models. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1–4).
- Sutthiwichaiorn, P., & Areekul, V. (2013). Adaptive boosted spectral filtering for progressive fingerprint enhancement. *Pattern Recognition*, 46(9), 2465–2486. <http://doi.org/http://dx.doi.org/10.1016/j.patcog.2013.02.002>
- Tian, J., Zhang, Y., & Cao, K. (2015). Fingerprint Matching, Automatic. In S. Li & A. Jain (Eds.), *Encyclopedia of Biometrics SE - 54* (pp. 649–655). Springer US. http://doi.org/10.1007/978-1-4899-7488-4_54
- Tico, M., & Kuosmanen, P. (2003). Fingerprint matching using an orientation-based minutia descriptor. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(8), 1009–1014.
- Tico, M., Onnia, V., & Kuosmanen, P. (2002). Fingerprint image enhancement based on second directional derivative of the digital image. *EURASIP Journal on Applied Signal Processing*, 2002(1), 1135–1144.
- Udell, C., & Woodill, G. (2014). *Mastering Mobile Learning*. Wiley Online Library.
- Ugray, Z. (2009). Security and privacy issues in mobile learning. *International Journal of Mobile Learning and Organisation*, 3(2), 202–218.
- Wahab, A., Chin, S. H., & Tan, E. C. (1998). Novel approach to automated fingerprint recognition. In *Vision, Image and Signal Processing, IEE Proceedings-* (Vol. 145, pp. 160–166).
- Wang, J., Olsen, M. A., & Busch, C. (2014). Finger image quality based on singular point localization. In *SPIE Defense+ Security* (p. 907503).
- Wang, L., & Dai, M. (2007). Application of a new type of singular points in fingerprint classification. *Pattern Recognition Letters*, 28(13), 1640–1650.
- Wang, Y., Hu, J., & Han, F. (2007). Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields. *Applied Mathematics and Computation*, 185(2), 823–833.
- Weng, D., Yin, Y., & Yang, D. (2011). Singular points detection based on multi resolution in fingerprint images. *Pattern Recognition*, 74(17).
- Willis, A. J., & Myers, L. (2001). A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips. *Pattern Recognition*, 34(2), 255–270.
- Wright, D., & Kreissl, R. (2014). *Surveillance in Europe*. Taylor & Francis. Retrieved from <https://books.google.dz/books?id=9amQBAAAQBAJ>
- Wu, C., Shi, Z., & Govindaraju, V. (2004). Fingerprint image enhancement method using directional median filter. In *Defense and Security* (pp. 66–75).
- Yang, G., Zhou, G.-T., Yin, Y., & Yang, X. (2010). K-means based fingerprint segmentation with sensor interoperability. *EURASIP Journal on Advances in Signal Processing*, 2010, 54.
- Yin, J., Zhu, E., Yang, X., Zhang, G., & Hu, C. (2007). Two steps for fingerprint segmentation. *Image and Vision Computing*, 25(9), 1391–1403. <http://doi.org/http://dx.doi.org/10.1016/j.imavis.2006.10.003>

- Zacharias, G. C., & Lal, P. S. (2013). Singularity detection in fingerprint image using orientation consistency. In *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on* (pp. 150–154).
- Zhao, F., & Tang, X. (2007). Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition*, 40(4), 1270–1281.
- Zhao, Q., Zhang, Y., Jain, A. K., Paulter, N. G., & Taylor, M. (2013). A generative model for fingerprint minutiae. In *Biometrics (ICB), 2013 International Conference on* (pp. 1–8).
- Zhou, J., & Gu, J. (2004). A model-based method for the computation of fingerprints' orientation field. *Image Processing, IEEE Transactions on*, 13(6), 821–835.
- Zhu, Y., Dass, S. C., & Jain, A. K. (2007). Statistical models for assessing the individuality of fingerprints. *Information Forensics and Security, IEEE Transactions on*, 2(3), 391–401.

•

