THE TECHNIQUES FOR FINGERPRINT MATCHING

SOUKSAMAY INSANKEOVILAY

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRONICS ENGINEERING

INTERNATIONAL COLLEGE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2013

KMITL-2013-IC-M-006-001

Thesis Title	The Technique for Fingerprint Matching
Student	Mr. Souksamay Insankeovilay
Student I.D	54601101
Degree	Master of Engineering
Program	Electronics Engineering
Year	2013
Thesis Advisor	Assoc. Prof. Dr. Somsak Choomchuay

ABSTRACT

Development in the personal identification by means of biometrics has drawn more attention due to the needs in reliable and easy to use security system with affordable cost. Among the many possible biometric schemes, the fingerprint is one of the most reliable mean for the identification of individual since each person holds distinctive pattern. Not only for personal identification, fingerprints are also widely used in many verification processes. Therefore, the ultimate goal can be assumed to be "fingerprint matching". In this thesis, we propose several techniques for fingerprint matching namely i) Fingerprint matching by using the normalized cross correlation and the minutiae score in this technique to speed up the matching process, the template and the test images are cropped to the size of 128×128 pixels and the core point is assumed to be the center of this square. ii) Fingerprint matching by using 2D-DFT features as well as 2D-DCT features. In this technique we crop input images from the size 480×640 pixels into 128×128 pixels, and then divided the image into 64 sub-images. Each sub-images (a tile) head the size of 16×16 pixels. Each tile is transformed, and its spectrum feature is compared between those of a test tile and a template tile. And finally we proposed fingerprint matching by using NCC and 2D-DFT in combination. In this technique the performance is measured by two steps, the NCC score and the spectrum score

A commonly known FVC-2004 (DB1-A, DB2-A, DB3-A) database has been used in our investigation. We can see that the combined method offers better performances (FAR, FAR, and computation times) when compared to other individual matching reported in the literature, our method is dos sensitive to rotational effect. However, the proposed technique is still based on the

availability of the core point. Therefore, the performance can be deterred if the core point cannot be located or improperly located.

ACKNOWLEDGMENTS

This thesis could not have been written without the support from supervisors. Also I would like to gratitude ASEAN University Network/Southeast Asia Engineering Education Development Network (AUN/SEED-Net) for awarding me the scholarship with the financial support for my study at King Mongkut's Institute of Technology Ludkrabang (KMITL), Thailand.

Firstly, I would like to express my great gratitude towards my supervisor, Assoc. Prof. Dr. Somsak Choomchuay who has given me much suggestion, support, and advice from the very early stage of this research as well as giving me extraordinary experiences throughout the work.

I would also like to gratitude and sincere goes also to all Professors, lectures and supporting staffs in the department of electronics engineering, who always continuously encouraged, helped and gave me a guideline during the whole period of my study at KMITL.

I would like to recognize all friends in Thailand who always encouraged and helped me during the period of my study. Throughout my years at KMITL, they have enriched my life with their companions and friendship.

Finally, I would also like to my parent for their patience, continuous encouragement, guidance, love, and support.

Table of Contents

English Abstract i

Acknowledgments iii

Table of Contents iii

List of Tables vi

List of Figures vii

List of Abbreviation vi

Chapter 1 Introduction 1

1. Introduction 1

1.1 Fingerprint as a Biometric 2

1.2 History Biometric Recognition 3

1.3 Biometric System 4

1.4 Biometric Characteristics 9

1.5 Biometrics feature 11

1.5.1 Physiological feature 11

1.5.2 Behavioral biometric feature 14

1.6 Application of Fingerprint System 16

1.7 History of Fingerprints 19

1.8 Formation of Fingerprints 22

1.9 Individuality of fingerprints 23

1.10 Fingerprint Sensing and storage 23

1.11 Fingerprint Representation and Feature extraction 26

1.12 Definitions of fingerprint 28

1.13 Approach 29

1.14 Thesis outline 30

Chapter 2 Background and literature review 31

2. Image processing 31

2.1 Fingerprint Enhancement 32
2.1.1 Fingerprint Enhancement process 34
2.1.2 Normalization 34
2.1.3 Segmentation 36
2.1.4 Orientation field estimation 37
2.1.5 Ridge frequency estimation 41
2.1.6 Minutiae Extraction 43
2.1.7 Minutiae detection 43
2.1.8 Binarization based methods 45
2.2 Fingerprint Enhancement using Gabor filter 46
2.3 Core piont finding 50
2.3.1 Point care index technique 50
2.4 Two dimensional discrete Fourier transforms and discrete cosine transform 52
2.4.1 Block divides 53
2.4.2 Discrete Fourier transforms 53
2.4.3 Discrete cosine transforms 54
2.4.4 Definitions 54
2.4.5 One-dimensional DCT 55
2.4.6 Two dimensional DCT 56
2.5 literature review of fingerprint Matching 58
2.5.1 Correlation-based techniques 59
2.5.2 Minutiae-based methods 62
2.5.3 Minutiae matching with pre-alignment 66
2.5.4 Local matching 67
Chapter 3 Proposed algorithms of fingerprint matching 69
3.1 Database construction 70
3.2 Fingerprint matching process 72
3.2.1 Fingerprint enhancement using Gabor filter 72
3.2.2 Core point finding 72

3.2.3 Angle finding 73
3.2.4 Template rotation 74
3.3 Proposedfingerprint matching techniques 75
3.3.1 Fingerprint matching by using the normalized cross correlation technique 75
3.3.1.1 Matching Procedure 78
3.3.2 Fingerprint matching base on Minutiae technique 80
3.3.3 Fingerprint matching base on two dimensional discrete Fourier transform 81
3.3.4 Fingerprint matching base on two dimensional discrete cosine transform 86
3.3.5 Fingerprint matching by using NCC and 2D-DFT 90
3.4 The pros and cons matching techniques 91
Chapter 4 Experiment and results 92
4.1 Preprocessing and Post process 92
4.2 Database 92
4.2.1 FVC2004DB1-A Database 93
4.2.2 FVC2004DB2-A Database 93
4.2.3 FVC2004DB3-A Database 94
4.3 Performance of evaluation 94
4.3.1 Experiment 1 95
4.3.2 Experiment 2 98
4.3.2.1 FVC2004DB1-A matching result 100
4.3.2.2 FVC2004DB2-A matching result 101
4.3.2.3 FVC2004DB3-A matching result 102
4.3.3 Experiment 3 104
4.3.4Experiment 4 106
4.3.4.1 NCC matching result 107
4.3.4.2 2D-DFT matching result 108
4.3.4.3 Combination matching result 108
4.3.5 Summary 111
Chapter 5 Discussion, Conclusion & Future Prospects… 112

5.1 Discussion 112
5.2 Conclusion..... 112
5.3 Future Prospects 113
Reference 113
Appendix A 118
Biography 119
List of International Conference and Proceeding Papers 120

List of Tables

Table Page
1.5.1 Comparison of commonly used biometric characteristics 16
2.1.7 Crossing Number computes in the eight neighboring pixels of minutiae detection 38
2.1.8 Properties of the Crossing Number 46
3.4 The pros and cons of domain matching 91
4.3 Constrain angles used in the minutiae matching 96
4.3.1Matching results versus fingerprint pattern 97
4.3.2.1 FVC 2004-DB1-A Matching Results 101
4.3.2.2 FVC 2004-DB2-A Matching Results 101
4.3.2.3 FVC 2004-DB3-A Matching Results 102
4.3.2.4 Compare the performance results from differences database 102
4.3.3 The 2D-DCT Results from FVC 2004-DB1-A 105
4.3.4.1 NCC matching Results from FVC 2004-DB1-A 108
4.3.4.2 The 2D-DFT Matching Results from FVC 2004-DB1-A 108
4.3.4.3 Combination NCC and 2D-DFT Matching results 109
4.3.4.4 Matching of different works 110

List of Figures

Figure Page

1.3.1 Enrollment, verification, and identification processes, these processes use the following modules 5

1.5.1 Physiological biometrics feature 11

1.5.2 Behavioral biometric feature 14

1.6.1 Various electronic access applications in widespread use that require automatic authentication 19

1.7.1 Examples of archaeological fingerprint carvings and historic fingerprint impressions 20

1.7.2 Example of the first scientific proposed ridge, valley and pore structure in fingerprint 21

1.7.3 Example of first using fingerprint and first classification scheme 21

1.10.1 Fingerprint images of acquisition 24

1.10.2 Fingerprint sensors can be embedded in a variety of devices for User recognition 25

1.11.1 Fingerprint global features of Level 1 27

1.11.2. Minutiae (black-filled circles) in a portion of fingerprint image; sweat pores (empty circles) on a single ridge line 28

1.12.1 Real fingerprint local features Level 2 (black line) 29

2.1.1 Example of histogram of the normalization 36

2.1.2 Example of fingerprint image segmentation 37

2.3.3. A fingerprint image faded into the corresponding orientation image computed over a square-meshed grid of size 16×16 38

2.1.4 Orientation field estimation is computed with the equation (2.3.6). 40

2.1.5 Example of orientation field smoothing 41

2.1.6 The projection of the intensity values of the pixels along a direction orthogonal to the local ridge orientation 42

2.1.7 The estimated ridge wavelength (ridge frequency) for fingerprint images of wavelength 43

2.1.8 Examples of a ridge ending and bifurcation pixel 44

2.1.9 Minutiae detection, circles red and green corresponding to ridges ending and ridge bifurcation 44
2.1.10 Results of applying binarization and thinning directly to the original image with enhanced45
2.1.11 Five most common minutiae types (black line) 46
2.2.1 Graphical appearance of the Gabor filter 47
2.2.2 Appearance of Gabor filters different of oriented filters 48
2.2.3 A graphical representation of a bank of 24 49
2.2.4 Examples of fingerprint enhancement have applied Gabor filter (GBF) 50
2.3.1 The Poincare index computed over a curve C immersed in a vector field G 51
2.3.2 Examples of Poincaré index computation in the 8-neighborhood of points belonging (from left to right) to a whorl, loop, and delta singularity, respectively 52
2.3.3 Examples of Poincare index technique detection (star) on the fingerprint image 52
2.4.1 Fingerprint Image divided into 64 blocks each block 16 ×16 pixel 53
2.4.2 The similar spectrum when sub_image opposite way 55
2.4.3 a) Original 64 sub-images, b) 2D-DFT 64 sub-images result c) Original one sub-images, b) 2D-DFT one sub-images result 55
2.5.1 Each row shows two impressions of the same finger and the absolute value of their difference (residual) 60
2.5.2 The minutiae of I mapped into T coordinates for a given alignment 64
2.5.3 In this example of mated minutia 65
2.5.4 The results of applying the matching algorithm to an input minutiae set and a template 67
2.5.5 An example of two false matched local structures 68
3.1 Database Construction System 70
3.2 Fingerprint matching construction systems 71
3.2.1 Examples of Poincare index technique detection (star) on the fingerprint image. 73
3.2.2 (a) Original image , (b) Define the circle of interest of which the radius of100 pixel. The core point is taken as a center, (c) The angle measurement 74
3.2.3 The template rotation 74

3.3.1 Matching of template *t* into the source image *f* 76
3.3.2 Example NCC matcher The Template a) and test image b) are the same figure 79
3.3.3 Example NCC matcher the Template a) and test image b) are differences figure 79
3.3.4 Minutiae, Reference and orientation point 80
3.3.5 Shown minutiae point a) The Template and the test image are the same figure. b) The Template and the test image are deference image 81
3.3.6 The similar spectrum when sub_image opposite way 82
3.3.7 (a) Fingerprint image cropped to size 128×128 pixels and divided into 64-sub image and each sub-image with size 16×16 pixels. (b) 64 sub-image is 2D Discrete Fourier transforms. (d) One sub-image with size 16×16 pixels. (c) Spectrum of one sub-image transform 83
3.3.8 (a) And (b) Image angle or image position ($\theta = 63.76^{o}$), (c) Angle of the template rotated85
3.3.9 (a) Fingerprint image cropped to size 128x128 pixels and divided into 64-sub image and each sub-image with size 16×16 pixels. (b) 64 sub-image is 2D Discrete Fourier transforms. (d) One sub-image with size 16×16 pixels. (c) Spectrum of one sub-image transform 87
4.2.1 Sample images from, FVC2004DB1-A Database with the size 480×640 pixels 93
4.2.2 Sample images from, FVC2004DB2-A Database with the size 480×640 pixels 93
4.2.3 Sample images from, FVC2004DB3-A Database with the size 480×640 pixels 94
4.3.1 The Flowchart of the proposed matching algorithm 95
4.3.2 Matching scores versus FAR and FRR 96
4.3.3 a) Percentage of FAR and FRR, b) Average computation Time machine 98
4.3.4 2D-DFT matching algorithm flowchart 99
4.3.5 Constrain score used in the 2D-DFT and the 2D-DCT matching 100
4.3.6 a) Percent of FAR and FRR, b) Average computation Time machine 103
4.3.7 Example Average values of the correlation score of different images 104
4.3.8 a) Percent of FAR and FRR, b) Average computation Time machine 105
4.3.9 Example Average values of the correlation score of different images 106
4.3.10 NCC and 2D-DFT matching algorithm flowchart 107
4.3.11 a) Percentage of FAR and FRR, b) Average computation Time machine 109

List of Abbreviations

Abbreviation	Meaning
1D-DCT	One Dimensional Discrete Cosine Transform
2D-DCT	Two Dimensional Discrete Cosine Transform
ADALINE	Adaptive Linear Element
AI	Artificial Intelligence
ANN	Artificial Neural Network
ART	Adaptive Resonance Theory
CGM	Constrained Generative Model
DCT	Discrete Cosine Transform
DFFS	Distance from Face Space
DNA	Deoxyribonucleic Acid
H	high
M	Medium
L	Low
CJIS	Criminal Justice Information Services
PIV	Personal Identity Verification
WSQ	Wavelet Scalar Quantization
FAR	False Acceptance Rate
FRR	False Rejection Rate
DFT	Discrete Fourier Transform
DST	Discrete Sine Transform
DWT	Discrete Wavelet Transform
FDCT	Forward Discrete Cosine Transform
GA	Genetic Algorithm
GUI	Graphical User Interface
GUIDE	Graphical User Interface Design Environment

HVS	Human Visual System
IEC	International Electro-Technical Commission
ISO	International Standards Organization
JPEG	Joint Photographic Experts Group
FTIR	Frustrated Total Internal Reflection
CN	Crossing Number
PC	Poincare index
DC	Direction of curvature
MAG	Minutia adjacency graph
AAD	Average absolute deviation
LBP	Local binary patterns
NCC	Normalized cross correlation
KDD	Knowledge Discovery in Databases
FVC	Fingerprint Verification Competition
PDAs	Personal Digital Assistants
FBI	Federal of Investigation
AFIS	Automated Fingerprint Identification System
FTIR	Frustrated Total Internal Reflection
RBF	Radial Basis Function
DPI	Dot Per Inch

Chapter 1

Introduction

1. Introduction

Rather than a century has passed since Alphonse Bertillon first conceived and then industriously practiced the idea of using body measurements for solving crimes. Just as his idea was gaining popularity, it faded into relative obscurity by a far more significant and practical discovery of the distinctiveness of the human fingerprints. In 1893, the Home Ministry Office, UK, accepted that no two individuals have the same fingerprints. Soon after this discovery, many major law enforcement departments saw the potential of fingerprints in identifying repeat offenders who used an alias, e.g., changed their names with each arrest to evade the harshest penalties reserved for recidivists in law. The law enforcement departments embraced the idea of "booking" the fingerprints of criminals at the time of arrest, so that their records are readily available for later identification. Fingerprints found an application in forensics. By matching leftover fingerprint smudges (latent) from crime scenes to fingerprints collected during the booking, authorities could determine the identity of criminals who have been previously arrested. The law enforcement agencies sponsored a rigorous study of fingerprints, developed scientific methods for visual identification/matching of fingerprints and instituted strong programs/ cultures for training fingerprint experts. They successfully applied the art of fingerprint recognition for nailing down the perpetrators.

Fingerprint recognition has been used for a long time to determine person identify in law enforcement, and it has become a more and more important task with increasing demand for person identification in various applications such as online banking, e-commerce, and security control, because fingerprints have significant characteristics such as exchangeability and uniqueness. A fingerprint consists of ridges separated by valleys, these ridges flow almost parallel to each other, and ridges change their flow at minutiae such as endings and bifurcations of ridges. The relation graph between fingerprint minutiae is unique for each finger and does not change during life. Although various algorithms and systems have been proposed as a means of determining the identity of fingerprints, most fingerprint identification systems adopt a matching.

Based on comparison of fingerprint minutiae. However, automatic detection of minutiae tends to be influenced by various noises as caused by dry skin and imprint condition. In order to suppress the influence of noise and enhance signal components of the print, fingerprint enhancement is performed based on fingerprint image properties. Ridge flow is characterized by local ridge direction and local ridge width. The directional features represent an outline of ridge flow. The ridge width between fingerprint ridges is different according to its location, imprint condition, and finger size. As a consequence, these differences result in a variety of ridge frequencies in the fingerprint. Therefore, these features are important to direction filters and to process fingerprint enhancement according to the local ridge features of the print [2].

1.1 Fingerprint as a Biometric

A fingerprint is an impression of the friction ridges, from the surface of a finger-tip. Fingerprints have been used for personal identification for many decades, more recently becoming automated due to advancements in computing capabilities. Fingerprint recognition is nowadays one of the most important and popular biometric technologies mainly because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and the established use and collections by law enforcement agencies. Automatic fingerprint identification is one of the most reliable biometric technologies. This is because of the well known fingerprint distinctiveness, persistence, ease of acquisition and high matching accuracy rates. Fingerprints are unique to each individual and they do not change over time. Even identical twins (who share their DNA) do not carry identical fingerprints. The uniqueness can be attributed to the fact that the ridge patterns and the details in small areas of friction ridges are never repeated. These friction ridges develop in the fetus in their definitive form before birth and are known to be persistent throughout life except for permanent scarring. Scientific research in areas such as biology, embryology, anatomy and histology has supported these findings [3]. Also, the matching accuracy of fingerprint based authentication systems has been shown to be very high. Fingerprint-based authentication systems continue to dominate the biometrics market by accounting for almost 52% of authentication systems based on biometric traits [4].

1.2 History Biometric Recognition

As our society has become electronically connected and more mobile, surrogate representations of identity such as passwords (prevalent in electronic access control) and cards (prevalent in banking and government applications) cannot be trusted to establish a person's identity. Cards can be lost or stolen and passwords or PIN can, in most cases, be guessed. Further, passwords and cards can be easily shared and so they do not provide non-repudiation [1].

Biometric recognition (or simply biometrics) refers to the use of distinctive anatomical (or physiological) (i.e., fingerprints, face, iris) and behavioral (i.e., speech) characteristics, called biometric identifiers or traits or characteristics for automatically recognizing individuals. Biometrics are becoming an essential component of effective person identification solutions because biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity. Recognition of a person by their body, then linking that body to an externally established "identity", forms a very powerful tool of identity management with tremendous potential consequences, both positive and negative. Consequently, biometrics is not only a fascinating pattern recognition research problem but, if carefully used, is an enabling technology with the potential to make our society safer, reduce fraud and provide user convenience (user friendly man–machine interface).

The word biometrics are derived from the Greek words bios (meaning life) and Metron (meaning measurement); biometric identifiers are measurements of the living human body. Perhaps all biometric identifiers are a combination of anatomical and behavioral characteristics and they should not be exclusively classified into either anatomical or behavioral characteristics. For example, fingerprints are anatomical in nature but the usage of the input device (e.g., how a user presents a finger to the fingerprint scanner) depends on the person's behavior. Thus, the input to the recognition engine is a combination of anatomical and behavioral characteristics. Similarly, speech is partly determined by the vocal tract that produces speech and partly by the way a person speaks. Often, a similarity can be noticed among parents, children, and siblings in their speech. The same argument applies to the face: faces of identical twins may be extremely similar at birth but during their growth

and development, the faces change based on the person's behavior (e.g., lifestyle differences leading to a difference in body weight, etc.).

A number of questions related to a person's identity are asked every day in a variety of contexts. Is this person authorized to enter the facility? Is this individual entitled to access privileged information? Is this person wanted for a crime? Has this person already received certain benefits? Is the given service being administered exclusively for the enrolled users? Reliable answers to questions such as these are needed by business and government organizations. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than the traditional token (ID cards) or knowledge-based (passwords or PIN) methods. The objectives of biometric recognition are user convenience (e.g., money withdrawal at an ATM machine without a card or PIN), better security (e.g., only authorized person can enter a facility), better accountability (e.g., difficult to deny having accessed confidential records), and higher efficiency (e.g, lower overhead than computer password maintenance). The tremendous success of fingerprint-based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all resulted in increasing use of fingerprint-based person recognition in commercial, government, civilian, and financial domains. In addition to fingerprints, some other traits, primarily hand shape, voice, iris and face have also been successfully deployed.

1.3 Biometric Systems

An important issue in designing a practical biometric system is to determine how an individual is going to be recognized. Depending on the application context, a biometric system may be called either a verification system or an identification system [1].

- A verification system authenticates a person's identity by comparing the captured biometric characteristic with her previously captured (enrolled) biometric reference template pre-stored in the system. It conducts one-to-one comparison to confirm whether the claim of identity of the individual is true. A verification system either rejects or accepts the submitted claim of identity.

- An identification system recognizes an individual by searching the entire enrollment template database for a match. It conducts one-to-many comparisons to establish if the individual is present in the database and if so, returns the identifier of the enrollment reference that matched. In an identification system, the system establishes a subject's identity (or determines that the subject is not enrolled in the system database) without the subject having to claim an identity.

The term authentication is also used in the biometric field, sometimes as a synonym for verification; actually, in the information technology language, authenticating a user means to let the system know the identity of the user regardless of the mode (verification or identification). Throughout this book we use the generic term recognition where we are not interested in distinguishing between verification and identification.

The block diagrams of verification and identification systems are depicted in Figure 1.3.1 user enrollment, which is common to both tasks is also graphically illustrated.

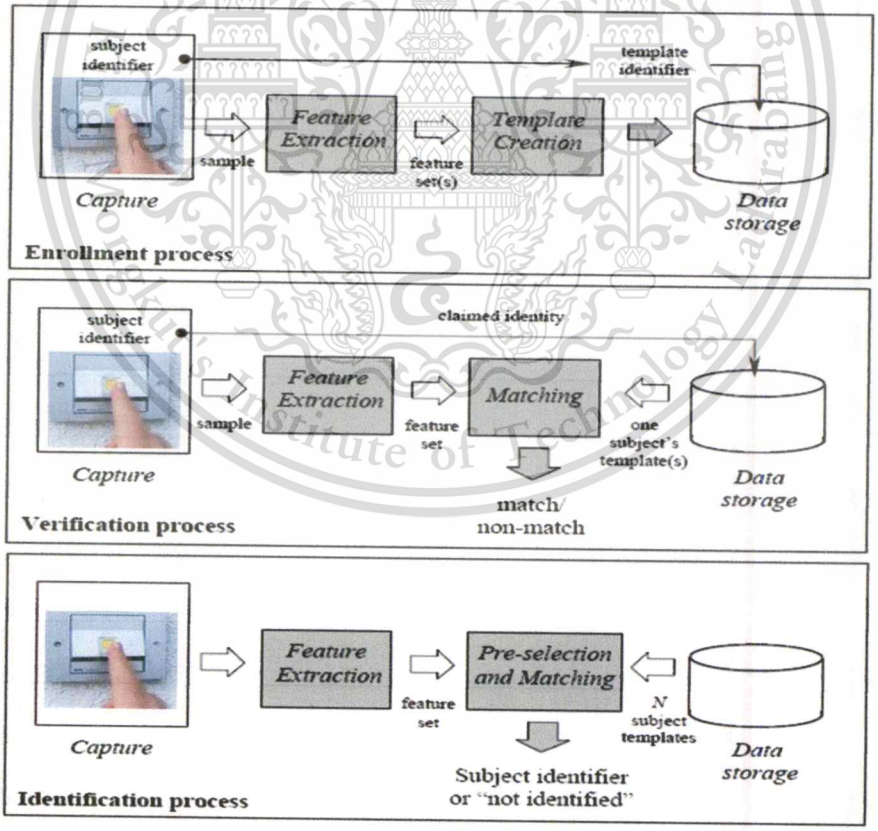


Figure 1.3.1 Enrollment, verification, and identification processes, these processes use the following modules[1].

Capture, feature extraction, template creation, matching, pre-selection, and data storage. In the identification process pre-selection and matching are often combined [1]. The enrollment, verification, and identification processes involved in user recognition make use of the following system modules:

- Capture: a digital representation of biometric characteristic needs to be sensed and captured. A biometric sensor, such as a fingerprint scanner, is one of the central pieces of a biometric capture module. The captured digital representation of the biometric characteristic is often known as a sample; for example, in the case of a fingerprint system, the raw digital fingerprint image captured by the fingerprint scanner is the sample. The data capture module may also contain other components (e.g., a keyboard and screen) to capture other (non-biometric) data.
- Feature extraction: in order to facilitate matching or comparison, the raw digital representation (sample) is usually further processed by a feature extractor to generate a compact but expressive representation, called a feature set.
- Template creation: the template creation module organizes one or more feature sets into an enrollment template that will be saved in some persistent storage. The enrollment template is sometimes also referred to as a reference.
- Pre-selection and matching: the pre-selection (or filtering) stage is primarily used in an identification system when the number of enrolled templates is large. Its role is to reduce the effective size of the template database so that the input needs to be matched to a relatively small number of templates. The matching (or comparison) stage (also known as a matcher) takes a feature set and an enrollment template as inputs and computes the similarity between them in terms of a matching score, also known as similarity score. The matching score is compared to a system threshold to make the final decision; if the match score is higher than the threshold, the person is recognized, otherwise not.
- Data storage: is devoted to storing templates and other demographic information about the user. Depending on the application, the template may be stored in internal or external storage devices or be recorded on a smart card issued to the individual.

Using these five modules, three main processes can be performed, namely, enrollment, verification, and identification. A verification system uses the enrollment and verification

processes while an identification system uses the enrollment and identification processes. The three processes are:

- Enrollment: user enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the biometric characteristic of a subject is first captured by a biometric scanner to produce a sample. A quality check is often performed to ensure that the acquired sample can be reliably processed by successive stages. A feature extraction module is then used to produce a feature set. The template creation module uses the feature set to produce an enrollment template. Some systems collect multiple samples of a user and then either select the best image (or feature set) or fuse multiple images (or feature sets) to create a composite template. The enrollment process then takes the enrollment template and stores it in the system storage together with the demographic information about the user (such as an identifier, name, gender, height, etc.).
- Verification: the verification process is responsible for confirming the claim of identity of the subject. During the recognition phase, an identifier of the subject (such as username or PIN [Personal Identification Number]) is provided (e.g., through a keyboard or a keypad or a proximity card) to claim an identity; the biometric scanner captures the characteristic of the subject and converts it to a sample, which further processes by the feature extraction module to produce a feature set. The resulting feature set is fed to the matcher, where it is compared against the enrollment template(s) of that subject (retrieved from the system storage based on the subject's identifier). The verification process produces a match/non-match decision
- Identification: in the identification process, the subject does not explicitly claim an identity and the system compares the feature set (extracted from the captured biometric sample) against the templates of all (or a subset of) the subjects in the system storage; the output is a candidate list that may be empty (if no match is found) or contain one (or more) identifier(s) of matching enrollment templates. Because identification in large databases is computationally expensive, a pre-selection stage is often used to filter the number of enrollment templates that have to be matched against the input feature set.

Depending on the application domain, a biometric system could operate either as an online system or an off-line system. An on-line system requires the recognition to be performed quickly

and an immediate response is imposed (e.g., a computer network logon application). On the other hand, an off-line system does not require the recognition to be performed immediately and a relatively long response delay is allowed (e.g., background check of an applicant). On-line systems are often fully automatic and require that the biometric characteristic be captured using a live-scan scanner, the enrollment process be unattended, there be no (manual) quality control, and the matching and decision making are fully automatic. Off-line systems, however, are often semi-automatic, where the biometric acquisition could be through an offline scanner (e.g., scanning a fingerprint image from a latent or inked fingerprint card), the enrollment may be supervised (e.g., when a suspect is "booked," a police officer guides the fingerprint acquisition process), a manual quality check may be performed to ensure good quality acquisition, and the matcher may return a list of candidates which are then manually examined by a forensic expert to arrive at a final decision.

The verification and identification processes differ in whether an identity is claimed or not by the subject. A biometric claim (or claim of identity) is defined as the implicit or explicit claim that a subject is or is not the source of a specified or unspecified biometric enrollment template. A claim may be [1]:

- Positive: the subject is enrolled.
- Negative: the subject is not enrolled.
- Specific: the subject is or is not enrolled as a specified biometric enroll.
- Non-specific: the subject is or is not among a set or subset of biometric enroll.

The application context defines the type of claim. In certain applications, it is in the interest of the subject to make a positive claim of identity. Such applications are typically trying to prevent multiple people from using the same identity. For example, if only Alice is authorized to enter a certain secure area, then it is in the interest of any subject to make a positive claim of identity (of being Alice) to gain access. But the system should grant access only to Alice. If the system fails to match the enrolled template of Alice with the input feature set, access is denied, otherwise, access is granted. In other applications, it is in the interest of the subject to make a negative claim of identity. Such applications are typically trying to prevent a single person from using multiple identities. For example, if Alice has already received certain welfare benefits, it is in her interest to now make a negative claim of identity

(that she is not among the people who have already received benefits), so that she can double-dip. The system should establish that Alice's negative claim of identity is false by finding a match between the input feature set of Alice and enrollment templates of all people who have already received the benefits. The following three types of claims are used depending on the application context:

- Specific positive claim: applications such as logical access control (e.g., network logon) may require a specific positive claim of identity (e.g., through a username or PIN). A verification biometric system is sufficient in this case to confirm whether the specific claim is true or not through a one-to-one comparison.
- Non-specific positive claim: applications such as physical access control may assume a non-specific positive claim that the subject is someone who is authorized to access the facility. One of the advantages of this scenario is that the subject does not need to make a specific claim of identity (no need to provide a username, PIN, or any other token), which is quite convenient. However, the disadvantage of this scenario is that an identification biometric system is necessary (which has a longer response time and lower accuracy due to one-to-many comparisons).
- Non-specific negative claim: applications such as border crossing typically assume a non-specific negative claim, i.e., the subject is not present in a "watch list". Again, an identification system must be used in this scenario. Note that such applications cannot use traditional knowledge-based or possession-based methods of recognition. Surrogates tokens such as passports have been traditionally used in such applications but if passports are forged (or if people obtain duplicate passports under different names), traditional recognition methods cannot solve the problem of duplicate identities or multiple enrollments.

1.4 Biometric Characteristics

Identity verification in computer systems is done based on measures like keys, cards, passwords, PIN and so forth. Unfortunately, these may often be forgotten, disclosed or changed. A reliable and accurate identification/verification technique may be designed using biometric technologies, which are further based on the special characteristics of the person such as face, iris,

fingerprint, signature and so forth. This technique of identification is preferred over traditional passwords and PIN-based techniques for various reasons [1, 5].

- The person to be identified is required to be physically present at the time of identification.
- Identification based on biometric techniques obviates the need to remember a password or carry a token.

There are many biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires the following properties of biometric characteristics:

- Universal: Everyone must have the attribute. The attribute must be one that is seldom lost to accident or disease.
- Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age or either episodic or chronic disease.
- Measurability: The properties should be suitable for capture without waiting time and it must be easy to gather the attribute data passively.
- Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are unique attributes, assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
- Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies; that is, technologies requiring a part of the human body to be taken or (apparently) impairing the human body.
- Reducibility: The captured data should be capable of being reduced to an easy-to-handle file.
- Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- Privacy: The process should not violate the privacy of the person.

- Comparable: The attribute should be able to be reduced to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
- Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

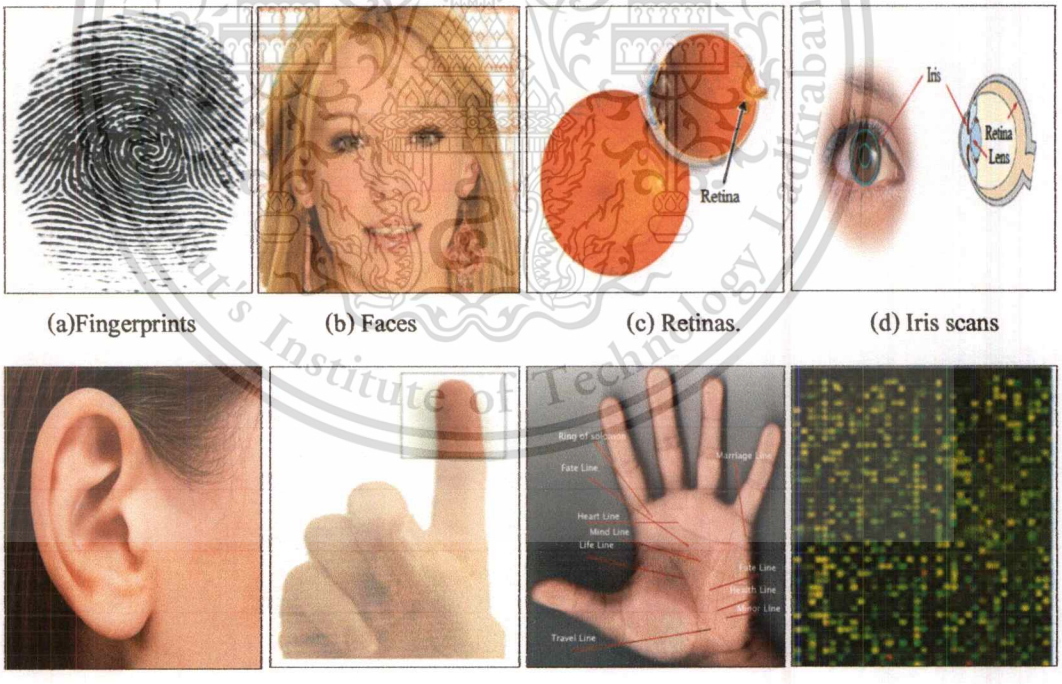
Among the various biometric technologies being considered are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature and so forth [1,5].

1.5 Biometrics feature

In typically Biometrics characteristics is basically divided into two features: i e, Physiological and Behavioral.

1.5.1 Physiological feature

The Biometrics physiological feature is shown in Figure 1.5.1 below.



(a)Fingerprints (b) Faces (c) Retinas. (d) Iris scans

(e) Ears. (f) Fingers. (g) Palm print. (h) DNA

Figure 1.5.1 Physiological biometrics feature [1]

a). Fingerprint: fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device requires each user to place a finger on a plate for the print to be read. Fingerprint biometrics currently have three main application areas: large-scale Automated Finger Imaging Systems (AFIS), generally used for law enforcement purposes; fraud prevention in entitlement programs; and physical and computer access. A major advantage of finger imaging is the long time use of fingerprints and its wide acceptance by the public and law enforcement communities as a reliable means of human recognition. Others include the need for physical contact with the optical scanner, possibility of poor-quality images due to residue on the finger such as dirt and body oils (which can build up on the glass plate), as well as eroded fingerprints from scrapes, years of heavy labor or mutilation.

b). Facial recognition: face recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of the distinguishing features of the face. Facial recognition technologies can encounter performance problems stemming from such factors as non-cooperative behavior of the user, lighting and other environmental variables. The main disadvantages of face recognition are similar to problems of photographs. People who look alike can fool the scanners. There are many ways in which people can significantly alter their appearance, like a slight change in facial hair and style.

c). Retinal scan: retinal scanning involves an electronic scan of the retina the innermost layer of the wall of the eyeball. By emitting a beam of incandescent light that bounces off the person's retina and returns to the scanner, a retinal scanning system quickly maps the eye's blood vessel pattern and records it into an easily retrievable digitized database. The eye's natural reflective and absorption properties are used to map a specific portion of the retinal vascular structure. The advantages of retinal scanning are its reliance on the unique characteristics of each person's retina, as well as the fact that the retina generally remains fairly stable throughout life. Disadvantages of retinal scanning include the need for fairly close physical contact with the scanning device. Also, trauma to the eye and certain diseases can change the retinal vascular structure, and there also are concerns about public acceptance.

d) Iris scans: iris scanning measures the iris pattern in the colored part of the eye, although the iris color has nothing to do with the biometric. Iris patterns are formed randomly. As a result, the iris patterns in the left and right eyes are different, and so are the iris patterns of identical twins. Iris templates are typically around 256 bytes. Iris scanning can be used quickly for both identification and verification applications because of its large number of degrees of freedom. Disadvantages of iris recognition include problems of user acceptance, relative expense of the system as compared to other biometric technologies and the relatively memory-intensive storage requirements.

e). Ear shape: identifying individuals by ear shape is used in law enforcement applications where ear markings are found at crime scenes. Problems are faced whenever the ear is covered by hair.

f). Hand/Finger geometry: hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes actual prints of palm or fingers. Only the spatial geometry is examined as the user puts a hand on the sensor's surface. Hand geometry templates are typically 9 bytes, and finger geometry templates are 20 to 25 bytes. Finger geometry usually measures two or three fingers, and thus requires a small amount of computational and storage resources. The problems with this approach are that it has low discriminating power, the size of the required hardware restricts its use in some applications and hand geometry-based systems can be easily circumvented.

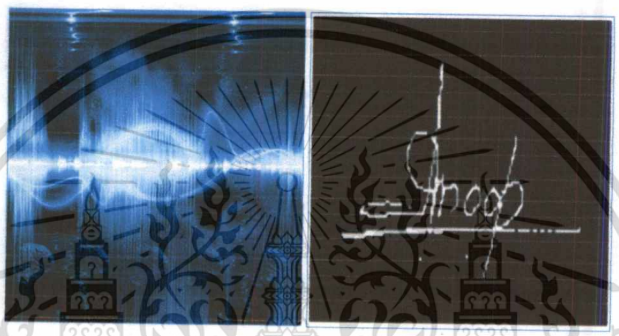
g). Palm print: palm print verification is a slightly modified form of fingerprint technology. Palm print scanning uses an optical reader very similar to that used for fingerprint scanning; however, its size is much bigger, which is a limiting factor for use in workstations or mobile devices.

Keystroke dynamics: keystroke dynamics are an automated method of examining an individual's keystroke on a keyboard. This technology examines dynamics such as speed and pressure, the total time of typing a particular password and the time that a user takes between hitting keys-dwell time (the length of time one holds down each key) as well as flight time (the time it takes to move between keys). Taken over the course of several login sessions, these two metrics produce a measurement of rhythm unique to each user. Technology is still being developed to improve robustness and distinctiveness.

h). DNA (Deoxyribonucleic Acid): DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far, DNA analysis has not been sufficiently automatic to rank it as a biometric technology. The analysis of human DNA is now possible within 10 minutes. If the DNA can be matched automatically in real time, it may become more significant. At present, DNA is very entrenched in crime detection and will remain in the law enforcement area for the time being.

1.5.2 Behavioral biometric feature

The Biometrics behavioral feature is shown in Figure 1.5.2 below.



(a) Voice. **(b) Signatures.**

Figure 1.5.2 Behavioral biometric features

1.5.2a). Voice recognition: voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. It involves taking the acoustic signal of a person's voice and converting it to a unique digital code that can be stored in a template. Voice recognition systems are extremely well-suited for verifying user access over a telephone. Disadvantages of this biometric are that not only is a fairly large byte code required, but also, people's voices can change (for example, when they are sick or in extreme emotional states). Also, phrases can be misspoken and background noises can interfere with the system.

1.5.2b). Signature verification: it is an automated method of examining an individual's signature. This technology examines dynamics such as speed, direction and pressure of writing; the time that the stylus is in and out of contact with the "paper"; the total time taken to make the signature; and where the stylus is raised from and lowered onto the "paper". Signature verification templates are typically 50 to 300 bytes. The key is to differentiate between the parts of the signature

that are habitual and those that vary with almost every signing. Disadvantages include problems with long-term reliability, lack of accuracy and cost.

Body odor: The body odor biometrics are based on the fact that virtually every human's smell is unique. The smell is captured by sensors that are capable of obtaining the odor from non-intrusive parts of the body, such as the back of the hand. The scientific basis is that the chemical composition of odors can be identified using special sensors. Each human smell is made up of chemicals known as volatiles. They are extracted by the system and converted into a template. The use of body odor sensors broaches on the privacy issue, as the body odor carries a significant amount of sensitive personal information. It is possible to diagnose some disease or activities in last hours by analyzing body odor.

The biometric identifiers described above are compared in Table 1.5.1. Note that the fingerprint has a nice balance among all the desirable properties. Every human being possesses fingers (with the exception of hand-related disability) and hence fingerprints. Fingerprints are very distinctive and they are permanent; even if they temporarily change slightly due to cuts and bruises on the skin, the fingerprint reappears after the finger heals. Live-scan fingerprint scanners can easily capture high-quality fingerprint images and unlike face recognition, they do not suffer from the problem of segmenting the fingerprint from the background. However, they are not suitable for covert applications (e.g., surveillance) as live-scan fingerprint scanners cannot capture a fingerprint image from a distance and without the knowledge of the person. The deployed fingerprint identification (recognition) systems offer good performance and fingerprint scanners have become quite compact and affordable. Because fingerprints have a long history of use in forensic divisions worldwide for criminal investigations, they have some stigma of criminality associated with them. However, this is rapidly changing with the high demand for automatic person recognition to fight identity fraud and security threats. With a layered approach involving fingerprint and other security technologies, fingerprint systems are difficult to circumvent. Fingerprint enhancement based recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. This is also reflected in the revenues generated by various biometric technologies.

Table 1.5.1 Comparison of commonly used biometric characteristic

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	H	M
Hand geometry	M	M	M	H	M	M	M
Hand/Finger vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Entries in the table are based on the perception of the authors. High, Medium, and Low denote by H, M, and L, respectively.

1.6 Applications of Fingerprint Systems

Fingerprint recognition systems have been deployed in a wide variety of application domains, ranging from forensics to mobile phones. But, the system design depends on the application characteristics that define the application requirements. Fingerprint one of most biometrics has been widely used in forensics applications such as criminal identification and prison security. The biometric technology is rapidly evolving and has a very strong potential to be widely adopted in civilian applications such as electronic banking, e-commerce, and access control (see Figure 1.13). Due to a rapid increase in the number and use of electronic transactions, electronic banking and electronic commerce are becoming one of the most important emerging applications of biometrics. These applications include credit card and smart card security, ATM security, check cashing and fund transfers, online transactions and web access. The physical access control applications have traditionally used token-based authentication. With the progress in biometric technology, these applications will increasingly use biometrics for authentication. Remote login and data access applications have traditionally used knowledge-based authentication. These applications have already started using biometrics for person authentication. The use of biometrics will become more

widespread in coming years as the technology matures and becomes more trustworthy. Other biometric applications include welfare disbursement, immigration checkpoints, national ID, voter and driver registration, and time and attendance.

The two most popular ways to categorize fingerprint-based biometric recognition applications are horizontal categorization and vertical categorization. In horizontal categorization, the categories are applications that have some commonalities in the features that they require from the fingerprint recognition system. The vertical categorization is based on the needs of a particular sector of industry or the government. Horizontal categorization results in the following main categories of biometric applications [1].

- Physical access control: access is restricted to facilities such as nuclear plants, bank vaults, corporate boardrooms, and even health-clubs, amusement parks, and lockers.
- Logical access control: access to desktop computers or remote servers and databases is restricted to authorized users. Increasingly, access to software applications is also being restricted to only authorize users.
- Transaction authentication (or consumer identification): transactions may be executed at ATM site or from remote locations for online banking or between banks (i.e., in high-value transactions). Fingerprint recognition systems are used for security of the transaction as well as accountability (so the parties involved in the transaction cannot later deny it).
- Device access control: laptops, PDAs, cell phones, and other electronic devices often contain personal and sensitive data. To protect such data, fingerprint recognition systems are used to conduct recognition on the stand-alone device.
- Time and attendance: time and attendance systems are used to keep track of employee working hours and to compute payrolls. Use of fingerprint recognition systems in these applications is fairly well received to improve efficiency for employees and also for preventing various types of payroll frauds (e.g., buddy-punching).
- Civil identification: in civilian identification application, the most important objective is to prevent multiple enrollments and to find duplicates (e.g., duplicate passport, driver license, national identification card). The size of the database can be of the order of millions (e.g., the entire population of a country). In some applications (such as border control to prevent

suspected terrorists or expelled from entering the country), the identification is not needed to be conducted against the entire population but rather against a "watch-list" database.

- Forensic identification: in forensic identification, latent fingerprints lifted from the crime scenes match against a criminal database to identify the suspect (and sometimes the victims). Vertical categorization results in the following main industries that benefit the most from the use of fingerprint systems:
  - Health care
  - Financial Gaming and hospitality (casinos, hotels, etc.)
  - Retail
  - Education
  - Manufacturing
  - High technology and telecommunications
  - Travel and transport
  - Federal, state, municipal, or other governments
  - Military
  - Law enforcement

Each vertical market may have a need for a number of different horizontal applications. For example, while the most widespread (almost ubiquitous) use of fingerprint identification systems in law enforcement departments is for criminal investigations, these departments also use computers that contain sensitive data. So, this sector needs solutions for fingerprint-based logical access control. Further, law enforcement departments have laboratories and other restricted physical areas, so they can benefit from fingerprint-based physical access control solutions. Fingerprint-based time and attendance solutions can also be used to manage the payroll of law enforcement officers (and other employees of the department).

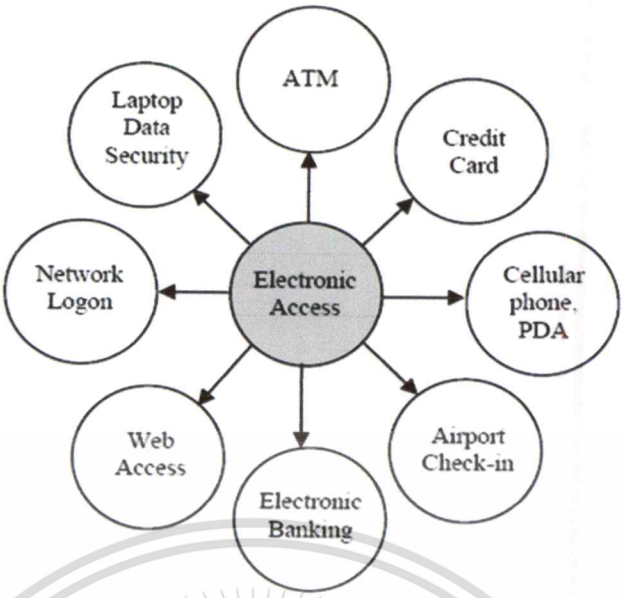
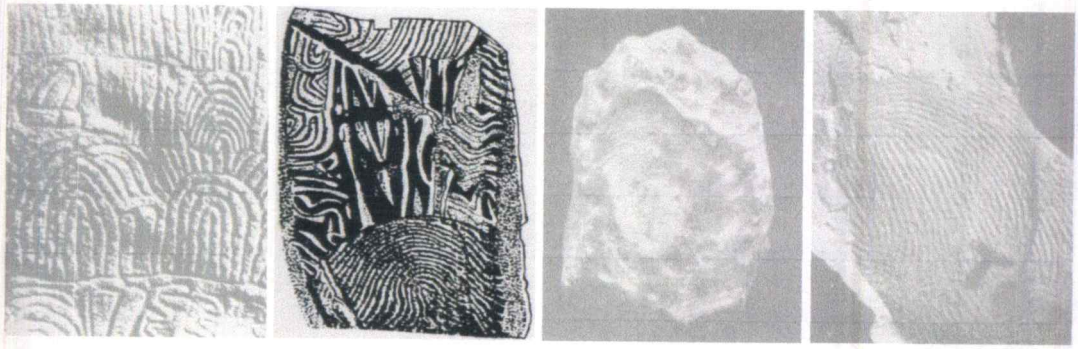


Figure 1.6.1 Various electronic access applications in widespread use that require automatic authentication

1.7 History of Fingerprints

Human fingerprints have been discovered on a large number of archaeological artifacts and historical items (Figure 1.7.1). While these findings provide evidence that ancient people were aware of the individuality of fingerprints, such awareness does not appear to have any scientific basis. It was not until the late sixteenth century that the modern scientific fingerprint technique was first initiated. In 1864, the English plant morphologist, Nehemiah Grew, published the first scientific paper reporting his systematic study on the ridge, valley, and pore structure in fingerprints Figure1.7.1 a).

The first detailed description of the anatomical formation of fingerprints was made by Mayer in 1788 in which a number of fingerprint ridge characteristics were identified and characterized Figure1.7.1 b). Starting in 1809, Thomas Bewick started using fingerprint as his trademark Figure 1.7.1 a), one of the most important milestones in the history of fingerprints. Purkinje, in 1823, proposed the first fingerprint classification scheme, which classified fingerprints into nine categories according to the ridge configurations Figure 1.7.1b)



a), b) c) d)

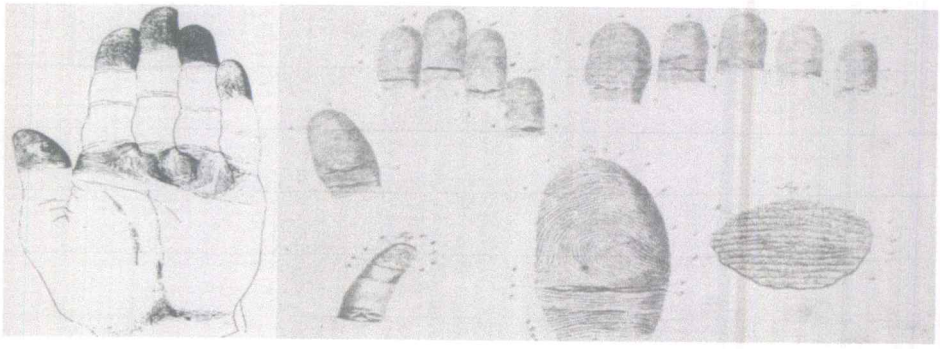
Figure 1.7.1 Examples of archaeological fingerprint carvings and historic fingerprint impressions[1].

a) Neolithic carvings (Gavrinis Island); b) standing stone (Goat Island), c) a Chinese clay seal and d) an impression on a Palestinian lamp. While impressions on the Neolithic carvings and the Goat Island standing stones might not be used to establish identity, there is sufficient evidence to suggest that the Chinese clay seal and impressions on the Palestinian lamp were used to indicate the identity of the fingerprint providers.

Henry fauld, in 1880, first scientifically suggested the individuality of fingerprints based on empirical observations. At the same time, Herschel asserted that he had practiced fingerprint recognition for about 20 years. These findings established the foundation of modern fingerprint recognition. In the late nineteenth century, Sir Francis Galton conducted an extensive study on fingerprints. He introduced the minutiae features for comparing fingerprints in 1888.

An important advance in fingerprint recognition was made in 1899 by Edward Henry, who (actually his two assistants from India) established the well-known "Henry system" of fingerprint classification. By the early twentieth century, the formation of fingerprints was well understood. The biological principles of fingerprints are summarized below:

1. Individual epidermal ridges and valley have different characteristics for different fingerprints.
2. The configuration types are individually variable, but they vary within limits that allow for a systematic classification.
3. The configurations and minute details of individual ridges and furrows are permanent and unchanging.



a) Dermatoglyphics drawn by Grew. b) Mayer's drawings of fingerprints.

Figure 1.7.2 Example of the first scientific proposed ridge, valley and pore structure in fingerprint **[1,5]**

a) Trademark of Thomas Bewick. b) The nine patterns illustrated in Purkinje's thesis

Figure 1.7.3 Example of first using fingerprint and first classification scheme [1,5]

The first principle constitutes the foundation of fingerprint recognition and the second principle constitutes the foundation of fingerprint classification. In the early twentieth century, fingerprint recognition was formally accepted as a valid personal identification method and became a standard routine in forensics. Fingerprint identification agencies were set up worldwide and criminal fingerprint databases were established. Various fingerprint recognition techniques, including latent fingerprint acquisition, fingerprint classification, and fingerprint comparison were developed. For example, the FBI fingerprint identification division was set up in 1924 with a database of 810,000 fingerprint cards (see Federal Bureau of Investigation).

With the rapid expansion of fingerprint recognition in forensics, operational fingerprint databases became so huge that manual fingerprint identification became infeasible. For example, the total number of fingerprint cards (each card contains one impression for each of the 10 fingers of a person) in the FBI fingerprint database now stands well over 200 million from its original number of

810,000 and is growing continuously. With thousands of requests being received daily, even a team of more than 1,300 fingerprint experts were not able to provide timely responses to these requests. Starting in the early 1960s, the FBI, Home Office in the UK, and Paris Police Department began to invest a large amount of effort in developing automatic fingerprint identification systems. Based on the observations of how human fingerprint experts perform fingerprint recognition, three major problems in designing AFISs were identified and investigated: digital fingerprint acquisition, local ridge characteristic extraction, and ridge characteristic pattern matching. Their efforts were so successful that today almost every law enforcement agencies worldwide uses an AFIS. These systems have greatly improved the operational productivity of law enforcement agencies and reduced the cost of hiring and training human fingerprint experts.

Fingerprint enhancement based automatic fingerprint recognition technology has now rapidly grown beyond forensic applications in civilian and commercial applications. In fact, fingerprint-based biometric systems are so popular that they have almost become the synonym for biometric systems.

1.8 Formation of Fingerprints

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the finger tips. This property makes fingerprints a very attractive biometric identifier. Biological organisms, in general, are the consequence of the interaction of genes and environment. It is assumed that the phenotype is uniquely determined by the interaction of a specific genotype and a specific environment. Physical appearance and fingerprints are, in general, a part of an individual's phenotype. In the case of fingerprints, the genes determine the general characteristics of the pattern. Fingerprint formation is similar to the growth of capillaries and blood vessels in angiogenesis.The general characteristics of the fingerprint emerge as the skin of the fingertip begins to differentiate. However, the flow of amniotic fluids around the fetus and its position in the uterus change during the differentiation process. Thus, the cells on the fingertip grow in a microenvironment that is slightly different from hand to hand and finger to finger. The finer details of the fingerprints are determined by this changing microenvironment. A small difference in micro environ is amplified by the differentiation process of the cells. There are so many variations during the formation of fingerprints that it would be virtually impossible for two fingerprints to be alike. But since the

fingerprints are differentiated from the same genes, they will not be totally random patterns either. We could say that the fingerprint formation process is a chaotic system rather than a random one.

1.9 Individuality of Fingerprints

Although the word "fingerprint" is popularly perceived as synonymous with individuality, uniqueness of fingerprints is not an established fact but an empirical observation. With the stipulation of widespread use of fingerprints, however, there is a rightfully growing public concern about the scientific basis underlying individuality of fingerprints. Lending erroneous legitimacy to these observations will have disastrous consequences, especially if fingerprints will be ubiquitously used to recognize citizens for reasons of efficiency, convenience, and reliability in guarding against security threats and identity fraud. Furthermore, automated fingerprint recognition systems do not appear to use all the available discriminatory information in the fingerprints, but only a parsimonious representation extracted by an automatic feature extraction algorithm.

1.10 Fingerprint Sensing and Storage

Based on the mode of acquisition, a fingerprint image may be classified as off-line or live-scan. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. The inked impression is then digitized by scanning the paper using an optical scanner or a high-quality video camera. A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact. A particular kind of off-line images, extremely important in forensic applications, are the so-called latent fingerprints found at crime scenes. The oily nature of the skin results in the impression of a fingerprint being deposited on a surface that is touched by a finger. These latent prints can be "lifted" from the surface by employing certain chemical techniques.

The main parameters characterizing a digital fingerprint image are: resolution, area, number of pixels, geometric accuracy, contrast, and geometric distortion. To maximize compatibility between digital fingerprint images and to ensure good quality of the acquired fingerprint impressions among various AFIS, the US Criminal Justice Information Services (CJIS) released a set of specifications that regulate the quality and the format of both fingerprint images and FBI-compliant off-line/live-scan scanners. More recently, the FBI has defined another, less stringent, image quality standard for single-finger capture devices in civilian applications (more specifically for the Personal Identity

Verification [PIV] program in the United States). Most of the commercial live-scan devices, designed for the non-AFIS market, do not meet the FBI specifications but, on the other hand, are designed to be compact, and cheap. The operational quality of fingerprint scanners (e.g., the impact of the scanner quality parameters on the fingerprint recognition accuracy) has been the subject of some recent studies.

There are a number of live-scan sensing mechanisms (e.g., optical FTIR, capacitive, thermal, pressure-based, ultrasound, etc.) that can be used to detect the ridges and valleys present on the fingertip. Figure 1.10.1 shows an off-line fingerprint image acquired with the ink technique, a latent fingerprint image, and some live-scan images acquired with different types of commercial live-scan devices. Although optical fingerprint scanners have the longest history, the new solid-state sensors are gaining increasing popularity because of their compact size and the ease with which they can be embedded in consumer products such as laptop computers, cellular phones and PDAs. Figure 1.10.1 fingerprint images from a) a live-scan FTIR-based optical scanner; b) a live-scan capacitive scanner; c) a live-scan piezoelectric scanner; d) a live-scan thermal scanner; e) an off-line inked impression, and f) a latent fingerprint.

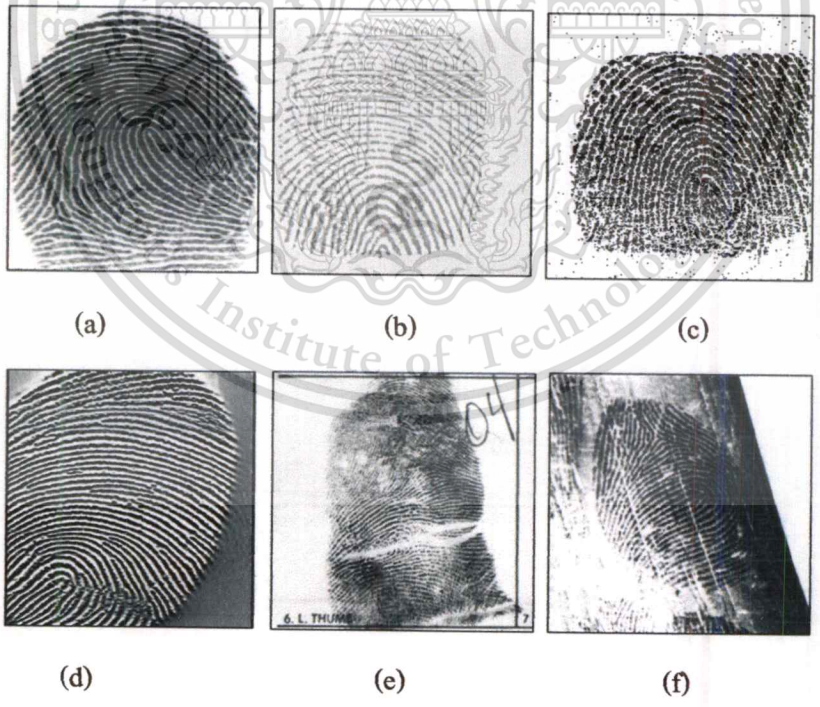


Figure 1.10.1 Fingerprint images of acquisition.

Figure 1.10.2 shows some examples of fingerprint sensors embedded in a variety of computer peripherals and other devices. Storing raw fingerprint images may be problematic for large-scale identification systems. In 1995, the size of the FBI fingerprint card archive contained over 200 million items, and archive size was increasing at the rate of 30,000 to 50,000 new cards per day. Although the digitization of fingerprint cards seemed to be the most obvious choice, the resulting digital archive could become extremely large. In fact, each fingerprint card, when digitized at 500 dpi requires about 10 megabytes of storage. A simple multiplication by 200 million yields the massive storage requirement of 2,000 terabytes for the entire archive. An effective compression technique was urgently needed. Unfortunately, neither the well-known lossless methods nor the JPEG methods were found to be satisfactory. A new compression technique (with small acceptable loss), called Wavelet Scalar Quantization (WSQ), became the FBI standard for the compression of 500 dpi fingerprint images. Besides WSQ, a number of other compression techniques (including JPEG2000) have been proposed.

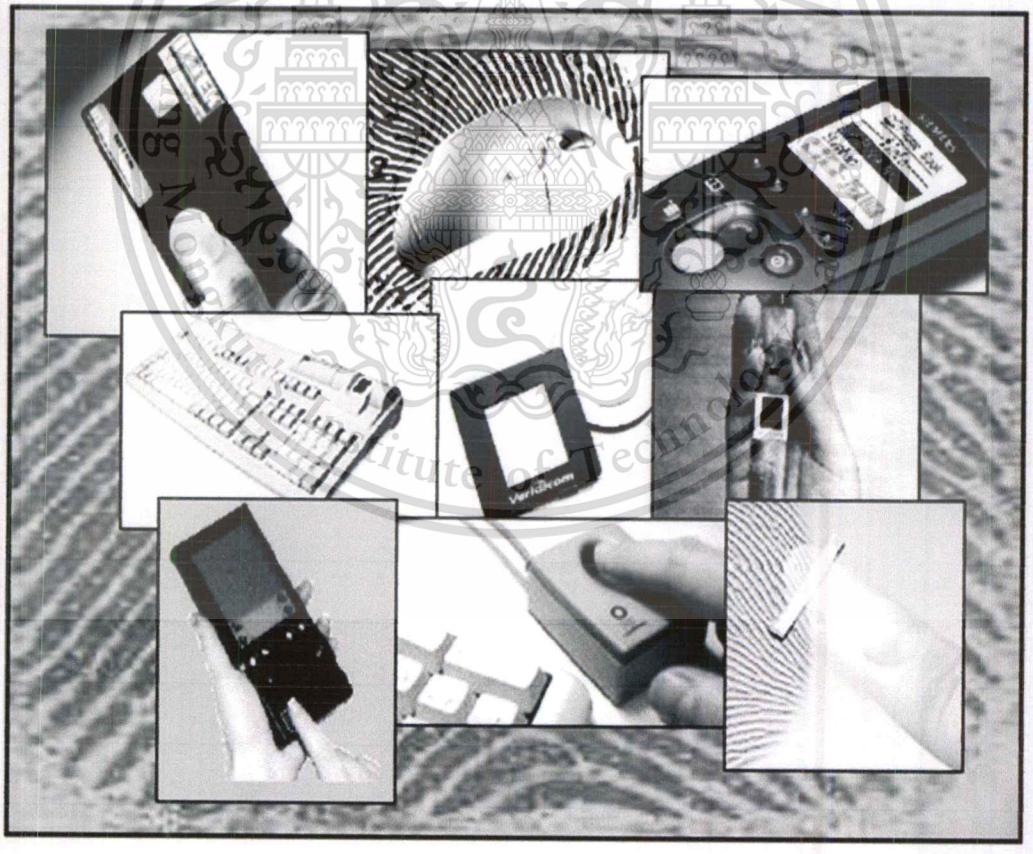


Figure 1.10.2 Fingerprint sensors can be embedded in a variety of devices for User recognition.

1.11 Fingerprint Representation and Feature Extraction

The representation issue constitutes the essence of fingerprint recognition system design and has far-reaching implications on the matching modules. The pixel intensity values in the fingerprint image are not invariant over time of capture and there is a need to determine salient features of the input fingerprint image that can discriminate between identities as well as remain invariant for a given individual. Thus the problem of representation is to determine a measurement (feature) space in which the fingerprint images belonging to the same finger form a compact cluster (low intra-class variations) and those belonging to different fingers occupy different portions of the space (high inter-class variations).

A good fingerprint representation should have the following two properties: Saliency and suitability. Saliency means that a representation should contain information about the distinctive fingerprint. Suitability means that the representation can be easily extracted, stored in a compact fashion, and be useful for matching. A salient representation is not necessarily a suitable representation. In addition, in some biometrics applications, storage space is at a premium. For example, only a few kilobytes of storage are typically available in a smart card. In such situations, the representation also needs to be compact.

Image-based representations, constituted by pixel intensity information, do not perform well due to factors such as brightness variations, image quality variations, scars, and large global distortions present in fingerprint images. Furthermore, an image-based representation requires a considerable amount of storage. On the other hand, an image-based representation preserves the maximum amount of information and makes fewer assumptions about the application domain. For instance, it is extremely difficult to extract any high level features from a (degenerate) finger devoid of any ridge structure. The fingerprint pattern, when analyzed at different scales, exhibits different types of features.

- Level 1: at the global level, the ridge line flow delineates a pattern similar to one of those shown in Figure 1.11.1. Singular points, called loop and delta (denoted as squares and triangles, respectively in Figure 1.11.1), act as control points around which the ridge lines are "wrapped".

- Level 2: at the local level, a total of 150 different local ridge characteristics, called minute details, have been identified. These local ridge characteristics are not evenly distributed. Most of them depend heavily on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics, called minutiae (see Figure 1.11.2) are: ridge endings and ridge bifurcations. A ridge ending is defined as the ridge point where a ridge ends abruptly. A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges. Minutiae in fingerprints are generally stable and robust to fingerprint impression conditions. Although a minutiae-based representation is characterized by a high saliency, reliable automatic minutiae extraction can be problematic in extremely low-quality fingerprints devoid of any ridge structure.

Figure 1.11.1 a) left loop, b) right loop, c) whorl, d) arch, and e) tented arch; squares denote loop-type singular points, and triangle delta-type singular points.

a) Whorl b) Left Loop c) Right Loop b) Tent or arch

Figure 1.11.1 Fingerprint global features

- Level 3: at the very-fine level, intra-ridge details can be detected. These include width, shape, curvature, edge contours of the ridges as well as other permanent details such as dots and incipient ridges. One of the most important fine-level details are the finger sweat pores (see Figure 1.11.2), whose positions and shapes are considered highly distinctive. However, extracting very-fine details including pores is feasible only in high-resolution (e.g., 1,000 dpi) fingerprint images of good quality and therefore this kind of representation is not practical for non-forensic applications.

Figure 1.11.2 Minutiae (black-filled circles) in a portion of fingerprint image; sweat pores (empty circles) on a single ridge line.

1.12 Definitions of Fingerprint

The fingerprint is the most important for today's information technology to be able to securely protect information access to the proper authenticated users. Critical information can be lost, stolen or tempered and that can result in lots of opportunities and/or revenues for the company and business. Fingerprint identification is a popular personal identification method for several key reasons: Fingerprints do not change over time; all fingerprints are unique; even identical twins have different sets of fingerprints; fast enrollment and matching of fingerprint; easy to use; low-cost implementation; unique identification is accepted worldwide; and able to store up to ten fingers for each personal enrollment in case of potential injury to the hand.

A fingerprint is the feature pattern of one finger shown in Figure 1.12.1 (a). It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have been used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and valley. These ridges and valley present good similarities in each small local window, like parallelism and average width.

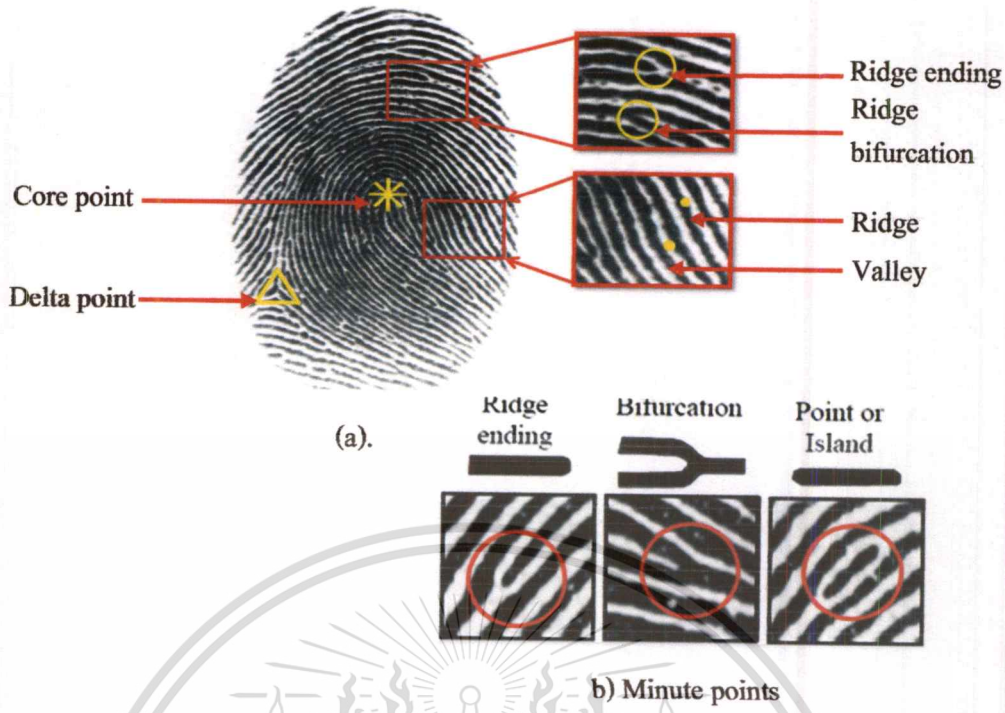


Figure 1.12.1 Real fingerprint local features Level 2 (black line).

However, shown by intensive research on fingerprint matching , fingerprint is distinguished by their ridges and valley, but by minutia for fingerprint identification, which are some abnormal points on the ridges shown in Figure 1.12.1 b). Among the variety of minutia types have been reported in fingerprint recognition, two are most significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive.

1.13 Approach

Fingerprint matching is the most of important in recognition a person based on his physiological and behavioral characteristics is known as biometrics. Biometrics have gained a lot of importance in the recent past due to increase in crime rate and the need of more robust and automated security. People from many different backgrounds have contributed for development of biometric system for number of years, for example researchers from fields like sensors, image processing, signal processing, pattern recognition, database management, software development etc. Fingerprints are the most widely used biometric features for personal identification based on physiological and behavioral characteristic.

In this thesis an approach has been presented which addresses the various issues (discussed in the previous section) in fingerprint matching. The aim is to reduce the error rates, namely False Acceptance Rate (FAR) and False Rejection Error (FRR) in the existing fingerprint matching algorithms. In the case of implementation, the proposed techniques and algorithms are implemented using MATLAB.

1.14 Thesis Outline

After the general introduction of biometric system, various characteristics of application of fingerprint with a background and related works in the area of fingerprint matching. The rest of the thesis is organized in the following way.

Chapter2 presents fingerprint matching , the background information and reviews of brief matching algorithm in the literature. The background includes the details of describing the general technique in image processing, fingerprint matching and classification techniques, the next literature review of fingerprint matching techniques corresponding to our proposed.

Chapter3 Proposed hierarchical of fingerprint matching, it is main methodologies for fingerprint matching techniques, i) fingerprint matching by using the normalized cross correlation technique, ii) Fingerprint Matching based on Minutiae Technique, iii) Fingerprint matching based on two dimensional discrete Fourier transform Features, iv) Fingerprint matching using the two dimensional discrete cosine transform, v) Fingerprint matching by using normalized cross correlation and two dimensional Fourier transform. And the next chapter will illustrate the experiment and the results.

Chapter4 will illustrate the experiment and the results. Further, discussion of each fingerprint matching techniques. The performance of fingerprint matching measures for its improvement by the score similarity between the template image and the test image.

Chapter5 presents the main of the contribution this thesis, discussion, conclusions and future extension possibilities of this work.

Chapter 2

Background and literature review

A fingerprint recognition system may operate either in verification mode or identification mode. In verification mode, the system verifies an individual's identity by comparing the input fingerprint with the individual's own template *(t)* stored in the database. In, the identification mode, the system identifies an individual by searching the templates of all the users in the database for a match. The fingerprint classifier cation and indexing techniques are used to speed up the search in fingerprint based identification systems. The fingerprint feature extraction and matching algorithms are usually quite similar for both fingerprint verification and identification problems. In this thesis the focus is on fingerprint based verification systems. This chapter discusses the current state of the art feature extraction techniques and gives a literature survey on the various fingerprint matching algorithms.

2. Image Preprocessing

The preprocessing steps try to compensate for the variations in lighting, contrast and other inconsistencies which are introduced by the sensor during the acquisition process. The following preprocessing steps are generally used:

- Gaussian Blur: A Gaussian blur is a convolution operation which is applied to the original fingerprint image to reduce image noise (introduced by the sensor). The Gaussian kernel used for blurring is given by:

$$G(x,y) = \frac{1}{2\pi\sigma} e^{-\frac{x^2+y^2}{2\sigma}} \tag{2.1}$$

Where σ is the variance of the Gaussian distribution, x is the distance from the origin along the horizontal axis, y is the distance from the origin along the vertical axis.

- Sliding-window Contrast Adjustment : Sliding-window contrast adjustment is used to compensate for any lighting inconsistencies within a fingerprint and to obtain contrast consistency among different fingerprints. A $m \times m$ window is centered on each pixel of the

Gaussian blurred image. The corresponding output pixel value is then calculated by finding the minimum and maximum intensity values within the window and by using:

$$O(i,j) = (I(i,j) - \min_{ij})\left(\frac{255}{\max_{ij} - \min_{ij}}\right) \tag{2.2}$$

Were $I(i,j)$ and $O(i,j)$ are the input and output pixel intensity values respectively, and are $\max_{ij}$ the minimum and maximum pixel intensity values within $m \times m$ window centered at pixel *(i,j)*.

- Histogram-based Intensity Level Adjustment : This final step is used to further enhance the ridges and valleys. The image's histogram is examined to determine two intensity values: a lower threshold L and an Upper threshold U. The intensity value $(I(i,j))$ of each pixel is processed using these thresholds to obtain the output pixel intensity $(O(i,j))$ which is given by the following equation:

$$O(i,j) = \begin{cases} 255 & \text{if } I(i,j) > U \\ 0 & \text{if } O(i,j) < L \\ (I(i,j-L)\left(\frac{255}{U-L}\right) & \text{else} \end{cases} \tag{2.3}$$

2.1 Fingerprint Enhancement

Fingerprints are widely used for authentication purpose due to their proved distinctiveness. This uniqueness comes from unique local characteristics ridge bifurcations and ridge endings known as minutiae. Most of the fingerprint matching algorithms use details of these minutiae points to compare two fingerprint images. The performance of these algorithms depends significantly on the quality of fingerprint images. In many cases, fingerprint with numerous discontinuous ridges poor quality such as dry, wet, damped, scars and smudges can cause errors in the fingerprinting identification process, and also the quality of fingerprint images differs due to many factors like imaging conditions, type of sensor is used, acquisition conditions, age, skin characteristics etc. Minutiae from poor quality images contain many pseudo-minutiae. These pseudo-minutiae can affect the performance of a matching algorithm significantly. Therefore, we need an effective fingerprint

image enhancement procedure to eliminate these pseudo-minutiae and thus improve the performance of a fingerprint matching algorithm.

In this [7,8] approach involves the normalization of the fingerprint image so that it has a pre-specified mean and variance. Due to imperfections in the fingerprint image capture process such as non-uniform ink intensity or non-uniform contact with the fingerprint capture device, a fingerprint image may exhibit distorted levels of variation in grey-level values along the ridges and valleys. Thus, normalization is used to reduce the effect of these variations, which facilitates the subsequent image enhancement steps.

An orientation image is then calculated [3,7,8,9], which is a matrix of direction vectors representing the ridge orientation at each location in the image. The widely employed gradient-based approach is used to calculate the gradient, which makes use of the fact that the orientation vector is orthogonal to the gradient. Firstly, the image is partitioned into square blocks and the gradient is calculated for every pixel, in the x and y directions. The orientation vector for each block can then be derived by performing an averaging operation on all the vectors orthogonal to the gradient pixels in the block. Due to the presence of noise and corrupted elements in the image, the ridge orientation may not always be correctly determined. Given that the ridge orientation varies slowly in a local neighborhood, the orientation image is then smoothed using a low-pass filter to reduce the effect of an outlier.

The next step in the image enhancement process is the estimation of the ridge frequency image. The frequency image defines the local frequency of the ridges contained in the fingerprint. Firstly, the image is divided into square blocks and an oriented window is calculated for each block. For each block, an x-signature signal is constructed using the ridges and valleys in the oriented window. The x-signature is the projection of all the gray level values in the oriented window along a direction orthogonal to the ridge orientation. Consequently, the projection forms a sinusoidal-sharp wave in which the center of a ridge maps itself as a local minimum in the projected wave. The distance between consecutive peaks in the x-signature can then be used to estimate the frequency of the ridges.

In our method used fingerprint enhancement methods based on the Gabor filter have been widely used to facilitate various fingerprint applications such as fingerprint matching and fingerprint

classification. Gabor filters are bandpass filters that have both frequency-selective and orientation-selective properties, which mean the filters can be effectively tuned to specific frequencies and orientation values. One useful characteristic of fingerprints is that they are known to have well defined local ridge orientation and ridge frequency. Therefore, the enhanced algorithm takes advantage of this regularity of spatial structure by applying Gabor filters that are tuned to match the local ridge orientation and frequency.

2.1.1 Fingerprint Enhancement Process

In this Fingerprint matching method we enhance the quality of fingerprint images by using directional filtering (Gabor filtering). And the process follows the step below.

2.1.2 Normalization

The normalization is basically employed to standardize the intensity values in an image by adjusting the range of gray-level values so that it lies within a desired range of values. Let, *I(x, y)* denote the gray-level value at pixel *(i,j)*, M and VAR denote the estimated mean and variance of image *I*, respectively, and *N(i,j)* denote the normalized gray-level value at pixel (*x, y*). The normalized image is defined as:

$$N(x,y)=\begin{cases} M_0+\sqrt{\dfrac{VAR_0(I(x,y)-M)^2}{VAR}} & \text{if } I(x,y) \\ M_0-\sqrt{\dfrac{VAR_0(I(x,y)-M)^2}{VAR}} & \text{otherwise} \end{cases} \tag{2.4}$$

Where, M_0 and VAR_0 are the desired mean and variance values, respectively. In this work, we set values mean $M_0 = 0.5$ and variance $VAR_0 = 1$. The mean and variance of a gray-level fingerprint image with the dimension of $M \times N$ pixels are defined respectively as:

$$M(I)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}I(x,y) \tag{2.4.1}$$

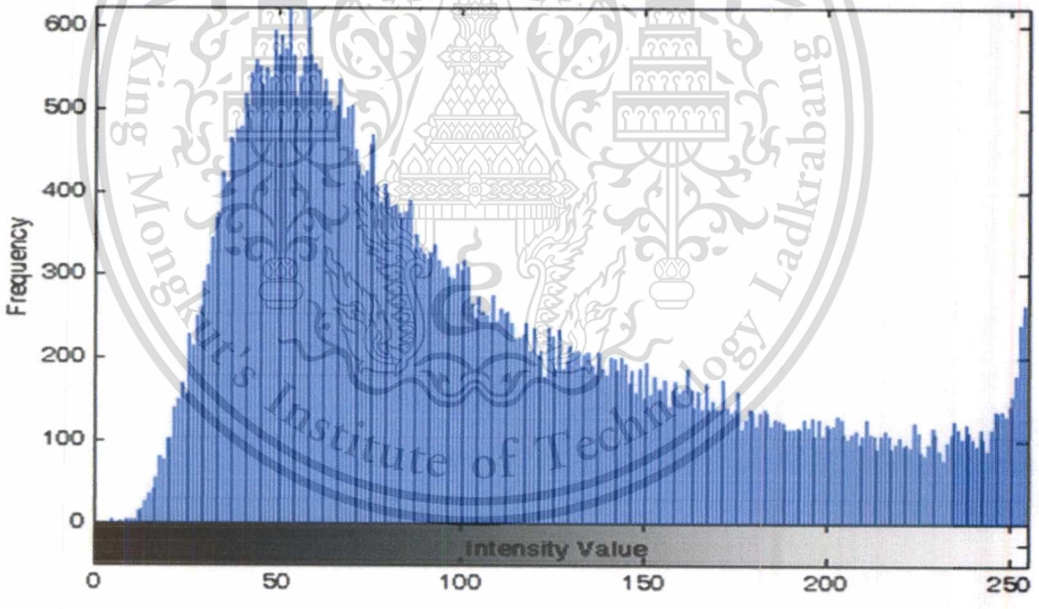
And

$$VAR(I)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\big(I(x,y)\_M(x,y)\big)^2 \tag{2.4.2}$$

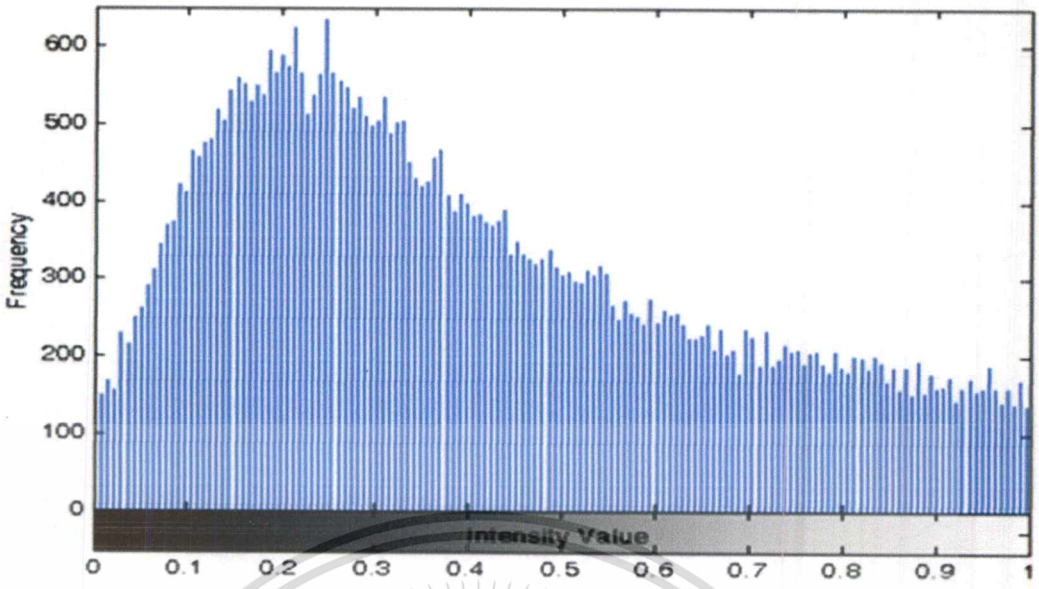
Where $I(x,y)$, represents the intensity of the pixel at x^{th} row and y^{th} column. The main purpose of the normalization operation is to reduce the variance of gray-level values along the ridges and valleys. The operation is pixel-wise and does not change the clarity of the ridges and valleys as Figure 2.1.1 shown examples of the histogram of the normalization.

(a) Original image

(b) Normalization



(c) Histogram of original image



(d) Histogram of normalized image

Figure 2.1.1 Example of histogram of the normalization.

2.1.3 Segmentation

The segmentation is the process of separating the foreground regions in the image from the background regions. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information. When minutiae extraction algorithms are applied to the background regions of an image, it results in the extraction of noise and false minutiae. Thus, segmentation is employed to discard these background regions, which facilitates the reliable extraction of minutiae.

In a fingerprint image, the background regions generally exhibit a very low grey-scale variance value, whereas the foreground regions have a very high variance. Hence, a method based on variance threes holding can be used to perform the segmentation. Firstly, the image is divided into blocks and the grey-scale variance is calculated for each block in the image. If the variance is less than the global threshold, then the block is assigned to be a background region;

otherwise, it is assigned to be part of the foreground. The grey-level varies for a block of size $W \times W$ is defined as:

$$V(k) = \frac{1}{W^2} \sum_{x=0}^{W-1} \sum_{y=0}^{W-1} (I(x,y) - M(k))^2 \quad (2.4.3)$$

Where $V(k)$ is the variance for block k, $I(x;y)$ is the grey-level value at pixel $(x; y)$, and $M(k)$ is the mean grey-level value for the block k and Figure 2.3.2 illustrated Example of segmentation.

(a) Original image (b) Segmentation

Figure 2.1.2 Example of fingerprint image segmentation.

2.1.4 Orientation field estimation

The ridge orientation (orientation field) at a pixel (x, y) is the angle θ_{xy} that the fingerprint ridges, crossing through an arbitrary small neighborhood centered at (x, y), form with the horizontal axis. Because fingerprint ridges are not directed, θ_{xy} is an unoriented direction lying in [0 -180°]. In the rest of the thesis we use the term orientation to denote an unoriented direction in [0 -180°], and the term direction to indicate an oriented direction in [0 - 360°].

Instead of computing ridge orientation field at each pixel, most of the fingerprint processing and feature extraction methods estimate the ridge orientation at discrete positions (this reduces computational efforts and still allows estimates at other pixels to be obtained through interpolation). The fingerprint orientation image (also called directional image), first introduced by [10] is a matrix whose elements encodes the local orientation of the fingerprint ridges. Each element θ_{ij} , corresponding to the node (i, j) of a square-meshed grid located over the pixel (x_i, y_j) , denotes the average orientation of the fingerprint ridges in a neighborhood of (x_i, y_j) (see Figure2.3.3). Each element denotes the orientation field of the fingerprint ridges; the element length is proportional to its reliability. An additional value r_{ij} is often associated with each element θ_{ij} to denote the reliability (or consistency) of the orientation. The value r_{ij} is low for noisy and seriously corrupted regions and high for good quality regions in the fingerprint image.

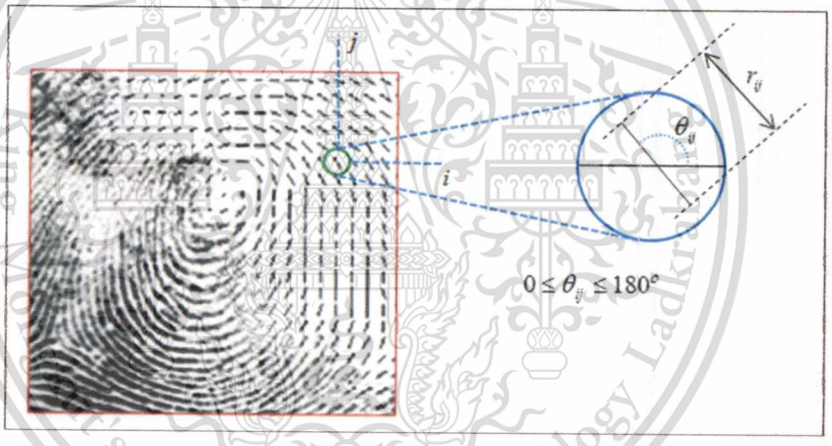


Figure 2.1.3 A fingerprint image faded into the corresponding orientation image computed over a square-meshed grid of size 16×16

Gradient-based approaches: the simplest and most natural approach for extracting local ridge orientation is based on computation of gradients in the fingerprint image. The gradient $\partial(x, y)$ at point (x, y) of m, is a two dimensional vector $[\partial x(x, y), \partial y(x, y)]$, where ∂x and ∂y components are the derivatives of I at (x, y) with respect to the x and y directions, respectively. It is well known that the gradient phase angle denotes the direction of the maximum intensity change. Therefore, the direction θ of a hypothetical edge crosses the region deterred at (x, y) is orthogonal to the gradient phase angle at (x, y). This method, although simple and efficient, has some drawbacks. First using the classical

Sobel convolution mask [8, 9] to determine ∂x and ∂y components of the gradient, and computing θ as the arc tangent of $\partial y/\partial x$ ratio, preset problem due to non-linearity and discontinuity around 90°. Second, a single orientation estimate reflects the ridge and the valley orientation at too fine a scale and is generally very sensitive to the noise in the fingerprint image; On the other hand, simply averaging gradient estimate is not meaningful due to the circularity of angles: the average orientation between 5° and 175° is not 90° (as an arithmetic average suggests) but 0°. Furthermore, the concept of average orientation is not always well defined; consider the two orthogonal orientation 0° and 90° ; is the correct average orientation 45° and 135°. In [11] proposed a simple but a smooth solution to the above problem, which allows a local gradient estimate is encoded by a vector:

$$d = [r\cos 2\theta, r\sin 2\theta] \tag{2.4.4}$$

Where 2θ is used in place of θ to discount the circularity of angles and r is proportion to the orientation estimate strength (e.g., the square norm of gradient: $\partial_x^2 + \partial_y^2$). Averaging angles in local $n \times n$ window W to obtain a more robust estimate $\overline{d}$, can be performed by separate averaging the two (x and y) components:

$$\overline{d} = \left[\frac{1}{n^2} \sum_W r\cos 2\theta, \frac{1}{n^2} \sum_W r\sin 2\theta, \right] \tag{2.4.5}$$

Computing the average between two orthogonal orientations with equation (2.4.5) involves summing to vectors facing each other, and therefore the length of the resulting vector is zero. This indicates that the vector is meaningless, independent of its orientation.

$$\theta_{ij} = 90° + \frac{1}{2} a\tan 2\left(2G_{xy}, G_{xx} - G_{yy}\right) \tag{2.4.6}$$

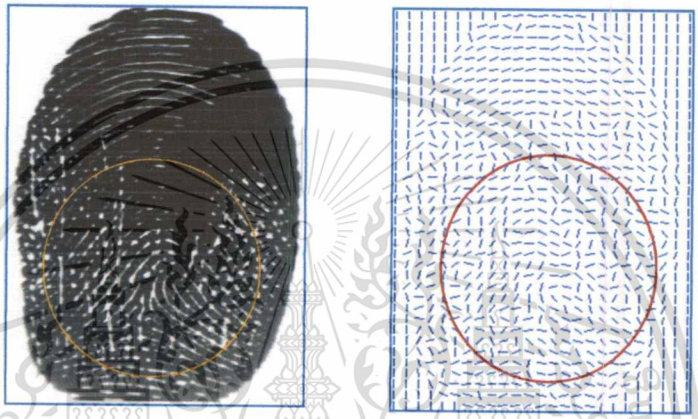
Where,

$$G_{xy} = \sum_{h=-8}^{8} \sum_{k=-8}^{8} \partial_x(x_i + h, y_j + k)\partial_y(x_i + h, y_j + k) \tag{2.4.7}$$

$$G_{xx} = \sum_{h=-8}^{8} \sum_{k=-8}^{8} \partial_x(x_i + h, y_j + k)^2 \tag{2.4.8}$$

$$G_{yy} = \sum_{h=-8}^{8} \sum_{k=-8}^{8} \partial_y (x_i + h, y_j + k)^2 \tag{2.4.9}$$

Where ∂x and ∂y are the x- and y-gradient components computed through 3x3 Sobel masks (see [59, 62]), and atan2 *(y,x)* calculates the arc tangent of the two variables y and x: it is similar to calculating the arc tangent of y/x, except that the signs of both arguments are used to determine the quadrant of the result. An example of local orientation image computed by equation (2.4.6) is shown in Figure 2.1.4 b).

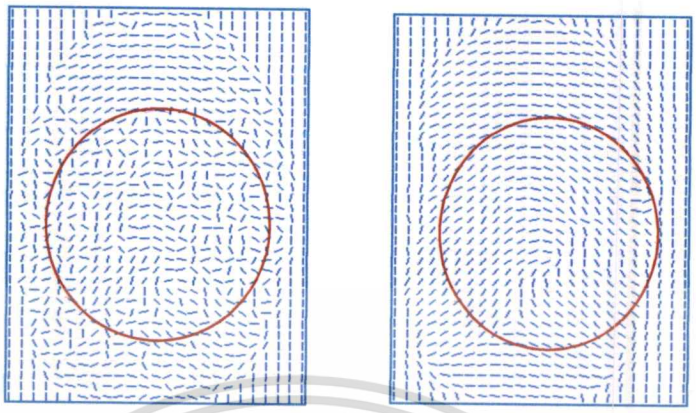


(a) Original image (b) Field estimation

Figure 2.1.4 Orientation field estimation is computed with the equation (2.4.6).

The orientation field smoothing computed from poor quality fingerprints may contain several unreliable elements due to creases, local cluttered noise. In this situation, a field smoothing can be very useful in enhancing. This can be done by (re) converting the angles in orientation vector d (equation (2.4.3) and by averaging them through equation (2.4.5). Figure 2.1.5 shows an example of orientation image smoothing. However, such a simple averaging has some limitations (Figure 2.1.4 b): It is ineffective when the incorrect orientations dominate the correct ones; tends to smooth out high curvature values, especially in singular point regions; and tends to slightly shift the loop singularities. Figure 2.1.5 a) field estimation of in a fingerprint through the gradient-based approach corresponding to equation (2.4.6), in the noisy regions the estimation is unreliable; b) increase window of filter smoothing are applied, resulting in a more consistent representation; it is worth noting that while the smoothing recovered the correct orientation at several places (e.g., inside the

solid circle), it altered the average orientation inside the region denoted by the circle where incorrect orientations were dominating the correct one.



(a) Field estimation (b) Field smooths

Figure 2.1.5 Example of orientation field smoothing.

2.1.5 Ridge frequency estimation

The local ridge frequency (or density) f_{xy} at point (x, y) is the number of ridges per unit length along a hypothetical segment centered at (x, y) and orthogonal to the orientation field θ_{xy}. A frequency image, analogous to the orientation image, can be defined if the frequency is estimated at discrete positions and arranged into a matrix. The ridge frequency estimation varies across different fingers, and may also noticeably vary across different regions of the same fingerprint. The next step is to project the gray-level values of all the pixels located inside each block along a direction orthogonal to the local ridge orientation. This projection forms an almost sinusoidal-sharp wave with the local minimum points corresponding to the ridges in the fingerprint. An example of a projected waveform is shown in Figure 2.1.6

Have referred the original frequency estimation stage used by [7, 8] to include an additional projection smooth step prior to computing the ridge spacing. This involves smoothing the projected waveform using a Gaussian lowpass filter of size to reduce the effect of noise in the projection. The ridge spacing $T(x,y)$ is then computed by counting the median number of pixels between consecutive minima points in the projected waveform. Hence, the ridge frequency $f(x,y)$ for a block center of a pixel (x_i, y_j) is defined as $f_{xy} = 1/T(x,y)$.

Given that the fingerprint scans at a fixed resolution, then ideally the ridge frequency values should lie within a certain range. However, there are cases where a valid frequency value cannot be reliably obtained from the projection. Examples are when no consecutive peaks can be detected from the projection, and also when minutiae points appear in the block. For the blocks where minutiae points appear, the projected waveform does not produce a well-defined sinusoidal shape wave, which can lead to an inaccurate estimation of the ridge frequency. Thus, the out of range frequency values are interpolated using values from neighboring blocks that have a well-defined frequency.

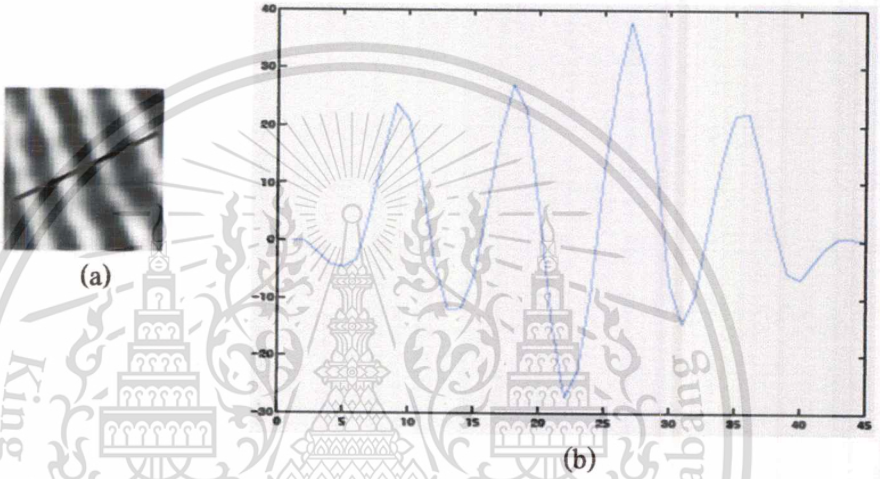


Figure 2.1.6 The projection of the intensity values of the pixels along a direction orthogonal to the local ridge orientation

The orientation field estimation, the ridge frequency estimation is an important parameter used in the construction of the directional filtering. Note that of the ridge frequency values will be presented in terms of ridge wavelength for easier interpretation of the results. For example, if the ridge spatial frequency value is 1/10 pixels. We modify the original wavelength estimation stage used by [8] to include smoothing of the projected waveform prior to computing the ridge wavelength (see Figure 2.1.7), (a) A 32 × 32 block from a fingerprint image, b) the projected waveform of the block .The results for well-defined images (see Figure 2.1.7) show that the majority of the estimated wavelength values for each 32 x 32 block match up accurately with the actual wavelength value of 10.

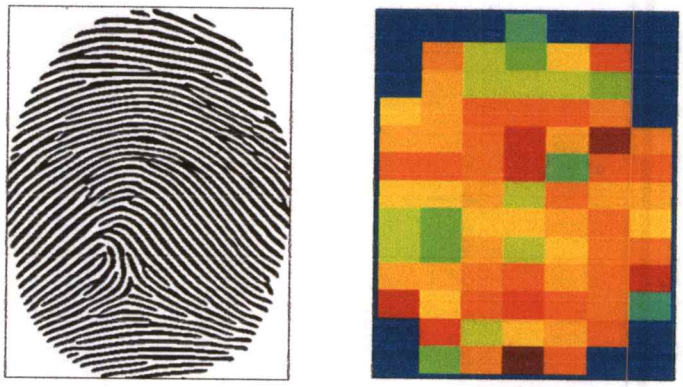


Figure 2.1.7 The estimated ridge wavelength (ridge frequency) for fingerprint images of wavelength

2.1.6 Minutiae Extraction

After a fingerprint image has been enhanced, the next step is to extract the minutiae from the enhanced image. Most automatic systems for fingerprint comparison are based on minutiae matching; hence, reliable minutiae extraction is an extremely important task and a substantial amount of research has been devoted to this topic. Most of the proposed methods require the fingerprint grayscale image to be converted into a binary image. Some binarization processes greatly benefit from an a priori enhancement; on the other hand, some enhancement algorithms directly produce a binary output, and therefore the distinction between enhancement and binarization is sometimes faded. The binary images are usually submitted to a thinning stage which allows for the ridge line thickness to be reduced to one pixel, resulting in the skeleton image (Figure 2.3.8). A simple image scans then allow the detection of pixels that correspond to minutiae .

2.1.7 Minutiae detection

The Crossing Number (CN) method is used to perform the minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3x3 window. The CN for a ridge pixel P is given by:

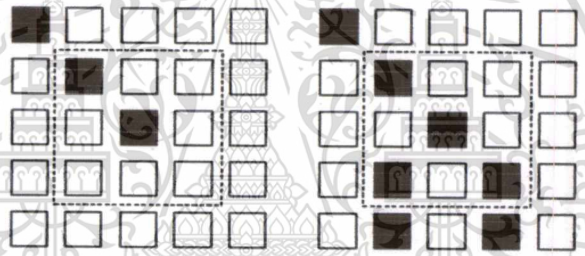
$$CN = 0.5\sum_{i=1}^{8}|P_i - P_{i+1}|, \qquad P_9 = P_1 \tag{2.4.10}$$

Where P_i is the pixel value in the neighborhood of P. For a pixel P, its eight neighboring pixels are scanned in an anti-clockwise direction as follows Table 2.1.7:

Table 2.1.7 Crossing Number computes in the eight neighboring pixels of minutiae detection.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value. As shown in Figure 2.3.8, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation and Figure 2.3.8 a) a Crossing Number of one corresponds to a ridge ending pixel. b). A crossing Number of three corresponds to the bifurcation pixel of minutiae detection.



a) CN=1 b) CN=3

Figure 2.1.8 Examples of a ridge ending and bifurcation pixel.

Figure 2.1.9 Minutiae detection, circles red and green corresponding to ridges ending and ridge bifurcation.

2.1.8 Binarization based methods

The general problem of image binarization has been widely studied in the fields of image processing and pattern recognition. The simplest approach uses a global threshold t and works by setting the pixels whose gray-level is lower than t to 0 and the remaining pixels to 1. In general, different portions of an image may be characterized by different contrast and intensity and, consequently, a single threshold for the entire image is not sufficient for a correct binarization. For this reason, the local threshold technique changes t locally, by adapting its value to the average local intensity. In the specific case of fingerprint images, which are sometimes of very poor quality, a local threshold method cannot always guarantee acceptable results and more effective fingerprint-specific solutions are necessary. In the rest of this section, the commonly used binarization methods used for fingerprints are briefly summarized.

a) Original image b) binary of enhancement c) Thinning

Figure 2.1.10 Results of applying binarization and thinning directly to the original image with enhanced.

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept [12]. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighborhoods. Using the properties of the CN as shown in Table 2.1.8 and Figure 2.1.11, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation.

Table 2.1.8 Properties of the Crossing Number.

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

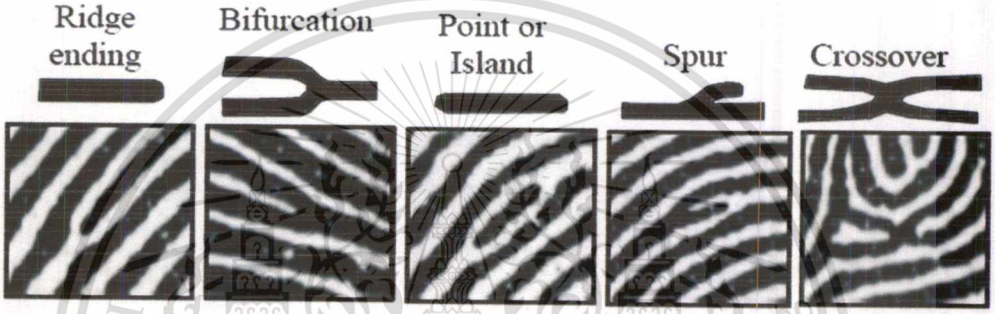


Figure 2.1.11 Five most common minutiae types (black line)

Other authors [13] have also performed minutiae extraction using the skeleton image. Their approach involves using a 3x3 window to examine the local neighborhood of each ridge pixel in the image. A pixel is then classified as a ridge ending if it has only one neighboring ridge pixel in the window, and classified as a bifurcation if it has three neighboring ridge pixels. Consequently, it can be seen that this approach is very similar to the Crossing Number method.

2.2 Fingerprint enhancement using Gabor filter

With an original fingerprint image there are noises, and may be low quality such as dry, wet, damped, scars, smudges and so on. In most cases, the degradation occurs in part. Without any attempts, it is hard to identify the core point and minutiae of such an image with those degradations. However, at this state noise could be removed by filtering techniques. Among those, Gabor filter is a promising one.

An effective method based on Gabor filters. Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains. As shown in Figure 2.4.1, a Gabor filter is defined by a sinusoidal plane wave (the second term of equation (2.4.1) tapered by a Gaussian (the first term in equation (2.4.2). Figure 2.2.1 Appearance of Gabor filter, only 0° and 90° oriented filters (mask size = 32x 32, $f = 0.11, \sigma_x = 4$, $\sigma_y = 4$). The even symmetric two-dimensional Gabor filter has the following form.

$$G(x, y : \theta, f) = \exp\left[-\frac{1}{2}\left(\frac{x_\theta^2 + y_\theta^2}{\sigma_x^2 + \sigma_y^2}\right)\right]\cos(2\pi f x_\theta) \tag{2.5}$$

Where θ is the orientation of the filter, and (x_θ, y_θ) are the coordinates of (x, y) after a clockwise rotation of the Cartesian axes by an angle of $(90°-\theta)$.

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \cos(90° - \theta) & \sin(90° - \theta) \\ -\sin(90° - \theta) & \cos(90° - \theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \tag{2.5.1}$$

In the above expressions, f is the frequency of a sinusoidal plane wave, and σ_x and σ_y are the standard deviations of the Gaussian envelope along the x- and y-axes, respectively. Figure 2.2.1 defined by the parameters $\theta = 135°$, $f = 1/5$ and $\sigma_x = \sigma_y = 3$.

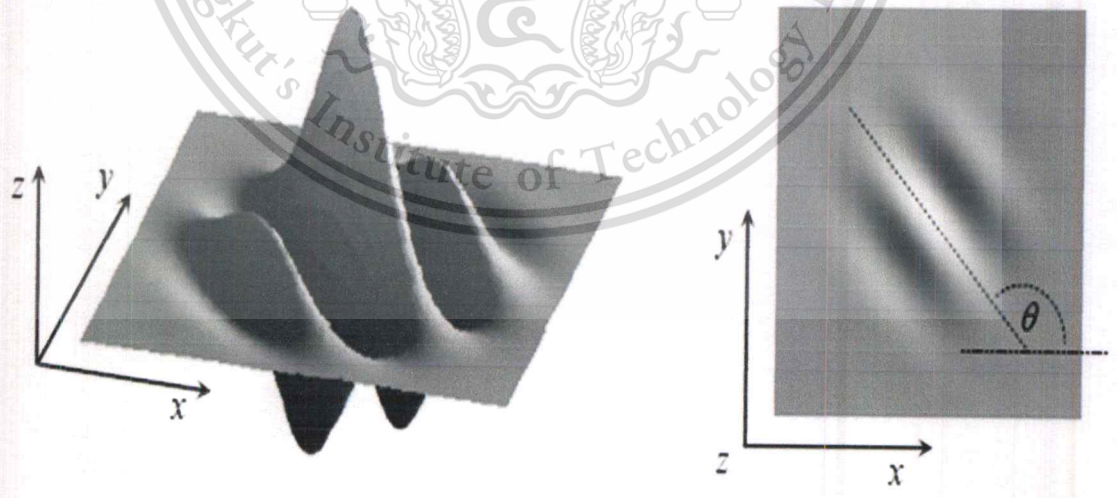
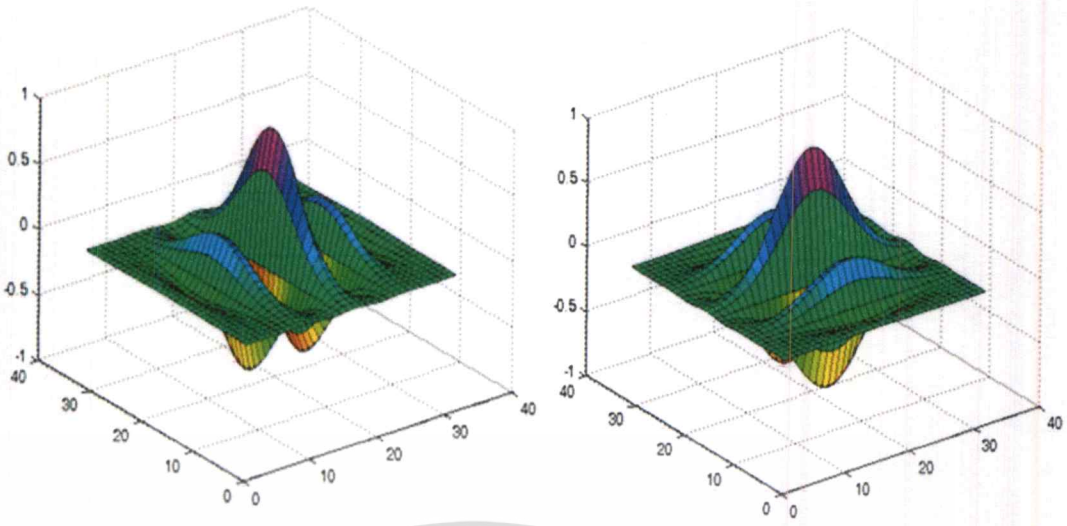


Figure 2.2.1 Graphical appearance of the Gabor filter.



a) $\theta = 0^\circ$ Orientation

b) $\theta = 90^\circ$ orientation

Figure 2.2.2 Appearance of Gabor filters different of oriented filters.

To apply Gabor filters to an image, the four parameters (θ, f, σ_x, σ_y) must be specified. Obviously, the frequency of the filter is completely determined by the local ridge frequency and the orientation is determined by the local ridge orientation. The selection of the values σ_x and σ_y involves a tradeoff. The larger the values, the more robust the filters are to the noise in the fingerprint image, but they are also more likely to create spurious ridges and valleys. On the other hand, the smaller the values, the less likely the filters are to introduce spurious ridges and valleys but then they will be less effective in removing the noise. In fact, from the Modulation Transfer Function (MTF) of the Gabor filter, it can be shown that increasing σ_x and σ_y decreases the bandwidth of the filter and vice versa. Based on empirical data, [65] set $\sigma_x = \sigma_y = 4$.

To make the enhancement faster, instead of computing the best-suited contextual filter for each pixel "on the fly," a set $\{g_{ij}(x,y) \mid i = 1 \ldots n,\ j = 1 \ldots n\}$ of filters is a prior created and stored, where n is the number of discrete orientations $\{\theta_i \mid i = 1 \ldots n\}$ and n the number of discrete frequencies $\{\{f_j \mid j = 1 \ldots n\}$. Then each pixel ($x$, y) of the image is convolved, in the spatial domain, with the filter $g_{ij}(x,y)$ such that θ_i is the discretized orientation closest to θ_{xy} and f_j is the discretized frequency closest to f_{xy}. Figure 2.2.3 shows an example of the filter set in $n_o = 8$ and $n_f = 3$ Gabor filters where $\sigma_x = \sigma_y = 4$.

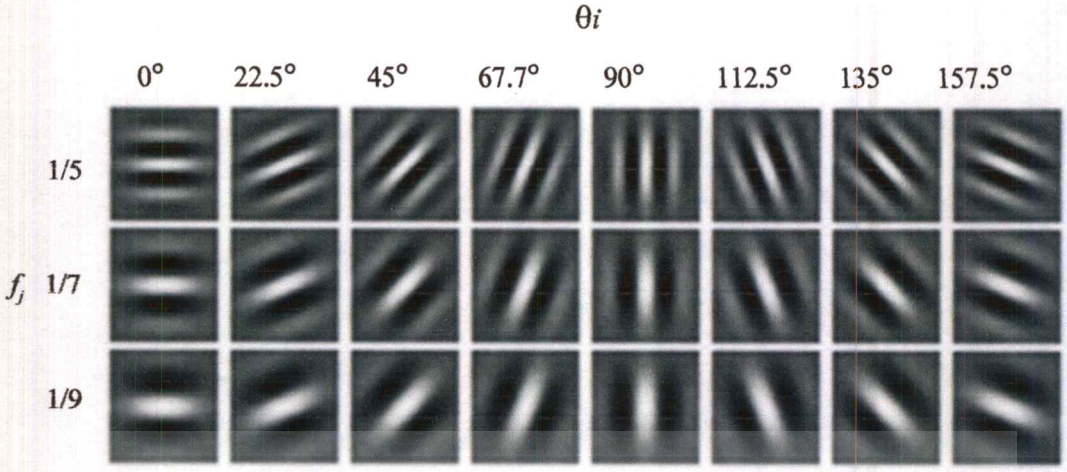


Figure 2.2.3 A graphical representation of a bank of 24

A drawback of using fixed values is that it forces the bandwidth to be constant, which does not take into account the variation that may occur in the values of the ridge frequency. For example, if a filter with a constant bandwidth is applied to a fingerprint image that exhibits significant variation in the frequency values, it could lead to non-uniform enhancement or other enhancement artifacts. Thus, rather than using fixed values, I have chosen the values of σ_x and σ_y to be a function of the ridge frequency parameter, which is defined as $\sigma_x = k_x f(x,y)$ and $\sigma_x = k_y f(x,y)$, where f is the ridge frequency image, k_x is a constant variable for σ_x, and k_y is a constant variable for σ_y. This allows a more adaptable approach to be used, as the values of σ_x and σ_y can now be specified adaptively according to the local ridge frequency of the fingerprint image. Figure 2.4.4 shows the application of Gabor-based contextual filtering on poor quality images first row (a) original and second row (b) the ridge enhanced recoverable regions are clear.

(a) Original images

(b) Ridges enhancement

Figure 2.2.4 Examples of fingerprint enhancement have applied Gabor filter (GBF).

2.3 Core point Finding

Most of the approaches proposed in the literature for singularity detection operate on the fingerprint orientation image. In the rest of this section, the main approaches are coarsely classified and a subsection is dedicated to each family of algorithms. The core point is generally recognized as the top-most point that the ridges making turns. In order to detect the fingerprint center point area, we first locate the core point corresponding to the uppermost point contained in the inner-most ridge line. There exist several techniques for core point detection. They are; for instance; Poincare index (PC), Direction of curvature (DC), and Geometry region (GR). Each holds its individual complexity and performance.

2.3.1 Poincare index technique (PC)

The Poincare one is fairly simple and suitable for both core point and delta point identifying both core point and delta point. Upon the availability of estimated orientation field $\theta(i, j)$ given above, for the pixel in the sub block centered as (i, j) we can compute the Poincare index [14, 15 16]. Let **G** be a vector field and C be a curve immersed in **G**; then the Poincaré index $P_{G,C}$ is defined as the total rotation of the vectors of **G** along C (see Figure 2.3.1).

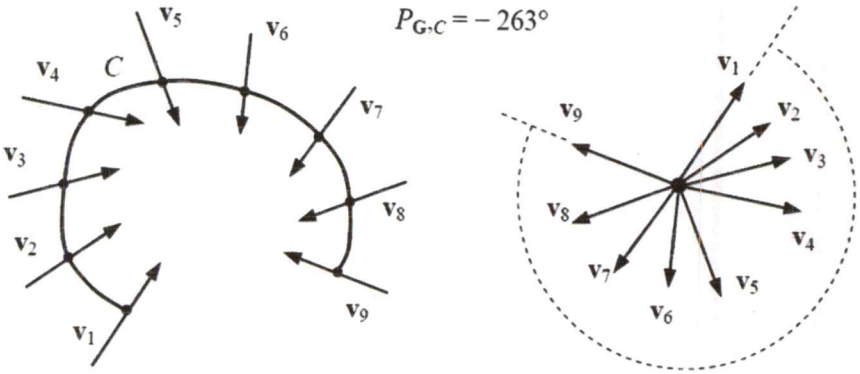


Figure 2.3.1 The Poincare index computed over a curve C immersed in a vector field G.

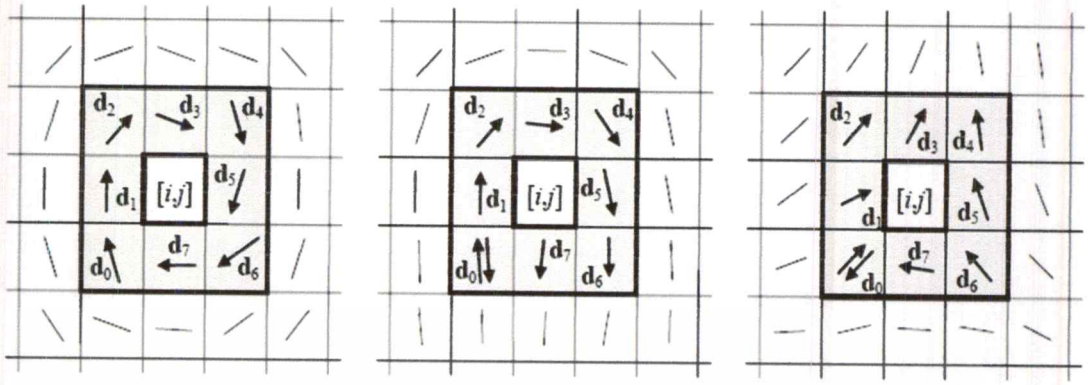
Let **G** be the discrete vector field associated with a fingerprint orientation image θ and let $[i,j]$ be the position of the element $\theta(i, j)$ in the orientation image; then the Poincaré index $P_{G,C}(i,j)$ at $[i,j]$ is computed as follows. The curve C is a closed path defined as an ordered sequence of some elements of θ, such that $[i,j]$ is an internal point.

$P_{G,C}(i, j)$ is computed by algebraically summing the orientation differences between the adjacent elements of C. Summing orientation differences requires a direction (among the two possible) to be associated at each orientation. A solution to this problem is to randomly select the direction of the first element and assign the direction closest to that of the previous element to each successive element. It is well known and can be easily shown that, on closed curves, the Poincaré index assumes only one of the discrete values: 0°, ± 180°, and ± 360°. In the case of fingerprint singularities:

$$P_{GC}(i,j) = \begin{cases} 0° & \text{if } [i,j] \text{ does not belong to any singular region} \\ 360° & \text{if } [i,j] \text{ belong to a whorl type singular region} \\ 180° & \text{if } [i,j] \text{ belong to a loop type singular region} \\ -180° & \text{if } [i,j] \text{ belong to a delta type singular region} \end{cases} \quad (2.5.2)$$

Figure 2.3.2 shows three portions of orientation image. The path defining C is the ordered sequence of the eight elements $\mathbf{d}$ (k = 0...7) surrounding $[i, j]$. The direction of the elements $\mathbf{d}$ is chosen as follows: $\mathbf{d}$ is directed upward; $\mathbf{d}$ (k = 1...7) is directed so that the absolute value of the angle between $\mathbf{d}_k$ and $\mathbf{d}_{k-1}$ is less than or equal to 90°. The Poincaré index is then computed as

$$P_{GC}(i,j) = \sum_{k=0}^{7} angle(d_k, d_{(k+1) \bmod 8}) \tag{2.5.3}$$



$P_{G,C}(i,j) = 360°$ $P_{G,C}(i,j) = 180°$ $P_{G,C}(i,j) = -180°$

Figure 2.3.2 Examples of Poincaré index computation in the 8-neighborhood of points belonging (from left to right) to a whorl, loop, and delta singularity, respectively.

Note that, for the loop and delta examples (center and right), the direction of d_0 are first chosen upward (to compute the angle between d_0 and d_1) and then successively downward (when computing the angle between d_7 and d_0).

(a) Core point detected without enhancement (b) Core point detected with enhancement

Figure 2.3.3 Examples of Poincare index technique detection (star) on the fingerprint image.

2.4 2D-Discrete Fourier transforms and Discrete Cosine Transform

Like any Fourier-related transform, Discrete Fourier Transform (DFT and discrete cosine transforms (DCT) express a function or a signal in terms of a sum of sinusoids with different

frequencies and amplitudes. Like the Discrete Fourier Transform (DFT), a DCT operates on a function at a finite number of discrete data points. The obvious distinction between a DCT and a DFT is that the former uses only cosine functions, while the latter uses both cosines and sines (in the form of complex exponentials). However, this visible difference is merely a consequence of a deeper distinction: a DCT implies different boundary conditions than the DFT or another relate transforms.

2.4.1 Block divides

For the block preparation an image is divided into individual blocks. A block consists of 16x16 pixels. Figure 2.4.1 illustrates block preparation by dividing an image into a block of 16x16 pixels.

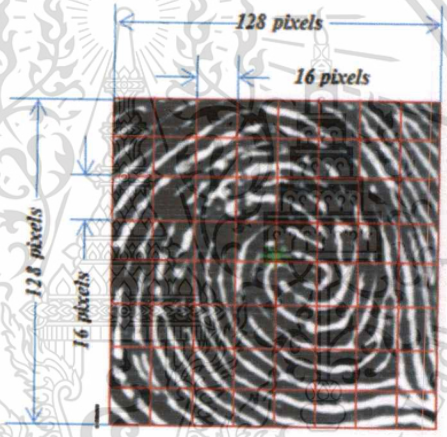


Figure 2.4.1 Fingerprint Image divided into 64 blocks each block 16 x16 pixel.

2.4.2 Discrete Fourier Transforms

The term image transform refers to a class of unitary matrices used for representing images. Images are expanded in terms of a discrete set of basis arrays called basis images [45]. Energy conservation, energy compaction, decoration is the important properties of these transforms. Image transforms like Discrete Fourier Transform (DFT) to digital image data is

well studied and extensively used for many years. The two dimensional DFT of an M x N image f (x, y) is a separable transform defined as:

$$F(u,v) = F[f(x,y)] = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} f(x,y)\exp\left\{-2\pi\left(\frac{ux}{M}+\frac{uy}{N}\right)\right\} \quad (2.6)$$

The u and v are frequency component of each dimension, and we can find a Fourier spectrum as:

And spectrum angles by $\varphi(u,v) = \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right]$ (2.6.1)

After transformation, the phase values provide little information, only magnitudes are further considered for our application.

2.4.3 Discrete CosineTransfroms

The block of 8x8 sampled values in space domain is transformed into another block of 8x8 coefficient values in the spectral frequency domain by applying the DCT, since it is easier to compress data in the frequency domain. Compression is based on the assumption that samples values in individual blocks of an image usually contain similar information (i.e. High coefficients that have low frequency) – spatial correlation.

2.4.4 Definitions

The DCT is regarded as a discrete-time version of the Fourier-cosine series. Hence, it is considered as a Fourier-related transform similar to the Discrete Fourier Transform (DFT), using only real numbers. Since DCT is real-valued, it provides a better approximation of a signal with fewer coefficients.

The DCT is a transform which transforms a signal or image from the spatial domain to the elementary frequency domain. Lower frequencies are more obvious in an image than higher frequencies an image is transferred into its frequency components and higher frequency coefficients are discarded, the amount of data needed to describe the image without sacrificing too much image quality will reduce. Thus, DCT can be computed with a Fast Fourier

Transform (FFT) like algorithm. Hence, it can be concluded that:

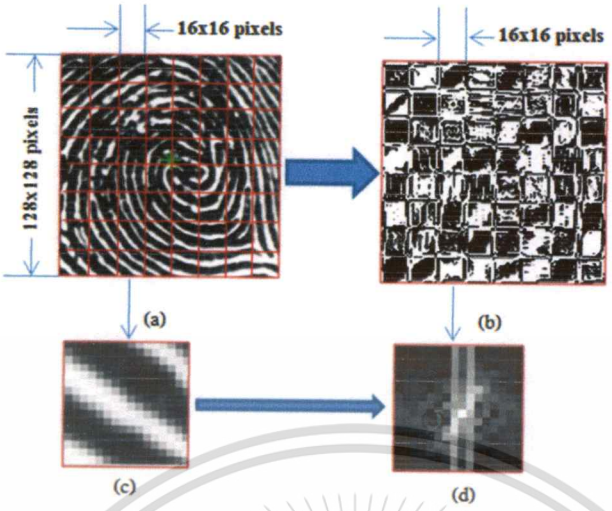


Figure 2.4.2 a) original 64 sub-images, b) 2D-DFT 64 sub-images result c) Original one sub-images, d 2D-DFT one sub-images result.

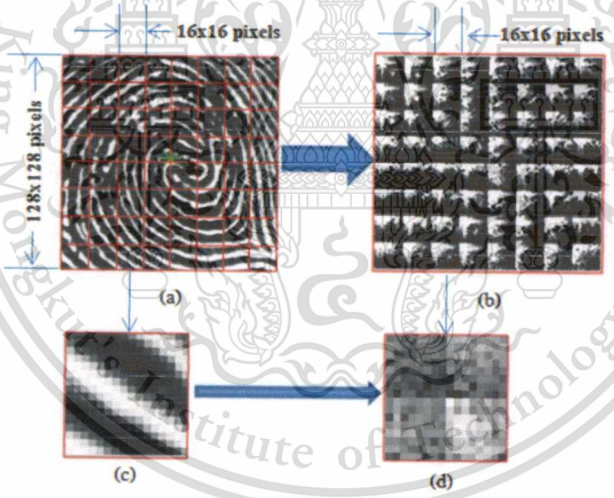


Figure 2.4.3 a) original 64 sub-images, b) 2D-DCT 64 sub-images result,c) Original one sub-images, d) 2D-DCT one sub-images result.

2.4.5 One-dimensional DCT

The discrete cosine transform is a linear invertible function F: RN > RN (where rdenotes the set of real numbers), or equivalently an $N \times N$ square matrix. Mathematically, the 1D

discrete cosine transform (1D - DCT) *X[k]* of a sequence *x[n]* of length *N* is defined as:

$$X[k] = a[k]\sum_{n=0}^{N-1} x[n]\cos\left(\frac{\pi(2n+1)k}{2N}\right), \qquad k = 0,1\ldots, N-1 \tag{2.6.2}$$

Also, the inverse 1D - DCT is defined as:

$$X[k] = a[k]\sum_{n=0}^{N-1} a[k]X[k]\cos\left(\frac{\pi(2n+1)k}{2N}\right), \qquad n = 0,1\ldots, N-1 \tag{2.6.3}$$

Where in both Equations (2.6.3) and (2.6.4), a [k] is defined as:

$$\alpha[k] = \begin{cases} \sqrt{\frac{1}{N}}, & for \quad k=0 \\ \sqrt{\frac{2}{N}}, & for \quad k=1,2,\ldots, N-1 \end{cases} \tag{2.6.4}$$

The basis sequences of the 1D - DCT are real, discrete-time sinusoids are defined by.

$$c_N[n,k] = \cos\left(\frac{\pi(2\pi+1)k}{2N}\right) \tag{2.6.5}$$

Each element of the transformed list *X[k]* in equation 2.6.1 is the inner dot product of the input list *x[n]* and a basis vector. Constant factors are chosen so the basis vectors are orthogonal and normalized. The DCT can be written as the product of a vector (the input list) and the $N \times N$ orthogonal matrix whose rows are the basis vectors.

2.4.6 Two-dimensional DCT

The two-dimensional discrete cosine transform (2D-DCT) is used for processing signals such as images. The 2D-DCT resembles the 1D-DCT transform since it is a separable linear transformation; that is if the two-dimensional transform is equivalent to a one-dimensional DCT performed along a single dimension followed by a one- dimensional DCT in the other dimension. For e.g., in a *n x m* matrix, S, the 2D -DCT is computed by applying it to each row of S and then for each column of the result.

The 2-D-DCT is similar to a Fourier transforming but uses purely real math. It has purely real transforms domain coefficients and incorporates strictly positive frequencies. The 2D-DCT is equivalent to a DFT of roughly twice the length, operating on real data with even symmetry, where in some variants the input and/or output data are shifted by half a sample. As the 2D-DCT is simpler to evaluate than the Fourier transform, it has become the transform of choice in image compression standards such as JPEG.

The 2D-DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies. It has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. The series form of the 2D discrete cosine transforms (2D-DCT) is defined as:

$$X[k_1,k_2]=\alpha[k_1]\alpha[k_2]\sum_{n=0}^{n_1-1}\sum_{n=0}^{n_2-1}x[n_1,n_2]\cos\left(\frac{\pi(2n_1+1)k_1}{2N_1}\right)\cos\left(\frac{\pi(2n_2+1)}{2N_2}\right) \quad (2.6.6)$$

$$for \quad k_1=0,1....,N-1 \quad and \quad k_2=0,1....N_2-1 \quad \text{And,}$$

$$x[n_1,n_2]=\sum_{n=0}^{n_1-1}\sum_{n=0}^{n_2-1}\alpha[k_1]\alpha[k_2]\,X[k_1k_2]\cos\left(\frac{\pi(2n_1+1)k_1}{2N_1}\right)\cos\left(\frac{\pi(2n_2+1)}{2N_2}\right) \quad (2.6.7)$$

$$for \quad n_1=0,1....,N-1 \quad and \quad n_2=0,1....N_2-1 \quad \text{With } \alpha\,[k] \text{ defined in equation} \quad (2.6.8)$$

Equation (2.6.7) is called the analytical formula or the 'forward transform', while equation (2.6.8) is called the synthesis formula or 'inverse transform'. Mathematically, the DCT is perfectly reversible and there is no loss of image definition until coefficients are quantized.

The 2D-DCT can be efficiently regarded as a set of basis functions which given a known input array size ($n \times m$) can be pre-computed and stored. The 2D basis matrices are the outer product of the 2D basis vectors. Each basis matrix can be thought of as an image and is characterized by a horizontal and vertical spatial frequency. This involves computing values for a convolution mask (8x8 window) that gets applied (sum values x pixels in the window which overlap with image apply a window across all rows/column image.

The 2D-DCT however, is partly restricted to compute to a limited size when it is used for image compression. Rather than taking the transform of the image as a whole, the DCT is applied separately to 8 x 8 blocks of the image. To compute the 2D blocked DCT, the image is not actually divided into blocks, since the 2D-DCT is separable, a partition of each row into lists of length 8 is performed, and the DCT is applied to them and the resulting lists are rejoined and then the whole image is transposed by repeating the process.

For an $N \times M$ input image, the DCT input is an 16 x 16 array of integers. This array contains each pixel's grayscale level, where the 16 bit pixels have levels from 0 to 255. When the two-dimensional blocked DCT of 8×8 blocks is computed, the coefficients are quantized, the entropy is coded and transmitted. Generally, N = 8 and the DCT formula are applied to each row and column of the block.

2.5 Literature review of fingerprint Matching

A variety of automatic fingerprint matching algorithms have been proposed in the pattern recognition literature. This chapter provides a survey of existing approaches for automatic fingerprint matching. Most of these algorithms have no difficulty in matching good quality fingerprint images, but matching low quality and partial fingerprints remains a challenging problem.

A fingerprint matching algorithm compares two given fingerprints and returns either a degree of similarity (without loss of generality, a score between 0 and 1) or a binary decision (matched/non-matched). Only a few matching algorithms operate directly on grayscale fingerprint images; most of them require that an intermediate fingerprint representation be derived through a feature extraction stage. Without loss of generality, hereafter we denote the representation of the fingerprint acquired during enrollment as the template ($\boldsymbol{T}$) and the representation of the fingerprint to be matched as the input ($\boldsymbol{I}$). In case no feature extraction is performed, the fingerprint representation coincides with the grayscale fingerprint image itself; hence, throughout this chapter, we denote both raw fingerprint images and fingerprint feature vectors (i.e., minutiae) with $\boldsymbol{T}$ and $\boldsymbol{I}$.

The fingerprint feature extraction and matching algorithms are usually quite similar for both fingerprint verification and identification problems. This is because the fingerprint identification problem (i.e., searching for an input fingerprint in a database of N fingerprints) can be implemented

as a sequential execution of N one-to-one comparisons (verifications) between pairs of fingerprints. Approaches to fingerprint matching can be coarsely classified into three families.

Correlation-based matching: two fingerprint images are superimposed and the correlation between the corresponding pixels is computed for different alignments (i.e., various displacements and rotations).

Minutiae-based matching: this is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae feature sets that result in the maximum number of minutiae pairings.

2.5.1 Correlation-based techniques

Let $\boldsymbol{T}$ and $\boldsymbol{I}$ be the two fingerprint images corresponding to the template and the input fingerprint, respectively. Then an intuitive measure of their diversity is the sum of squared differences (SSD) between the intensities of the corresponding pixels:

$$SSD(T,I) = \|T-I\|^2 = (T-I)^T(T-I) = \|T\|^2 + \|I\|^2 - 2T^T I \qquad (2.7.1)$$

Where the superscript "T" denotes the transpose of a vector. If the terms $\|\boldsymbol{T}\|^2$ and $\|\boldsymbol{I}\|^2$ are constant, the diversity between the two images is minimized when the cross-correlation (CC) between $\boldsymbol{T}$ and $\boldsymbol{I}$ is maximized:

$$CC(T,I) = T^T I \qquad (2.7.2)$$

Note that the quantity $-2 \times CC(\boldsymbol{T}, \boldsymbol{I})$ appears as the third term in the equation (2.7.1). The cross-correlation (or simply correlation) is then a measure of the image similarity. Due to the displacement and rotation that unavoidably characterize two impressions of a given finger, their similarity cannot be simply computed by superimposing $\boldsymbol{T}$ and $\boldsymbol{I}$ and applying equation (2.9.2). Let $\boldsymbol{I}^{(\Delta_x, \Delta_y, \theta)}$ represent a rotation of the input image $\boldsymbol{I}$ by an angle θ around the origin

(usually the image center) and shifted by Δx and Δy pixels in directions x and y, respectively; then the similarity between the two fingerprint images $\boldsymbol{T}$ and $\boldsymbol{I}$ can be measured as

$$S(T,I) - \max_{\Delta x,\Delta y,\theta} CC\left(T, I^{(\Delta x,\Delta y,\theta)}\right) \tag{2.7.3}$$

A direct application of equation (2.7.3) rarely leads to acceptable results (see Figure 2.5.1a) mainly due to the following problems. Figure 2.5.1 for the best alignment (e.g., that maximize correlation). In the first row, a) the two impressions are very similar and their images correlate well (the residual is very small). In the second row, b) and third row c), due to high distortion and skin condition, respectively, the residuals are high and the global correlation methods fail.

Figure 2.5.1 Each row shows two impressions of the same finger and the absolute value of their difference (residual).

As to the computational complexity of the correlation technique, smart approaches may be exploited to achieve efficient implementations.

- The correlation theorem [17] states that computing the correlation in the spatial domain (operator $\otimes$) is equivalent to performing a point-wise multiplication in the Fourier domain; in particular,

$$T \otimes I = F^{-1}\left(F^{*}(T) \times F(T)\right) \tag{2.7.4}$$

Where $F(T)$ is the Fourier transform of an image, $F^{-1}(T)$ is the inverse Fourier transform, "*" denotes the complex conjugate, and "×" denotes the point-by-point multiplication of two vectors. The result of Equation (2.7.4) is a correlation image whose value at the pixel $[x,y]$ denotes the correlation between T and I when the displacement is $\Delta x = x$ and $\Delta y = y$. However the output of Equation (2.7.4) is dependent on the image energy and the correlation peak (corresponding to the optimal registration can be small. The Symmetric Phase Only Filter (SPOF) often provides better results (equation (2.7.5):

$$T \otimes_{SPOF} I = F^{-1}\left(\frac{F^{*}(T)}{|F(T)|} \times \frac{F(I)}{|F(I)|}\right) \tag{2.7.5}$$

To reduce the effect of noise [8] suggests restricting the SPOF domain to the frequency range characterizing a fingerprint image: this can be simply dealt with through a band-pass filter in the Fourier space. Equations (2.7.4) and (2.7.5) do not take into account rotation, which has to be dealt with separately; in any case, the computational saving is very high when correlation is performed globally [18] and considerable when it is performed locally by using medium-size regions.

- Computing the maximum correlation need not necessarily be done in a sequential, exhaustive manner; multi-resolution approaches, space-searching techniques (e.g., gradient descent), and other heuristics can be adopted to reduce the number of evaluations. For example, [19], proposes to coarsely pre-align the two fingerprints based on their orientation images.
- The Fourier-Mellin transform [20] may be used instead of the Fourier transform to achieve rotation invariance in addition to translation invariance; on the other hand,

some additional steps (such as the log-polar coordinate transformation) have to be performed, that can reduce the accuracy of this solution. [21] Method computes the Fourier-Mellin descriptors locally and uses SPOF to determine the similarity between any two image portions.

- The approach proposed by [22] partitions both T and I into local regions and computes the maximum correlation (in the Fourier domain) between any pair of regions. This method suffers from "border effects" because of the partial overlapping between the different blocks, but can considerably speed up the whole matching process.

2.5.2 Minutiae-based methods

A minutiae matching is certainly the most well-known and most widely used methods for fingerprint matching, thanks to its strict analogy with the way forensic experts compare fingerprints and its acceptance as a proof of identity in the courts of law in almost all countries around the world.

a) Problem formulation

Let T and I be the representation of the template and input fingerprint, respectively. Unlike in correlation-based techniques, where the fingerprint representation coincides with the fingerprint image, here the representation is a feature vector (of variable length) whose elements are the fingerprint minutiae. Each minutia may be described by a number of attributes, including its location in the fingerprint image, orientation, type (e.g., ridge ending or ridge bifurcation), a weight based on the quality of the fingerprint image in the neighborhood of the minutia, and so on. Most common minutiae matching algorithms consider each minutia as a triplet $m = \{x,y,\theta\}$ that indicates the x, y minutia location coordinates and the minutia angle θ:

$$T = \{m_1, m_2, \cdots, m_m\}, \qquad m_i = \{x_i, y_i, \theta_i\}, \quad i = 1 \cdots m$$

$$I = \{m'_1, m'_2, \cdots, m'_n\}, \qquad m'_j = \{x'_j, y'_j, \theta'_j\}, \quad j = 1 \cdots n,$$

Where m and n denote the number of minutiae in T and I, respectively. A minutia m'_j in I and a minutia m_i in T are considered "matching," if the spatial distance (sd) between

them is smaller than a given tolerance r_0 and the direction difference (dd) between them is smaller than an angular tolerance θ_0:

$$sd\left(m'_j, m_i\right) = \sqrt{\left(x'_j - x_i\right)^2 + \left(y'_j - y_i\right)^2} \leq r_0 \tag{2.7.6}$$

$$dd\left(m'_j, m_i\right) = \min\left(\left|\theta'_j - \theta_i\right|, 360° - \left|\theta'_j - \theta_i\right|\right) \leq \theta_0 \tag{2.7.7}$$

Equation (2.7.7) takes the minimum of $\left|\theta'_j - \theta_i\right|$ and $360° - \left|\theta'_j - \theta_i\right|$ because of the circularity of angles (the difference between angles of 2° and 358° is only 4°). The *tolerance boxes* (or hyper- spheres) defined by r_0 and θ_0 are necessary to compensate for the unavoidable errors made by feature extraction algorithms and to account for the small plastic distortions that cause the minutiae positions to change.

Aligning the two fingerprints is a mandatory step in order to maximize the number of matching minutiae. Correctly aligning two fingerprints certainly requires displacement (in x and y) and rotation (θ) to be recovered and likely involves compensating for other geometrical transformations:

- The scale has to be considered when the resolution of the two fingerprints may vary (e.g., the two fingerprint images have been taken by scanners operating at different resolutions).
- Other distortion-tolerant geometrical transformations could be useful to match minutiae in case one or both of the fingerprints is affected by severe distortions. In any case, tolerating more geometric transformations beyond translation and rotation results in additional degrees of freedom to the minutiae matcher: when a matcher is designed, this issue needs to be carefully evaluated, as each degree of freedom results in a huge number of new possible alignments which significantly increases the chance of incorrectly matching two fingerprints from different fingers:

Let $map(f)$ be the function that maps a minutia m'_j (from **I**) into m''_j according to a given geometrical transformation; for example, by considering a displacement of [Δx, Δy] and a counterclockwise rotation θ around the original

$$map_{\Delta x,\Delta y,\theta}\left(m'_j=\left\{x'_j,y'_j,\theta'_j\right\}\right)=m''_j=\left\{x''_j,y''_j,\theta'_j+\theta\right\}\ ,\qquad \text{where,}$$

$$\begin{bmatrix}x''_j\\y''_j\end{bmatrix}=\begin{bmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{bmatrix}\begin{bmatrix}x'_j\\y'_j\end{bmatrix}+\begin{bmatrix}\Delta x\\\Delta y\end{bmatrix}$$

Let *mm (i)* be an indicator function that returns 1 in the case where the minutiae m''_j and m_i match according to Equations (2.7.1) and (2.7.2):

$$mm\left(m''_j,m_i\right)=\begin{cases}1 & sd\left(m''_j,m_i\right)\le r_0 \quad and \quad dd\left(m''_j,m_i\right)\le\theta_0\\0 & otherwise.\end{cases}$$

Then, the matching problem can be formulated as

$$\max_{\Delta x,\Delta y,\theta,P} imize\sum mm\left(map_{\Delta x,\Delta y,\theta}\left(m'_{P(i)}\right),m_i\right) \tag{2.7.8}$$

Where $P(i)$ is an unknown function that determines the pairing between I and T minutiae; in particular, each minutia has either exactly one mate in the other fingerprint. Figure 2.5.1 shows an example of minutiae pairing given a fingerprint alignment. To achieve the optimum pairing (according to equation (2.7.3), a slightly more complicated scheme should be adopted: in fact, in the case when a minutia of I falls within the tolerance hyper-sphere of more than one minutia of T, the optimum assignment is that which maximizes the number of mates (refer to Figure 2.5.2 for a simple example). Figure 2.5.1 minutiae of T are denoted by O, whereas I minutiae are denoted by x. Note that I minutiae are referred to as m'', because what is shown in the figure is their mapping into T coordinates. Pairing is performed according to the minimum distance. The dashed circles indicate the maximum spatial distance. The gray circles denote successfully mated minutiae; minutia m_1 of T and the minutia m''_3 of I have no mates, minutiae m_3 and m''_6 cannot be mated due to their large direction difference [23].

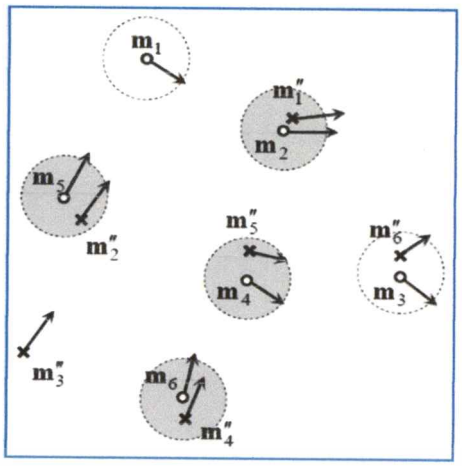


Figure 2.5.2 Minutiae of I mapped into T coordinates for a given alignment.

As shown in Figure 2.5.3 if m_1 was mated with m_2'' (the closest minutia), m_2 would remain unmated; however, pairing m_1 with m_1'' , allows m_2 to be mated with m_2'' , thus maximizing equation (2.7.3).

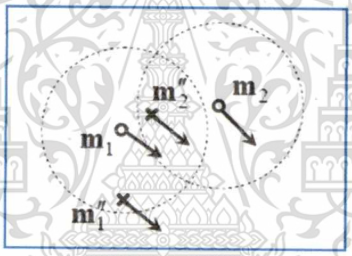


Figure 2.5.3 in this example of mated minutia.

b) Similarity score

Unlike in manual matching performed by forensic experts where the number of matching minutiae is itself the main output of the comparison, automatic matching systems must convert this number into a similarity score. This is often performed by simply normalizing the number of matching minutiae (here denoted by k) by the average number $(m + n)/2$ of minutiae in T and I:

$$score = \frac{k}{(n+m)/2} \tag{2.7.9}$$

However, further information can be exploited, especially in case of noisy images and limited overlap between T and I, to compute a more reliable score, in fact.

- Minutiae quality can be used to weight differently reliable and unreliable minutiae pairs: the contribution from a pair of reliable minutiae should be higher than that from a pair where at least one the two minutiae are of low quality [24]. The quality of a minutia (and of a minutia pair) can be defined according to the fingerprint quality in the region where the minutia lies and/or by keeping into account other local information.
- The normalization in equation (2.7.3) tends to excessively penalize fingerprint pairs with partial overlap; a more effective normalization considers the number or minutiae belonging to the intersection of the two fingerprints after the optimal alignment have been determined [25].

2.5.3 Minutiae matching with pare alignment

Embedding fingerprint alignment into the minutiae matching stage (as the methods presented in the previous section do), certainly leads to the design of robust algorithms, which are often able to operate with noisy and incomplete data. On the other hand, the computational complexity of such methods does not provide a high matching throughput (i.e., 10,000 or more matches per second), as required by AFIS or civil systems.

Storing pre-aligned templates in the database and pre-aligning the input fingerprint before the minutiae matching can be a valid solution to speed up the 1:*N* identification. In theory, if a perfect pre-alignment could be achieved, the minutiae matching could be reduced to a simple pairing. Two main approaches for pre-alignment have been investigated.

- Absolute pre-alignment: each fingerprint template is pre-aligned, independently of the others, before storing it in the database. Matching an input fingerprint *I* with a set of templates requires *I* to be independently registered just once, and the resulting aligned representation to be matched with all the templates. The most common absolute pre-alignment technique translates the fingerprint according to the position of the core point. Unfortunately, reliable detection of the core is very difficult in noisy images and in arch type patterns, and a registration error at this level is likely to result in a matching error. Absolute pre-alignment with respect to rotation is even more critical; some authors proposed using the shape of the external fingerprint silhouette (if available), the orientation of the core delta segment (if a delta exists),

the average orientation in some regions around the core or the orientations of the singularities [32].

- Relative pre-alignment: the input fingerprint *I* have to be pre-aligned with respect to each template *T* in the database; 1: *N* identification requires *N* independent pre-alignments. Relative pre-alignment may determine a significant speed up with respect to the algorithms that do not perform any pre-alignment, but cannot compete in terms of efficiency with absolute pre-alignment. However, relative pre-alignment is in general more effective (in terms of accuracy) than absolute pre-alignment, because the features of the template *T* may be used to drive the registration process. Figure 2.5.4 a) input minutiae set; b) template minutiae set; c) alignment result based on the minutiae marked with green circles; d) matching result where template minutiae and their correspondences are connected by green lines [33].

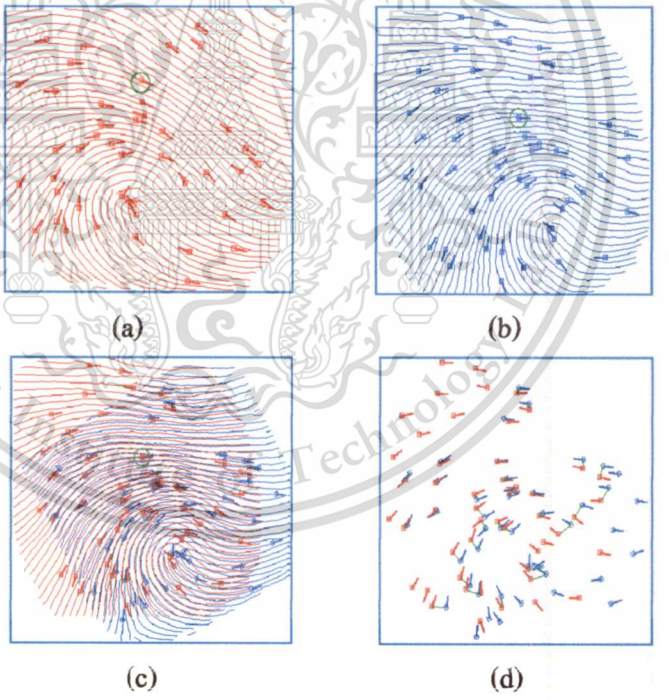


Figure 2.5.4 Results of applying the matching algorithm to an input minutiae set and a template.

2.5.4 Local Matching

The local matching approaches rely on evidence accumulated from matching local structures in neighborhoods of minutia points. These local structures are generally characterized by properties that are invariant with respect to global transformation, and therefore are suitable for matching without any a priori alignment. However, local neighborhoods do not sufficiently capture the global structural relationships thereby making false accepts very common. Thus, it is possible that local minutia structures in two non-matching fingerprints might match. Figure 2.5.4 shows an example of two false matched local structures. They are similar at the local structures but conflict with each other in global context (at very different locations with respect to the core and delta points).

To deal with this problem, the local matching algorithms use an additional console-ideation step to check whether the locally matched minutia points match at the global level or not. A large number of local matching techniques have been proposed in literature. An overview of some of the algorithms is discussed here. Jiang and Yau [34] use a local structure formed by a central minutiae and its two nearest-neighbor minutiae; the feature vector v_i associated with the minutia m_i, whose nearest neighbors are m_j and m_k is :

$$v_i = \left[d_{ij} d_{ik}, \theta_{ij}, \theta_{ik}, \phi_{ij}, \phi_{ik}, n_{ij}, n_{ik}, t_i, t_j, t_k \right]$$

Where d_{ab} is the distance between minutiae m_a and m_b, φ_{ab} is the direction difference

Figure 2.5.5 An example of two false matched local structures [36]

Between the angle θ_a of m_a and the direction of the edge connecting m_a to m_b, n_{ab} is the ridge count between m_a and m_b, and t_a is the minutia type of m_a. In all minutia pairs (m_i, m_j'), $m_i \in T$ and $m_j' \in Q$ Q weighted distance between their vectors v_{mi} and v_{mj}' is calculated. An additional consolidation step is used to enforce the result of local matching. The best matching pair (with least distance) is used for registering the two minutia sets. The feature vectors of the remaining aligned pairs are matched and a final score is computed by taking into account contributions from the first stage and consolidation stage.

Jain et al. [38] have proposed a filter bank based local texture analysis technique.The fingerprint image is tessellated into 80 cells (5 bands and 16 cells) around the core point and a feature vector representing texture information is obtained from the tessellated. The feature vector consists of an ordered enumeration of the features extracted from the local information contained in each sector. Thus the feature elements capture the local texture information and the ordered enumeration of the tesselation captures the global relationship among the local contributions. A bank of 8 Gabor filters (8 orientations and 1 scale = 1/10) is used to obtain texture information from each sector. Thus each fingerprint is represented by a 640 (80 × 8) fixed-size feature vector called the Finger Code. The generic element V(*i, j*) of the vector (i = 1..80 is the cell index, j = 1..8 is the filter index) denotes the energy revealed by the filter j in the cell i, and is computed as the average absolute deviation (AAD) from the mean of the responses of the filter j over all the pixels of the cell i. Matching two fingerprints are then performed by computing the Euclidean distance between their Finger-Codes. The disadvantage of this approach is that it uses a core point as a reference. When the core points cannot be reliably detected, or it is close to the border of the fingerprint area, the Finger Code of the input fingerprint may be incomplete or incompatible with the template. Also, finger Codes are found to be not as distinctive as minutiae. However, they carry complementary information which can be combined with minutiae to yield higher accuracy.

Chapter 3

Proposed algorithms of fingerprint matching

Fingerprint Matching is the most important stage in the fingerprint recognition process. A fingerprint matching algorithm compares two sets of features originating from two fingerprints and determines whether or not they represent the same finger. Fingerprint matching is an extremely difficult problem, mainly due to the large intra class variations that exists in different impressions of the same finger. In this chapter we have investigated 5 techniques for fingerprint matching they are: i) Fingerprint matching by using normalized cross correlation (NCC) technique, in this technique we have to measure the performance with the normalized cross correlation matching score. ii) Fingerprint matching based on minutiae technique. In this technique we measure the performed by forensic experts where the number of matching minutiae is itself the main output of the comparison, automatic matching systems must convert this number into a similarity score iii) Fingerprint Matching based on two dimensional discrete Fourier transform Features technique. This algorithm we measure the performance by correlation-based fingerprint matching. Using the value of the spectrum and the value of the line angles between the template images and test images. After via discrete Fourier transforms. iv) Fingerprints matching based on two dimensional discrete cosine transforms technique. In this algorithm we also use correlation technique for measurement the algorithm performance by using the spectrum magnitude after via discrete cosine transform (DCT), v) Fingerprint matching by using normalized cross correlation (NCC) and two dimensional discrete Fourier transform features technique in this technique we measure the algorithm performance by two steps: first NCC score and second values of the spectrum of 2D-DFT.

There are two folds in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. Details are given as follows:

3.1 Database Construction

In practice there could be a huge fingerprint pattern stored as database. To identify the case an anonymous pattern must seek its most similar to one or few database patterns. Storing those tons of patterns without losing their originality is also a problem to be solved. In our approach database construction is as shown in the figure 3.1 below.

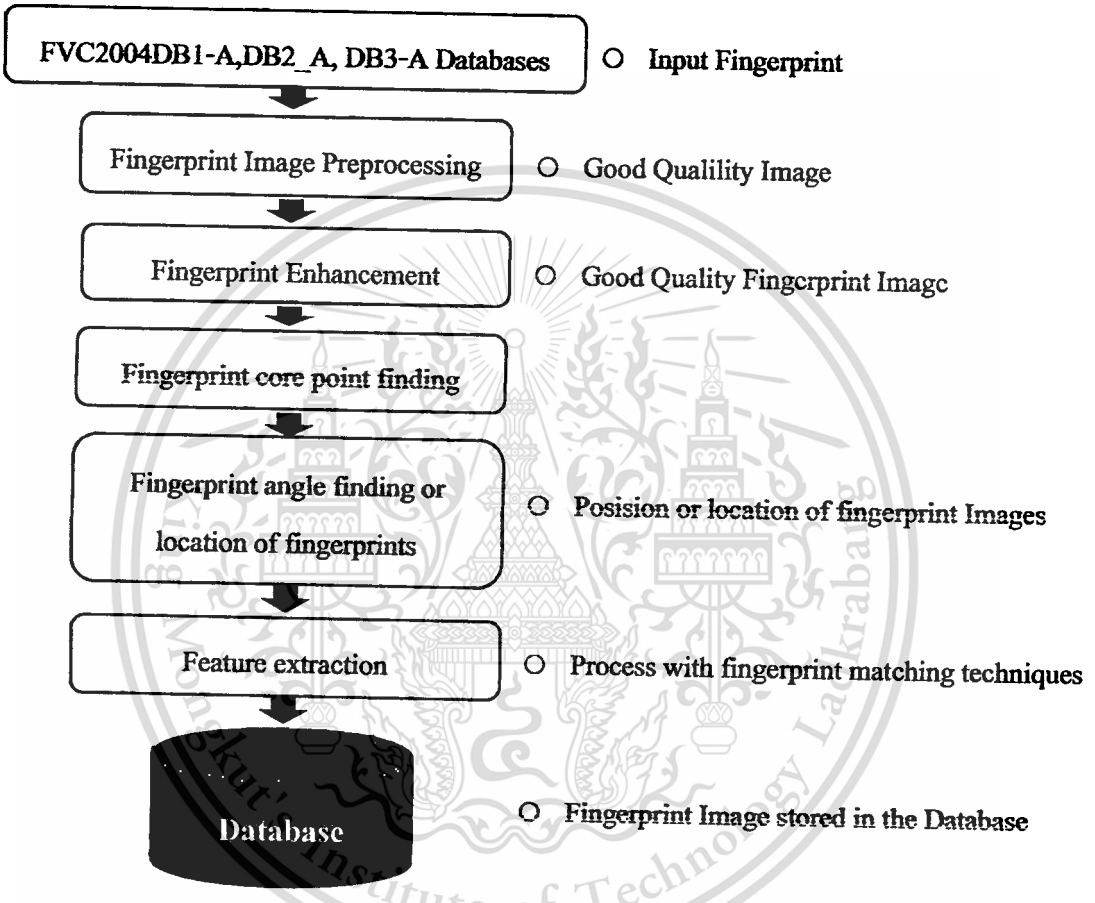


Figure 3.1 Database Construction System

In the **chapter 2** we have provided an overview of different fingerprint matching approaches. The correlation based method requires the complete image to be stored (large template sizes). The texture based methods are less accurate than minutiae based matters since most regions in the fingerprint carry low textural content. Both types of methods require accurate alignment of fingerprints. The minutia based techniques on the other hand are more accurate and they very closely resemble the manual approach as used by forensic experts. Studies [40,41] have shown that by

combining additional information in the form of texture features, level 3 features with minutia based matcher, higher accuracy can be achieved. The minutia based approaches like other approaches cannot give a high confidence match when the images are of poor quality or when there is a very small overlap i.e. very few minutia points are available for matching. Level 3 features are known to carry discriminative information and forensic examiners often make use of Level 3 features when insufficient minutia points are present. Our matching techniques have been proposed in this chapter. Figure (3.2) illustrates the architectural design of the proposed matching construction system.

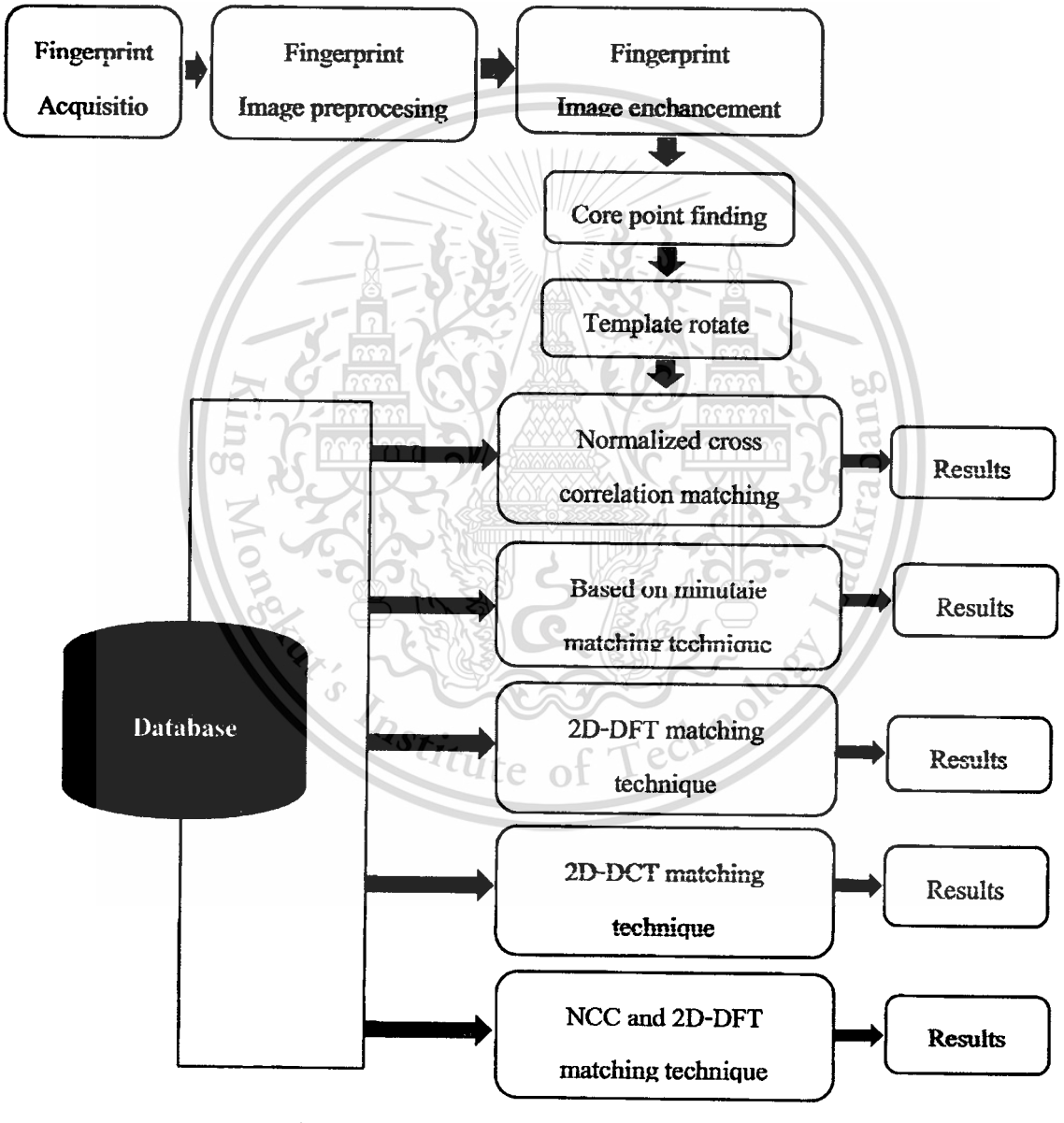


Figure 3.2 Fingerprint matching construction systems

3.2 Fingerprint matching processed

In his thesis we propose a method for fingerprint matching techniques. Those techniques i.e., i) Fingerprint matching by using" Normalized cross correlation" technique, ii) Fingerprint matching "based on minutiae" technique, iii) Fingerprint matching by using the "two dimensional discrete Fourier transforms" technique, iv) Fingerprint matching by using the" two dimensional discrete cosine transforms" technique, v) Fingerprint by using normalized cross correlation and two dimensional discrete Fourier transform technique. Those machine techniques procedure followings by the steps below:

3.2.1 Fingerprint enhancement using Gabor filter

Before the matching process we have to enhancement make the fingerprint images clear. In our method used fingerprint enhancement methods based on the Gabor filter have been widely used to facilitate various fingerprint applications such as fingerprint matching and fingerprint classification. Gabor filters are bandpass filters that have both frequency-selective and orientation-selective properties, which mean the filters can be effectively tuned to specific frequencies and orientation values. One useful characteristic of fingerprints is that they are known to have well defined local ridge orientation and ridge frequency. Therefore, the enhanced algorithm takes advantage of this regularity of spatial structure by applying Gabor filters that are tuned to match the local ridge orientation and frequency. And those details have proposed in chapter 2.

3.2.2 Core point Finding

Most of the approaches proposed in the literature for singularity detection operate on the fingerprint orientation image. In the rest of this section, the main approaches are coarsely classified and a subsection is dedicated to each family of algorithms. The core point is generally recognized as the top - most point that the ridges making turns. In order to detect the fingerprint center point area, we first locate the core point corresponding to the uppermost point contained in the inner-most ridge lines. There exist several techniques for core point

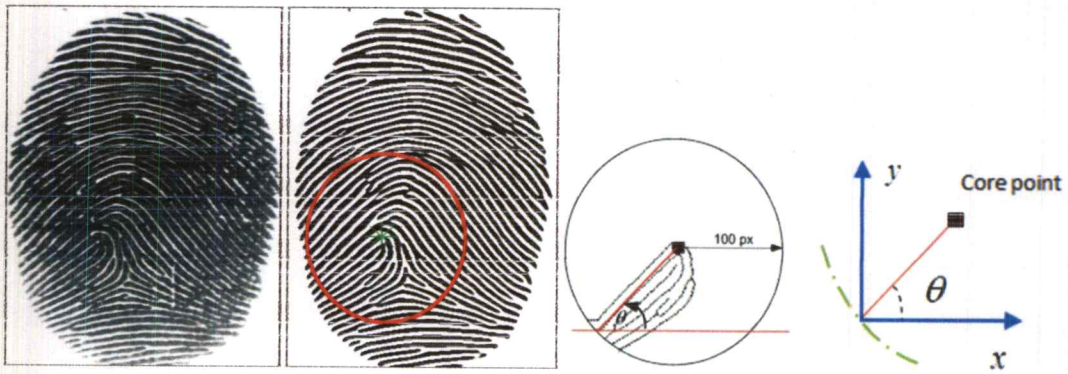
detection. The performance of the filter is also measured by the success in the core point (singular point) detection using Poincare technique. A result of singularities detected by the Poincare technique method is shown in Figure 3.2.1 a) Good quality fingerprint and b) poor quality fingerprint (stars highlight the false singularities) or low-quality fingerprints is difficult and the Point care method may lead to the detection of false singularities. However, this method is simple and widely used.

a) Core point Good quality b) Core point poor quality

Figure 3.2.1 Examples of Poincare index technique detection (star) on the fingerprint image.

3.2.3. Angle Finding

In our fingerprint matching algorithm before matching process the template image must be rotated before segmentation or transformation. Obtained with the core point we can find an images angel the first we define the circle of interest of which the radius of 100 pixels and fine the core point is taken as a center of this circle after these draw a box of 15x15 pixels around the core point and the lines connected between the box and the circumstance of the circle are considered for angle measurement and then average values were taken.

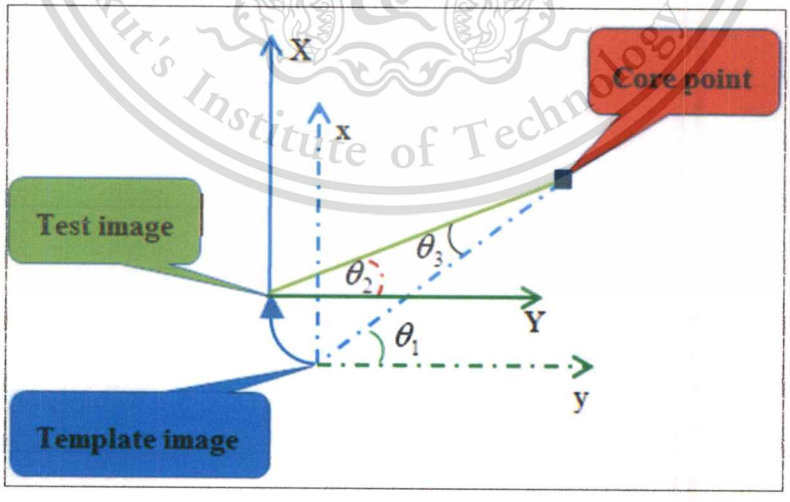


(a) (b) (c)

Figure 3.2.2 (a) Original image , (b) Define the circle of interest of which the radius of100 pixel. The core point is taken as a center, (c) The angle measurement

3.2.4 Template Rotation

To overcome the rotation problem, the raw image must be rotated before segmentation or transformation. Obtained with the core point we can find a different angle between the two images. That enables us to rotate the sampled image to the same orientation as that of the referenced non-rotate image [49]. If given θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled), then θ_3 is the angle differences between those two images. We then have to rotate the template image by (θ_3) degree, ($\theta_3 = \theta_1 - \theta_2$). Shown in the Fig. 3.2.3, below.



Figur3.2.3 The template rotating

3.3 Proposed fingerprint matching techniques

In our proposed we have investigated 5 techniques for fingerprint matching algorithm, are: i) Fingerprint matching by using normalized cross correlation (NCC), ii) Fingerprint matching based on minutiae technique, iii) Fingerprint Matching based on two dimensional discrete Fourier transform Features techniques, iv) Fingerprints matching based on two dimensional discrete cosine transforms techniques and v) Fingerprint matching by using normalized cross correlation (NCC) and two dimensional discrete Fourier transform technique. And those algorithms are proposed in the next step below.

3.3.1 Fingerprint matching by using the normalized cross correlation technique

Although it is well known that cross correlation can be efficiently implemented in the transform domain, the normalized form of cross correlation preferred for feature matching applications does not have a simple frequency domain expression. Normalized cross correlation has been computed in the spatial domain for this reason.

The correlation between two signals (cross-correlation) is a standard approach to feature detection [41,42] as well as a component of more sophisticated techniques [43]. Textbook presentations of correlation describe the convolution theorem and the attendant possibility of efficiently computing correlation in the frequency domain using the fast Fourier transform. Unfortunately the normalized form of correlation (correlation-coefficient) preferred in template matching does not have a correspondingly simple and efficient frequency domain expression. For this reason normalized cross correlation has been computed in the spatial domain [44].

In this technique the main purpose of using this procedure is to evaluate the coarse matching of two patterns, for best matching result; size and orientation of the detail image are assumed to be the same. Generally, a correlation method is a technique which can show how strongly pairs of variables are related. The result indexed by the correlation coefficient value of which -1.0 to +1.0. The close range of +1, the more closely one variable is related to the other. The correlation between two signals (cross-correlation) is a standard approach to find out how the two signals are related. It has shown its best applications in pattern recognition and

cryptanalysis. Of its kinds, normalized cross correlation (NCC) has also been used extensively in machine vision for industrial inspection including defect detection in complicated images.

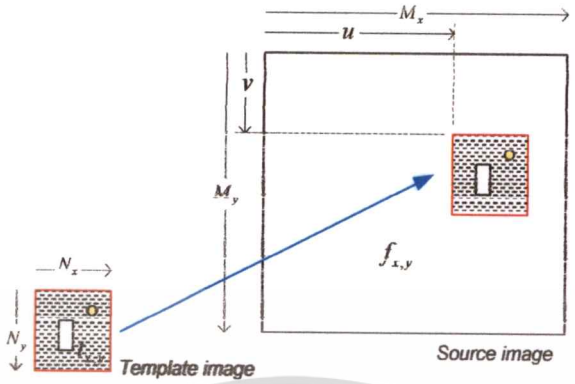


Figure 3.3.1 Matching of template t into the source image f

Shown in Fig. (1.1) f Let $f(x,y)$ is a test image (source image) of size $M_x \times M_y$ at the point $(x,y), x \in \{0,.....M_x - 1\}, y \in \{0,.....M_y - 1\}$. And t be a template image, of the size $N_x \times N_y$. We want to seek any similarity of the template t to any portion of the test image f . In this particular case, the image size t is smaller or equal to f a simple method for measuring similarity or mismatch performed by taking the absolute difference between template image t and given the test image f over a specific region.

If we take the sum of difference square between template t and give image f over an region offset by u and v in each dimension, then we can get:

$$d^2_{f,t}(u,v) = \sum_{x,y} \left[f(x,y) \quad t(x \quad u, y \quad v) \right]^2 \tag{3.1}$$

The above equation (3.1) can be expanded to,

$$d^2_{f,t}(u,v) = \sum_{x,y} \begin{bmatrix} f^2(x,y) - 2f(x,y)t(x-u,y-v) \\ +t^2(x-u,y-v) \end{bmatrix} \tag{3.2}$$

The term $\sum_{x,y} \left[t^2(x-u,y-v) \right]$ is fixed for a given template image. Likewise, the term

$\sum_{x,y}\left[f^2(x,y)\right]$ Is also approximated to be fixed. Then the cross correlation expression given in qe(3.3) will give the degree of similarity. $c(u,v)=\sum_{x,y}\left[f(x,y)t(x-u,y-v)\right]$ Direct implementation of (3.3) leads to a problem that image intensity may vary from region to region. The obtained result is not consistent. To avoid such a problem, both means and variances are taken into account. A common way to calculate the position (u_{pos},v_{pos}) of the pattern in the image f is to evaluate the normalized cross correlation value γ at each point (u,v) for f and the template t, which has been shifted by u step index direction and by v steps in the y direction Equation (3.3) gives a basic definition for the normalized cross correlation coefficient. (NCC).

$$\gamma(u,v)=\frac{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]\left[t(x-u,y-v)-\bar{t}\right]}{\sqrt{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]^2\sum_{x,y}\left[t(x-u,y-v)-\bar{t}\right]^2}} \tag{3.3}$$

In (3.3) $\bar{f}_{u,v}$ denotes the mean value of $f(x,y)$ within the area of the template $\bar{t}$ which is calculated by .

$$\bar{f}_{u,v}=\frac{1}{N_xN_y}\sum_{x=u}^{u+N_x-1}\sum_{y=v}^{v+N_y}f(x,y). \tag{3.4}$$

With similar notation $\bar{t}$ is the mean value of the template t. The denominator in (3.3) is the variance of the zero mean image function $f(x,y)-\bar{f}_{u,v}$ and the shifted zero mean template function $t(x-u,y-v)-\bar{t}$. Due to this normalization $\gamma(u,v)$ is independent of changes in brightness or contrast of the image, which are related to the mean value and the standard deviation.

$$\bar{t}_{u,v}=\frac{1}{N_xN_y}\sum_{x=u}^{u+N_x-1}\sum_{y=v}^{v+N_y}f(x,y). \tag{3.5}$$

In practice to avoid excessive computation, fast and approximated techniques are used to compute [45].

3.3.1.1 Matching Procedure

There are two folds in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. Details are given as follows:

*A. **Database Construction***

In practice there could be a huge fingerprint pattern stored as database. To identify the case, an anonymous pattern must seek its most similar to one or few database patterns. Storing those tons of patterns without losing their originality is also a problem to be solved. In our approach database construction is as follows:

- The raw image is enhanced with Gabor filtering.
- The core point of the enhanced imaged is located using point care technique.
- Fingerprint orientation is determined.

In determining the pattern orientation we firstly did image binarization and thinning. Around the core point, the circle of interest with the radius of 100 pixels is drawn. An area of 15x15 pixels around the core point is assumed as a core point. Average angles of ridge line between this box to the circumference is considered to be the orientation of the pattern. There could be some other directional filters, a Gabor filter one can be used nicely with reasonable computational cost. Likewise there are also some other methods, i.e. Maximum curvature and geometric region that can be alternatively used in determining the location of the core point.

B. Matching Steps

The specimens (test images) are then compared to the template (database) using the following steps:

- Use the given above procedure to determine the core point and pattern orientation.
- To the aligned core point, the template image is rotated by the amount of degrees difference between the two images.
- Two images are then cropped into the size of 128x128 pixels (a core point is at the center).

- Each image is then divided into 4 sub-image; 64x64 pixels.
- The corresponding sub-images are then matched with NCC template matching. Each region's matching score are summed up. Image with scores above the set value (threshold) can pass this coarse matching. And by varying the NCC matching score as FAR and FRR are observed, it is found that the score around 0.5 is ideal.

In the figure 3.3.2 shown NCC matching the template and the test images.

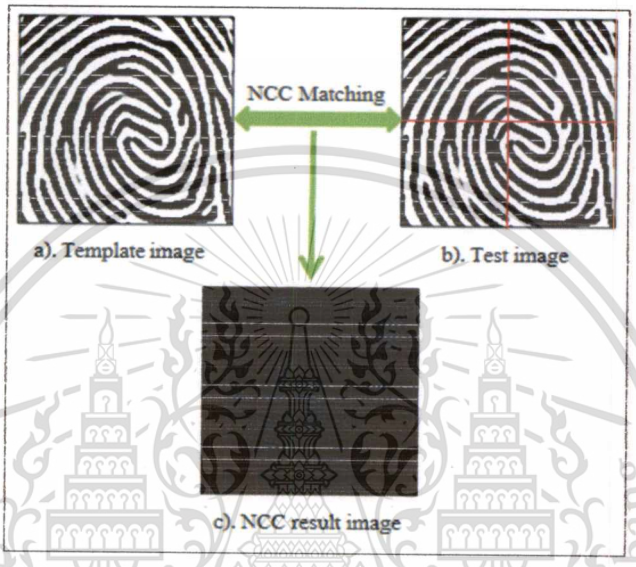


Figure 3.3.2 Example NCC matcher The Template a) and test image b) are the same figure

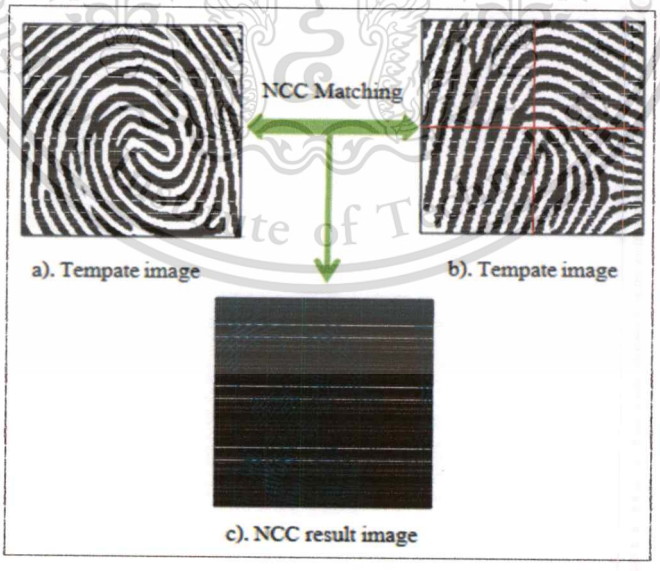


Figure 3.2.3 Example NCC matcher the Template a) and test image b) are differences figure

3.3.2 Fingerprint Matching based on Minutiae Technique

A minutia matching is certainly the most well-known and most widely used methods for fingerprint matching, thanks to its strict analogy with the way forensic experts compare fingerprints and its acceptance as a proof of identity in the courts of law in almost all countries around the world. In this algorithm the minutiae feature extraction Since during scanning the fingerprint it may have been translated and/or oriented, the extracted features must be independent of these operations. In our method the features are extracted somehow that are independent of these operations. Features are extracted based on the reference point and reference orientation. Candidate images are fed into the binarization and minutiae extraction. The minutiae extraction offers us the type of minutiae (bifurcate or end point) as well as the corresponding distance (from the core point) and the angle, i.e. distance from the core point and leverage angle, $g(r,\theta)$. Minutiae-based matching: this is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae feature sets that result in the maximum number of minutiae pairings. And the score is counted once the criteria are met, i.e. $r \pm 3$ pixel and $\theta \pm \frac{\pi}{12}$ radians. In the figure 3.2.4 shown minutiae point .

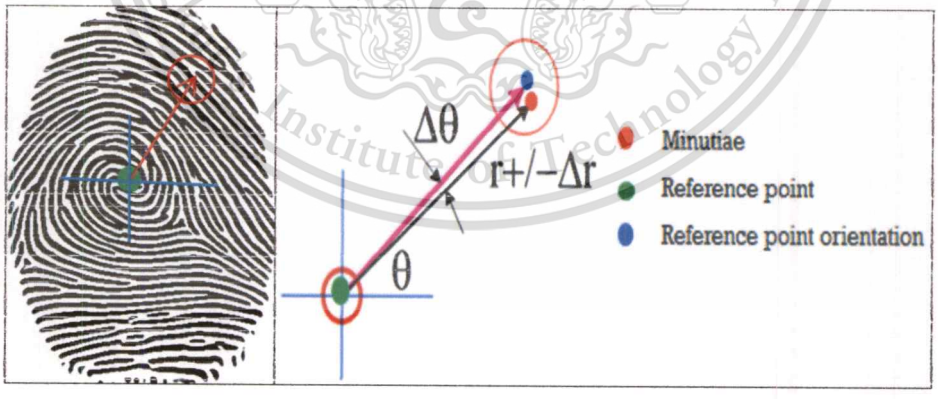
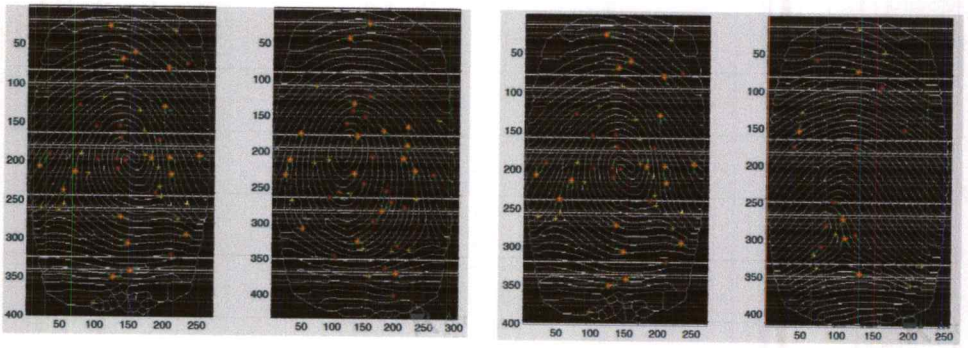


Figure 3.3.4 Minutiae, Reference and orientation point



(a) (b)

Figure 3.3.5 Shown minutiae point a) The Template and the test image are the same figure. b) The Template and the test image are deference image.

3.3.3 Fingerprint Matching based on 2D-Discrete Fourier Transform Features

The DFT/FFT is excellent for convolution, and useful for frequency-domain analysis of sampled analog signals. For good image compression, we would like energy compaction; a good transform will result in "Fourier coefficients" that are mostly near zero; we can discard or coarsely quantize the small coefficients, and use most of the bits to represent the larger coefficient. Image transforms like Discrete Fourier Transform (DFT) to digital image data is well studied and extensively used for many years.

In this technique the main purpose of using this procedure is fine of two patterns the term image transform refers to a class of unitary matrices used for representing images. Images are expanded in terms of a discrete set of basis arrays called basis images [46]. The fingerprint matching techniques by using the 2D -DFT features. During the procedure,

- Fingerprint enhancement using Gabor filter
- Core point finding
- Angle finding
- Template Rotation

We cropped the template and the test images from the size of 480x640 pixels into 128x128 pixels, and then divide the image into 64 sub-images. Each sub-image (a tile) holds the size of 16x16 pixels.

Each tile is transformed, and its spectrums are obtained. The achieved spectrums are then compared between those of a test tile and those of a template tile. A commonly known FVC- 2004 (DB1-A, DB2-A, DB3-A) database has been used in our investigation. The two dimensional DFT of an $M \times N$ image f (x, y) is a separable transform defined as:

$$F(u,v) = F[f(x,y)] = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} f(x,y)\exp\left\{-2\pi\left(\frac{ux}{M}+\frac{uy}{N}\right)\right\} \tag{3.6}$$

The u and v are frequency component of each dimension, and we can find a Fourier spectrum as:

And spectrum angles by $\varphi(u,v) - \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right]$ (3.7)

After transformation, the phase values provide little information, only magnitudes are further considered for our application. The two dimensional Fourier transforms when we rotate image they have a similar spectrum when the image opposite way, for example. Fig. 3.2.5 Below.

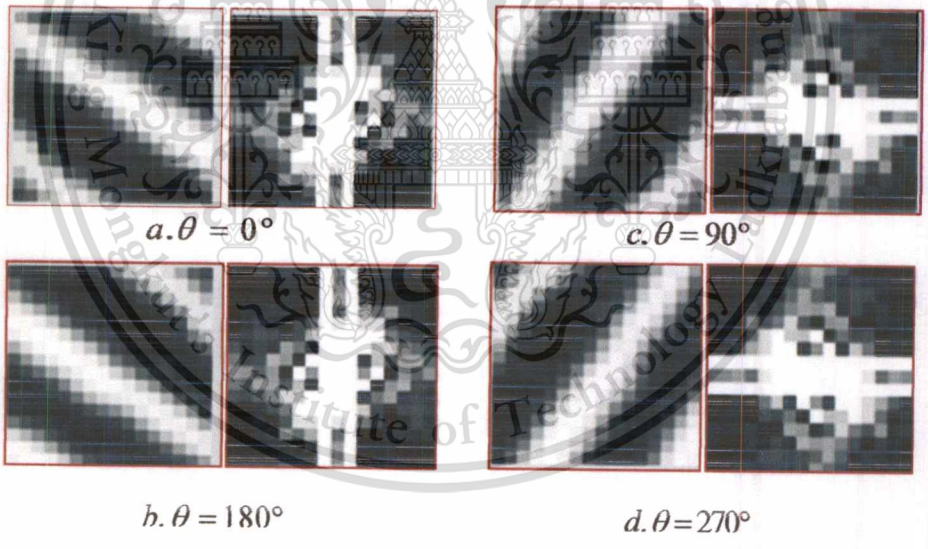


Fig. 3.3.6 The similar spectrum when sub_image opposite way

Form Fig. 3.2.5 We can see the picture a and b have a similar spectrum when image $a = 0^o$ and image $b = 180^o$, and picture c and d have similar when image $c = 90^o$ and image, $d = 270^o$. From this feature the whorl one holds rather high percent of FAR when compared to others pattern. This is because the line of the whorl pattern at the core point have similar.

If the DFT is applied to the real data, the result is also real. The DFT tends to concentrate information, making it useful for image compression applications. We have also considered the transformed information as a feature for fingerprint matching. The cropped 128 ×128 pixel image is further divided into 64 sub-images of each with the dimension of 16 ×16 pixels. Both DFT is applied to each sub-image. The resulted transformed images are illustrated below.

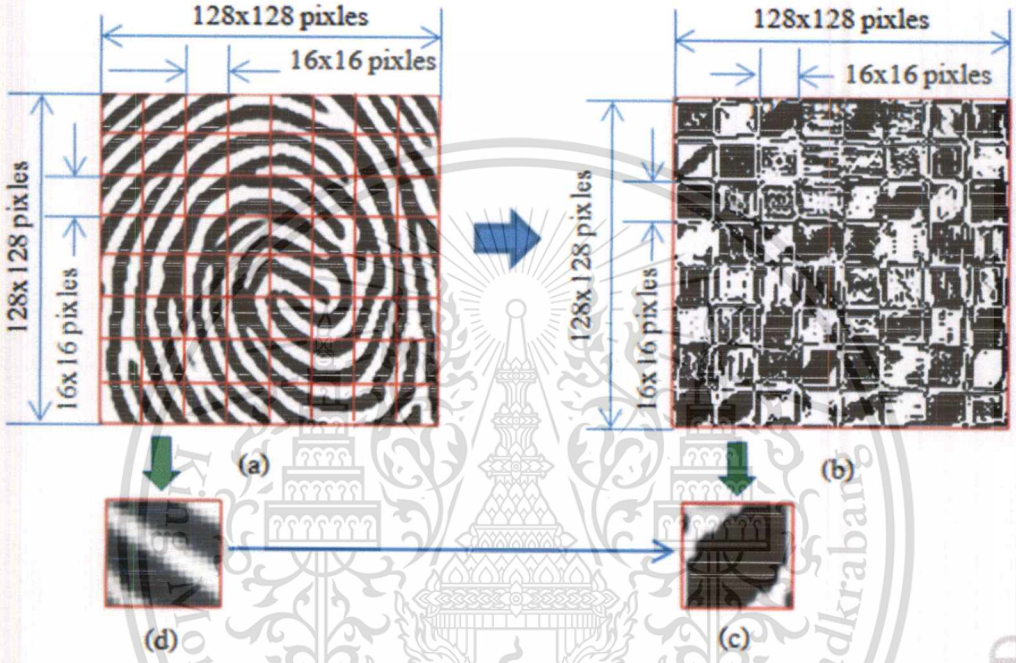


Figure 3.3.7 (a) Fingerprint image cropped to size 128×128 pixels and divided into 64-sub image and each sub-image with size 16×16 pixels. (b) 64 sub-image is 2D Discrete Fourier transforms. (d) One sub-image with size 16×16 pixels. (c) Spectrum of one sub-image transform.

The feature of a sub-image is in fact defined alternatively in its DFT domain. To make a justification whether the sub-image of the test image is actually the same with its corresponding of the template sub-image. At this stage, to examine their similarity, we are focusing to the cross correlation.

For the image "A" with the dimension $M_a \times N_a$ and the image "B" with the dimensions $M_b \times N_b$, the equation for the two-dimensional discrete cross-correlation can be given by:

$$r(i,j) = \sum_{m=0}^{M_a-1} \sum_{n=0}^{N_a-1} A(m,n)B(m+i,n+j) \tag{3.8}$$

Where $0 \le i < M_a + M_b - 1$ and $0 \le j < N_a + N_b - 1$. It should be noted that the resulted image is with the dimensions of twice larger compared to the original images. We also do not want to use all available value. In addition, the resulted minimum peak can be affected by the brightness level of the original images. Instead, we just need the maximum value that the brightness levels have been taken into account. Fortunately, a normalized cross correlation operation given by the equation (3.9), below can offer what we need.

$$r = \frac{\sum_m \sum_n \left(A_{mn} - \bar{A}\right)\left(B_{mn} - \bar{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{mn} - \bar{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{mn} - \bar{B}\right)^2\right)}} \tag{3.9}$$

The score given by 2 most similar sub-images can be close to +1, whilst that of the different images is very low. The average matching score can then be easily calculated based on the score of each sub-image matching. The highest average score implies the most similarity of those two cropped images.

$$S_{Avg} = \frac{1}{64} \sum_{i=1}^{64} r_i \tag{3.10}$$

The value the similarity average of spectrum between the template image and test images between 0.75 to 1.

Making the transformation to the image is in fact trying to look into the image in the different point of view. In the transformed domain, the spectrum feature can define well the uniqueness of the fingerprint that is hard to be of served in the spatial domain. However, under this assumption, the orientation as well as the resolution of the images must be the same. The resolution can be controlled in the acquiring process. Although the orientation of the finger can be controlled during the scanning process, the exact orientation of the acquired fingerprint is still not ensured. To overcome the rotation problem, the raw image must be rotated before segmentation or transformation. Obtained with the core point we can find a different angle between the two images. That enables us to rotate the

sampled image to the same orientation as that of the referenced non-rotate image [12,30]. After finding the raw image angle or image position. If given θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled), then θ_3 is the angle differences between those two images. We then have to rotate the template image by (θ_3) degree, ($\theta_3 = \theta_1 - \theta_2$). Shown in the Fig.3.3.8, (c) below.

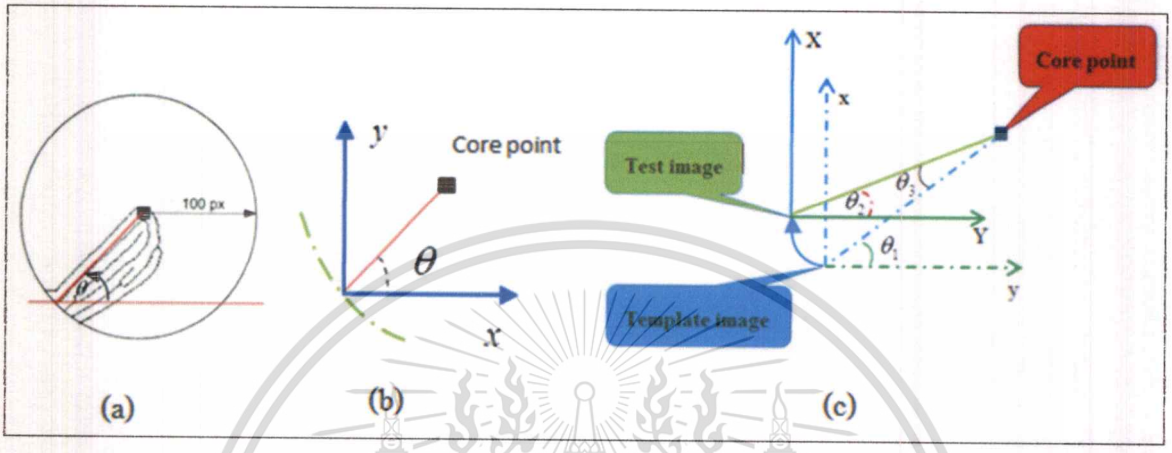


Fig 3.3.8 (a) And (b) Image angle or image position ($\theta = 63.76^{\circ}$), (c) Angle of the template rotated

From the (a) finding the image angles or image position the first defines the circle of interest of which the radius of 100 pixels. And the core point is taken as a center of this circle. And then draw a box of 15x15 pixels around the core point. And draw a line connected between the box and the circumstance of the circle are considered for angle measurement. Average values were taken.

For a normal scanned fingerprint image, the core point has generally appeared at the center of the image. With such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a reference core point the 2D-Discrete Fourier transform is applied to 64 sub-image of 16x16 pixels.

According to the symmetry properties of the DFT, some left side and right side image can offer the very similar spectrum values. That can lead to the wrong justification. To avoid the ambiguous, the line angle must be computed and store for further use. We find the value of the line angle from 64sub-image and then find Average value from 64-sub-image. And we compare the similarity of two images by subtraction the average value of the template image and the average value of the test image.

3.3.4 Fingerprint Matching Using the 2D- discrete cosine transform

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG. (The Joint Photographic Experts Group). The discrete cosine transform (DCT) is closely related to the discrete Fourier transform. It is a separable linear transformation; that is, the two-dimensional transform is equivalent to a one-dimensional DCT performed along a single dimension followed by a one-dimensional DCT in the other dimension. With the dimension of $M \times N$, the definition of the type-II two-dimensional DCT of an input image A and output image B can written as shown in Eq. (3.11). Here m,n and p,q are indexed along each dimension of A and B respectively.

$$B(p,q) = C_p C_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A(m,n) \cos\left\{\frac{p\pi}{2N}(2m+1)\right\} \left\{\cos\frac{q\pi}{2M}(2n+1)\right\} \tag{3.11}$$

Where

$$C_p = \begin{cases} \frac{1}{\sqrt{M}}, & for \quad p = 0 \\ \sqrt{\frac{2}{M}}, & for \quad 1 \le p \le M-1 \end{cases}$$

And likewise C_q.

If the DCT is applied to the real data, the result is also real. The DCT tends to concentrate Information, making it useful for image compression applications. We have also considered the transformed information as a feature for fingerprint matching. The cropped 128×128 pixel image is

further divided into 64 sub-images of each with the dimension of 16×16 pixels. Both DCT is applied to each sub-image. The resulted transformed images are illustrated below.

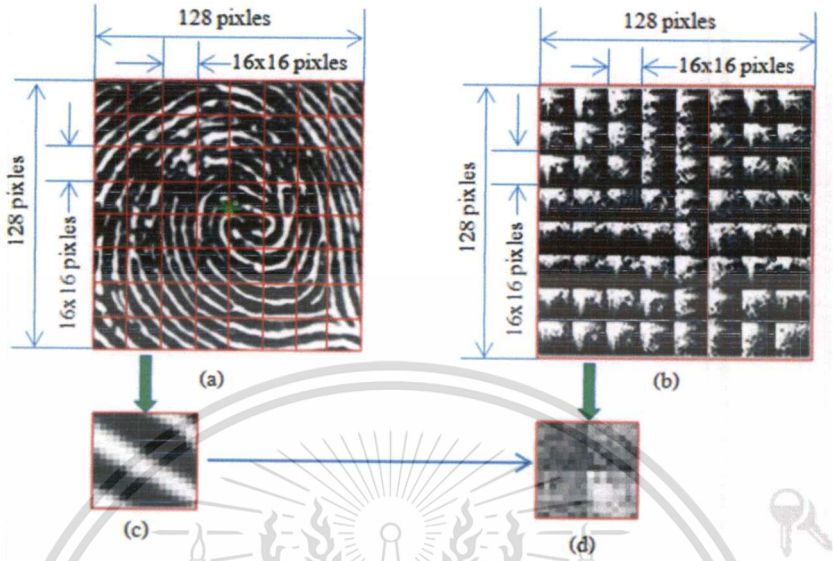


Figure 3.3.9 (a) Fingerprint image cropped to size 128×128 pixels and divided into 64-sub image and each sub-image with size 16×16 pixels. (b) 64 sub-image is 2D Discrete Fourier transforms. (d) One sub-image with size 16×16 pixels. (c) Spectrum of one sub-image transform.

The feature of a sub-image is in fact defined alternatively in its DCT domain. To make a justification whether the sub-image of the test image is actually the same with its corresponding of the template sub-image. At this stage, to examine their similarity, we are focusing to the cross correlation.

For the image "*A*" with the dimension $M_a \times N_a$ and the image "*B*" with the dimensions $M_b \times N_b$, the equation for the two-dimensional discrete cross-correlation can be given by:

$$r(i,j) = \sum_{m=0}^{M_a-1} \sum_{n=0}^{N_a-1} A(m,n)B(m+i,n+j) \tag{3.12}$$

Where $0 \le i < M_a + M_b - 1$ and $0 \le j < N_a + N_b - 1$. It should be noted that the resulted image is with the dimensions of twice larger compared to the original images. We also do not want to use all available value. In addition, the resulted minimum peak can be affected by the brightness level of the original images. Instead, we just need the maximum value that the brightness levels have been taken

into account. Fortunately, a normalized cross correlation operation given by the equation (3.13), below can offer what we need.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \tag{3.13}$$

The score given by 2 most similar sub-images can be close to +1, whilst that of the different images is very low. The average matching score can then be easily calculated based on the score of each sub-image matching. The highest average score implies the most similarity of those two cropped images.

$$S_{Avg} - \frac{1}{64}\sum_{i=1}^{64} r_i \tag{3.14}$$

The transformation to the image is in fact trying to look into the image in the different point of view. In the transformed domain, the spectrum feature can define well the uniqueness of the fingerprint that is hard to be of served in the spatial domain. However, under this assumption, the orientation as well as the resolution of the images must be the same. The resolution can be controlled in the acquiring process. Although the orientation of the finger can be controlled during the scanning process, the exact orientation of the acquired fingerprint is still not ensured. To overcome the rotation problem, the raw image must be rotated before segmentation or transformation. Obtained with the core point we can find a different angle between the two images. That enables us to rotate the sampled image to the same orientation as that of the referenced non-rotate image [12,30]. We can find the raw image angle or image position by step 3 to step 5 in database construction. If given θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled) image, then θ_3 is the angle differences between those two images. We then have to rotate the template image by θ_3 degree, ($\theta_3 = \theta_2 - \theta_1$). For a normal scanned fingerprint image, the core point has generally appeared at the center of the image with such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a

reference core point the 2D discrete cosine transforms is applied to 64 sub-image of 16x16 pixels. And the matching details are given as follows:

A. Database construction

Fingerprint pattern stored as database. To identify the case an anonymous pattern must seek its most similar to one or few database patterns. In our approach database construction is as follows.

- The raw image is enhanced with Gabor filtering
- Mark the core point of the enhanced imaged using point care technique
- Define the circle of interest of which the radius of 100 pixels. The core point is taken as a center of this circle.
- Draw a box of 15x15 pixels around the core point.
- The lines connected between the box and the circumstance of the circle are considered for angle measurement. Average values were taken.
- Determine the main ridge angle (respective to the vertical line). The obtained angle is stored in the database together with the image name.
- Images are cropped to the size 128x128 pixels (a core point is at the center). The 128x128 pixel image is divided into 64 sub-images, each is with the size of 16x16 pixels.
- Each sub-image is transformed via a 2D-DCT
- Determine the value of the spectrum components. There are 256 components for each sub-image. For the DCT transformation, spectrum magnitude is stored.
- The location where it is in the 8x8 sub-image grid, together with its spectrum values are additionally stored. This is how the database is formed.

B. Matching steps

The specimens (test) are then compared to the test images (template) using the following steps.

- Image occurring.

- Enhancement and core point determination. This is the same as step 1 to step 5 in database construction.
- Determine the angle of this test (respect to the vertical line) image. Compute the different angle between the template image and the test image. Rotate the test image by the degree of the angle difference.
- Images are cropped to the size 128x128 pixels (a core point is at the center). This 128x128 pixel image is then also divided into 64 sub-images, each of with 16x16 pixels in size
- Perform both 2D-DCT to the sub-image
- Find the spectrum values (256 values). And matching the value of the spectrum, via normalized cross correlation. The matching score is obtained
- Average matching score of those 64 sub-images can tell us how similar those 2 images.and the score similar the hod more than 0.75

According to the symmetry properties of the DCT, some left side and right side image can offer the very similar spectrum values. That can lead to the wrong justification. To avoid the ambiguous, the line angle must be computed and store for further use. We find the value of the line angle from 64 sub-image and then find Average value from 64-sub-image. And we compare the similarity of two images by subtraction the average value of the template image and the average value of the test image.

3.3.5 Fingerprint Matching Using NCC and 2D-DFT

In this technique we have proposed a fingerprint matching using Normalized cross correlation (NCC) and two dimensional Discrete Fourier transform (2D-DFT). In this method to measure the performance of the algorithm have to test two step NCC step and second step we used high score or who past the first step to process with 2D-DFT again. The algorithm detail has proposed in the 3.3.1 for NCC and 3.3.2 for 2D-DFT. Moreover, this method doesn't sensitive to rotational effect. The proposed technique is, however, based on the availability of core point. The technique fails if the core point cannot be located or incorrectly located. The matching is performed based on the NCC score and two dimensional discrete Fourier transforms magnitude, matching of the pattern around core point. Using this matching, we can improve the percent of FAR and FRR better when we

compare with other techniques. Images under tested are those obtained in FVC-2004 (DB1-A). There are 16 templates (4 groups of 4 patterns each). We have included 3 images come from the same individual each image has difference position or a different angle, in our experiment.

3.4. Pros and cons matching techniques.

In our proposed fingerprint matching we have two types of matching, first Image domain matching and second Geometric domain matching. In image domain matching consists of spectrum matching and correlation matching, and in the Geometric domain matching consist of detail feature of minutiae. And the detail shown in the table 3.4 below.

TABLE 3.4 THE PROS AND CONS OF DOMAIN MATCHING

1. Image Domain Matching	Pros	Cons
Spectrum matching	- No need to find an exact reference point - Matching faster	- Computational resource consuming
Correlation Matching	- No need to find an exact reference point	- Computational resource consuming - Take long time for matching
2. Geometric Domain Matching	Pros	Cons
Detail feature of minutiae (distance, type, orientation)	- Quite a reliable result Needless computational resource	- Require good reference point

Chapter 4

Experiment and results

4.1 Preprocessing and Post Process

All the methods and algorithms described in this dissertation were implemented using MATLAB R2010 a V7.1 on the Laptop, Microsoft Windows HP Intel Core™ i5. The experiments were performed on a Centrino 2.16 GHz with 4GB of RAM, 500GB of HD. When testing the performance of the matching algorithm, the computational time was differences measures for each matching technique.

This chapter describes the various experiments conducted and discusses the obtained results. The proposed approach has been evaluated on three databases.

4.2 Databases

The experimental results section is to show the results of each stage in the matching algorithm. We used the downloaded a fingerprint database from three databases. FVC 2004DB1-A Database, FVC2004DB2-A Database, and FVC4004 DB3_A Database. They are explained in detail below.

- The first database FVC 2004DB1-A, consists of 100 different fingers with 8 impressions per finger resulting in 800 images and each image with the size 480×640 pixels. And scanned with an optical scanner (Cross Match verifier 300) at 500 dpi
- The second database FVC2004DB2-A, consists of 100 different fingers with 8 impressions per finger resulting in 800 images and each image with the size and 328×364 pixels. The fingerprint samples from FVC2004DB1-A databases, is scanned with an optical scanner (Cross Match verifier 300) at 500 dpi. The sample images from this database are shown in Figure 4.2.1 and 4.2 .2
- The third FVC2004DB3-A Database: this database consists of 100 different fingers with 8 impressions per finger resulting in 800 images and each image with the size and 300×480 pixels. The fingerprint is scanned with a thermal sweeping sensor (Finger chip FCD4B14CB by Atmel) at 512 dpi. The sample images from this database are shown in Figure 4.2.1 below.

4.2.1 FVC2004DB1-A Databases

Figure 4.2.1 Sample images from, FVC2004DB1-A Database with the size 480×640 pixels.

4.2.2 FVC2004DB2-A Databases

Figure 4.2.2 Sample images from, FVC2004DB2-A Database with the size and 328×364 pixels.

4.2.3 FVC2004DB3-A Database

The FVC 2004DB3-A database is known to be difficult because of the perturbations which were deliberately introduced during database collection.The sample images from this database are shown in the Figure 4.2.3 below.

Figure 4.2.3 Sample images from FVC2004DB3-A Database

4.3 Performance evaluations

Each sample in a Database is matched against the remaining samples of the same finger to compute the False Rejection Rate (FRR). The FRR is the fraction of genuine fingerprints which are rejected and is calculated as follows.

$$FRR = \frac{false\_rejected\_numeber}{Total\_matching\_number} \times 100\%$$

The FAR is the fraction of impostor fingerprints which are accepted and is calculated as follows.

$$FAR = \frac{false\_acecpted\_numeber}{Total\_matching\_number} \times 100\%$$

4.3.1 EXPERMENT 1

In this experiment proposed an alternative method for fingerprint matching by using Normalized cross correlation followed by minutiae matching has been proposed. The first step can be considered as a coarse matching whilst the second is a fine matching. To speed up the matching process, the images are cropped to the size of 128×128 pixels and core point is assumed to be the center of this square. With FVC2004-DB1A database. Matching algorithm detailed in previous sections, we have set up 16 template images (16 individuals) from 4 group patterns (4 images for each pattern). Those patterns are whorl, left loop, right loop, and Tent. 100 images including templates are primarily selected as test images. We have repeated the testing for 10 times. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 database DB1-A set has been employed in this experiment. The Flowchart of the proposed matching algorithm. Shown in the fig 4.3.1 below

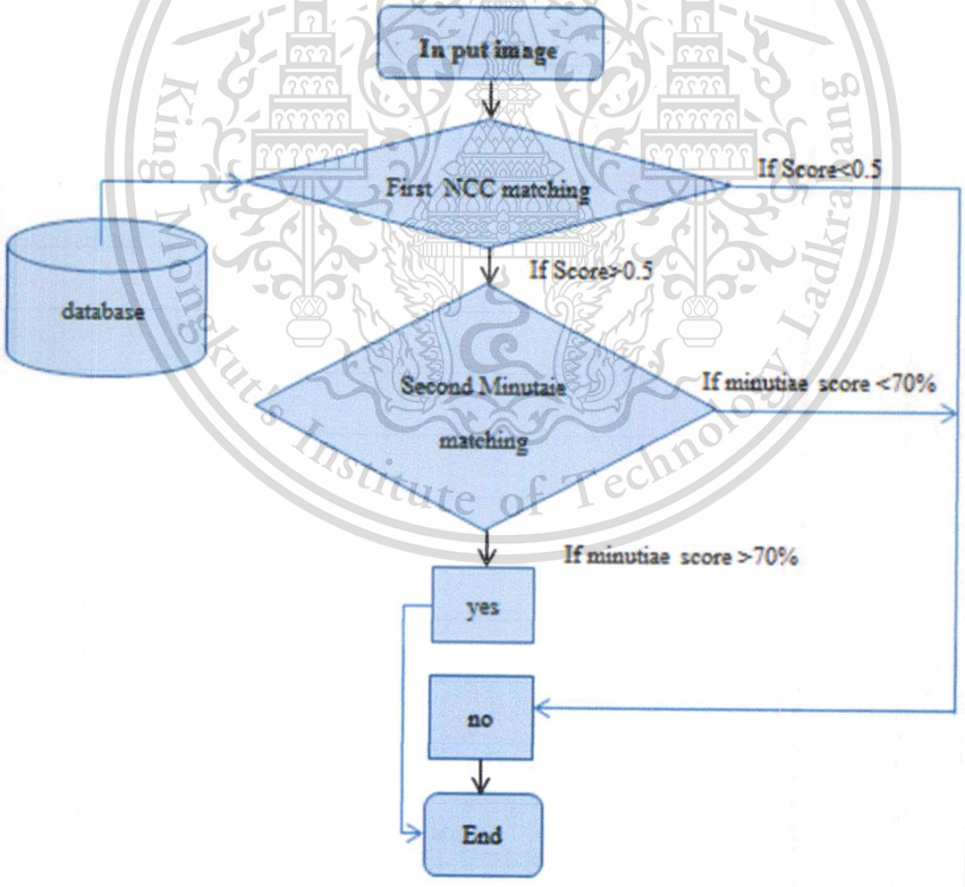
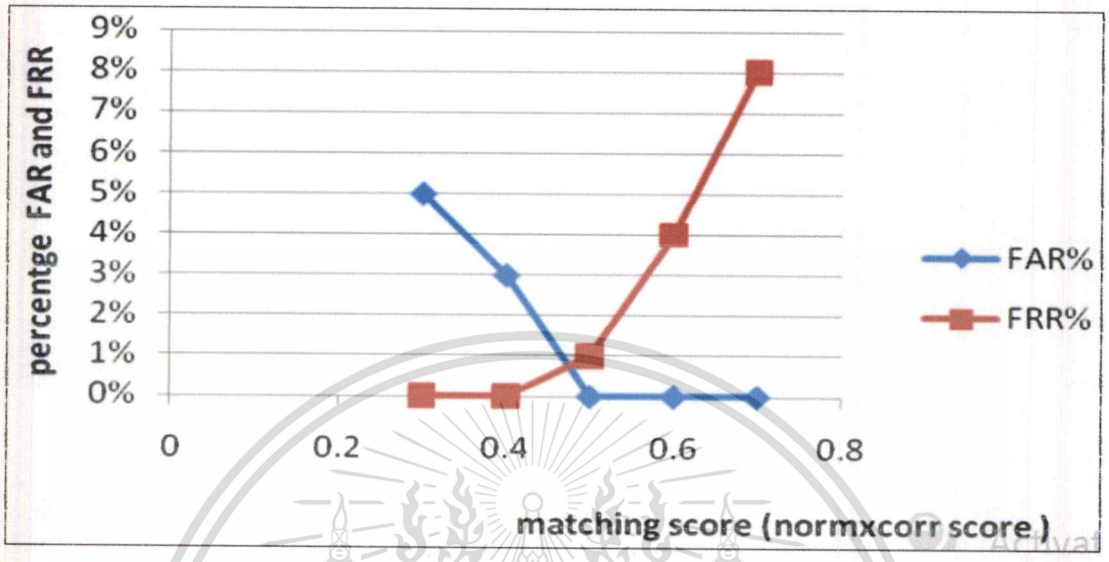


Figure 4.3.1 The Flowchart of the proposed matching algorithm

By varying the NCC Matching score as FAR and FRR are observed, it is found that the score around 0.5 is ideal. This can be clearly noticed from the graph shown in Fig. 4.3.2. Too high score can help fault acceptance rate but destroying the fault rejection rate



Figuer4.3.2 Matching scores versus FAR and FRR

Although we have rotated the image before any other processing, the average angle obtained in orientation finding cannot be so accurate. We have investigated this by varying the constrain angle in the minutiae matching step. The (minutiae) candidates are considered if they hold the angle between ±9°, ±12°, ±15°, and ±18°. As shown in Table 4.3, the machine still offers desirable result provided that we have kept the tolerance of 15 degrees or less. When the angle grows larger, the nearby minutiae are the main cause of the failure

TABLE 4.3 CONSTRAIN ANGLES USED IN THE MINUTIAE MATCHING

Test	Error. Matching Score $\geq$ 0.5 and $r \pm 3$		
	Constraint angle	***% FAR***	***% FRR***
1	$\frac{\pi}{20} = 9^\circ$	0	0
2	$\frac{\pi}{15} = 12^\circ$	0	0
3	$\frac{\pi}{12} = 15^\circ$	0	0
4	$\frac{\pi}{10} = 18^\circ$	4	0

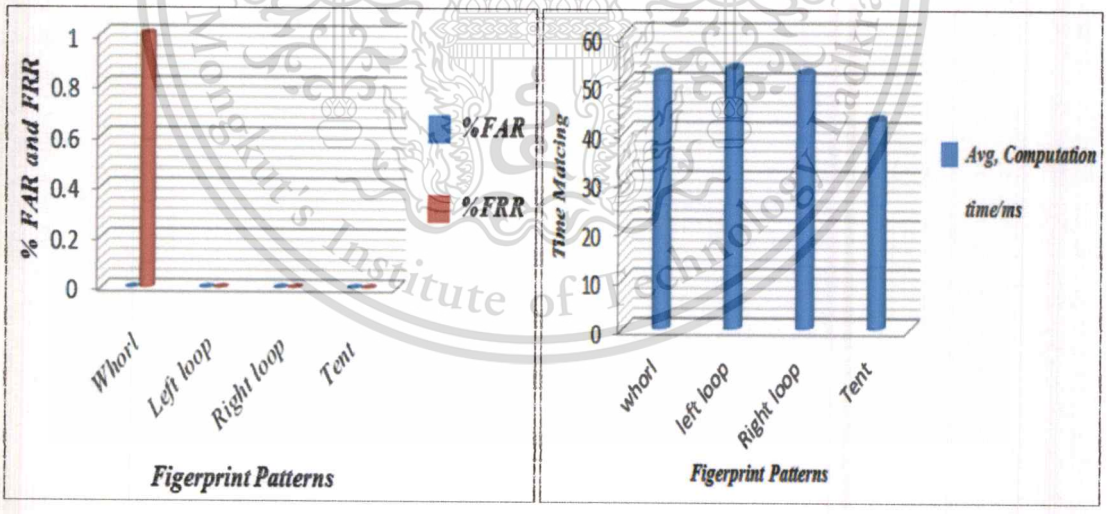
For each investigated pattern, we found that the whole pattern is sensitive to be a fault rejection one. This can be noted in Table 4.3.1 below. However we need few more investigations to check whether the case is strongly concerned with the pattern or it just because of the image quality.

TABLE 4.3.1. MATCHING RESULTS VERSUS FINGERPRINT PATTERN

Pattern	**Number of Templates**	**Number of test images**	Error. Matching Score ≥ 0.5, $\theta=\frac{\pi}{12}$, and $r \pm 3$		
			Avg. Computation Time (ms)	***% FAR***	***% FRR***
Whorl	4	22	0.527	0	1
Left loop	4	35	0.529	0	0
Right Loop	4	22	0.52	0	0
Tent	4	18	0.42	0	0
Avg	16	100	0.492	0	1

Intel i5, 2.1 GHz, 4 GB RAM

From table 4.3.1 we can see the matching results in the Figure 4.3.3 a, and b, below.



(a) (b)

Figuer4.3.3 (a) Percentage of FAR and FRR (b) Average computation Time machine

The purpose of a fingerprint matching technique is to improve the percentage of false accept rate (FAR) and false reject rate (FRR). From these experimental results, we can improve the performance when fingerprint images have A high efficiency of the scanner applied to the input images and the test images, and the proposed technique is based on the availability of core point. The technique fails if the core point cannot be located or incorrectly located and the fingerprint images have low quality . The first matching is performed based on the NCC score matching of the pattern around core point. Only few candidates are again matched based on the observed minutiae (i.e., bifurcate and end points with a particular range of pre-defined angle). Using this 2-step matching, we can improve the FAR and FRR. Images under tested are those obtained in FVC-2004 (DB-1A). There are 16 templates (4 groups of 4 patterns each). We have used 1,000 specimens (100 patterns for 10 times) in our experiment. From the results in the table 4.3.1 and figure 4.3.3, we have obtained 0% FAR and 1% FRR. And the whorl pattern has high percentages when we compare with another pattern is because the fingerprint image have a low quality and the core point cannot be determined precisely.

4.3.2. EXPERMENT 2

In this experiment we proposed an alternative method for fingerprint matching by using Two dimensional discrete Fourier transform features. And we are testing three databases: i,e: FVC 2004DB1-A, FVC2004DB2-A, and FVC2004DB3-A databases. To test in this experiment. And the flowchart of the matching algorithm shown in the Fig. 4.3.4 below.

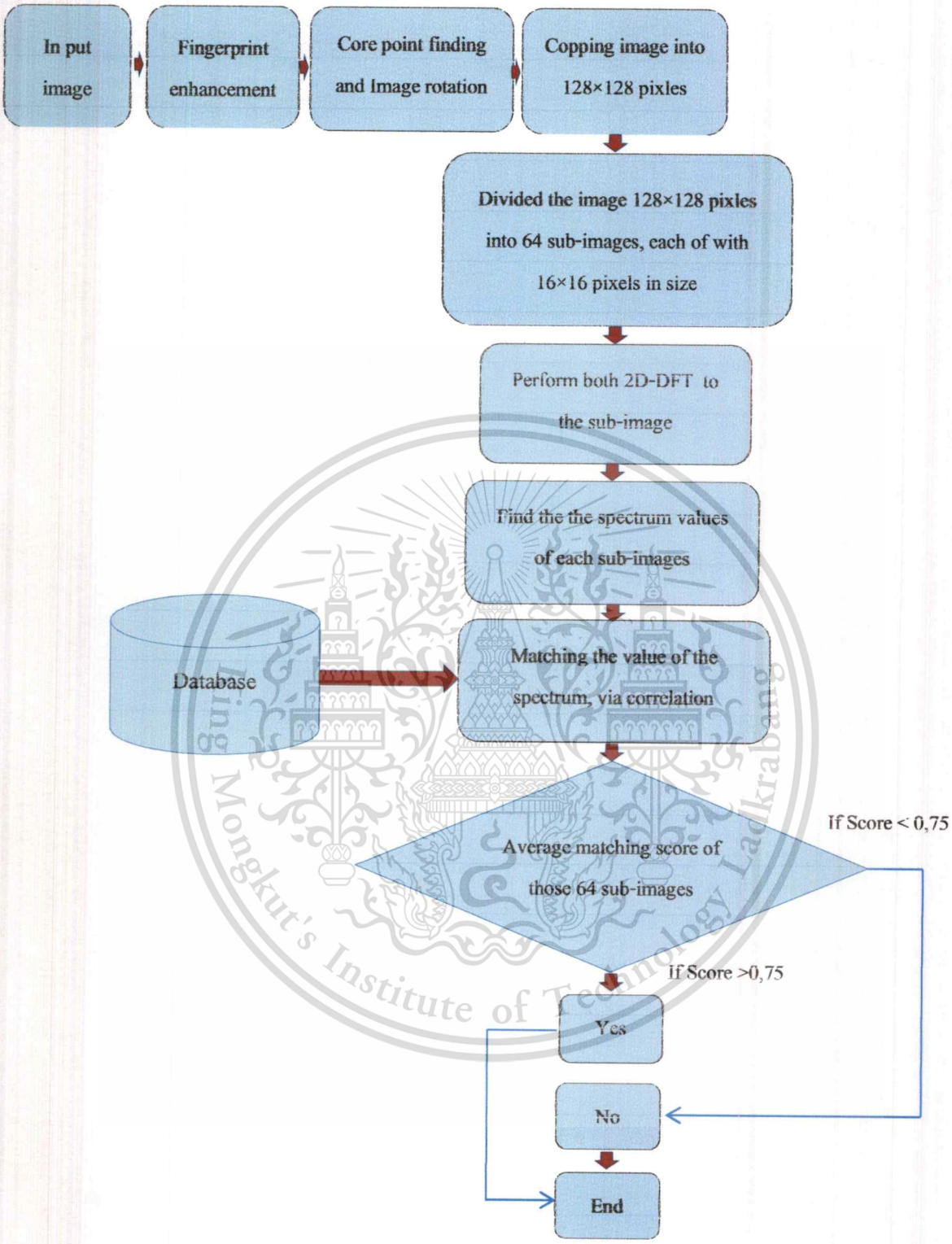


Figure 4.3.4 2D-DFT matching algorithm flowchart

In 2D-DFT and 2D-DCT Matching score as FAR and FRR are observed, it is found that the score around 0.75 is ideal. This can be clearly noticed from the values shown in the Figure 4.3.5. Too high score can help fault acceptance rate but destroying the fault rejection rate.

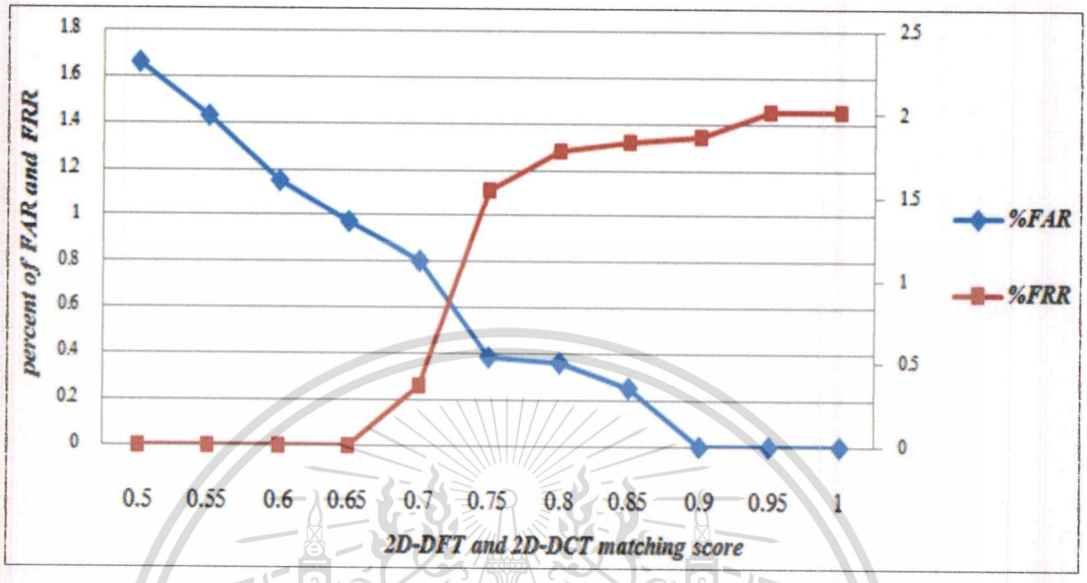


Figure 4.3.5 Constrain score used in the 2D-DFT and the 2D-DCT matching

From the Figure 4.3.5 the matching results shown in the experiments below.

4.3.2.1 FVC 2004-DB1-A Matching Results

In this experiment we have set up 16 template images from 4 group patterns (4 images for each pattern). Those patterns are 22 of whorls, 35 of left loops, 22 of right loops, and 18 of the tents. As such we have 97 individuals including test images and one individual. There are in fact 3 images come from the same image, each image is difference angle or difference position. All of images in the database to test images 291 images. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 DB1-A database set has been employed in this experiment. The result in Table 4.3.2.1 below.

TABLE 4.3.2.1. FVC 2004-DB1-A MATCHING RESULTS

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75 , *line angles* $\pm 0.5^{o}$		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	66	0.62	0.336	1.56
Left loop	4	105	0.39	0.57	1.27
Right Loop	4	66	0.67	0.63	1.34
Tent	4	54	0.72	0	2.02
Avg%	16	291	0.58	0.384	1.54

Intel i5, 2.1 GHz, 4 GB RAM

4.3.2.2 FVC 2004-DB2-A Matching Results

In this experiment we have set up 16 template images from 4 group patterns (4 images for each pattern). Those patterns are 34 of whorls, 24 of left loop, 32 of right loop, and 10 of the tents. As such we have 100 individuals including test images and one individual. There are in fact 3 images come from the same image, each image is difference angle or difference position. All of images in the database to test images 300 images. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 DB2-A database set has been employed in this experiment. The result in table 4.3.2.2 below.

TABLE 4.3.2.2 FVC 2004-DB2-A MATCHING RESULTS

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75 , *line angles* $\pm 0.5^{o}$		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	102	0.21	1	1.33
Left loop	4	72	0.213	0.66	1
Right Loop	4	96	0.217	0	1.33
Tent	4	30	0.276	0	1.66
Avg%	16	300	0.216	0.415	1.33

Intel i5, 2.1 GHz, 4 GB RAM

4.3.2.3 FVC 2004-DB3-A Matching Results

In this experiment we have set up 16 template images from 4 group patterns (4 images for each pattern). Those patterns are 32 of whorls, 24 of left loops, 27 of right loops, and 16 of the tents. As such we have 100 individuals including test images and one individual. There are in fact 3 images come from the same image, each image is difference angle or difference position. All of images in the database to test images 300 images. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 DB3-A database set has been employed in this experiment. The result in table 4.3.2.3 below

TABLE 4.3.2.3 FVC 2004-DB3-A MATCHING RESULTS

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75 , *line angles* ± 0.5°		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	96	0.249	0.66	1.33
Left loop	4	75	0.242	0.33	1.66
Right Loop	4	81	0.253	1.66	1.66
Tent	4	48	0.247	0.33	2
Avg%	16	300	0.247	0.745	1.6625

Intel i5, 2.1 GHz, 4 GB RAM

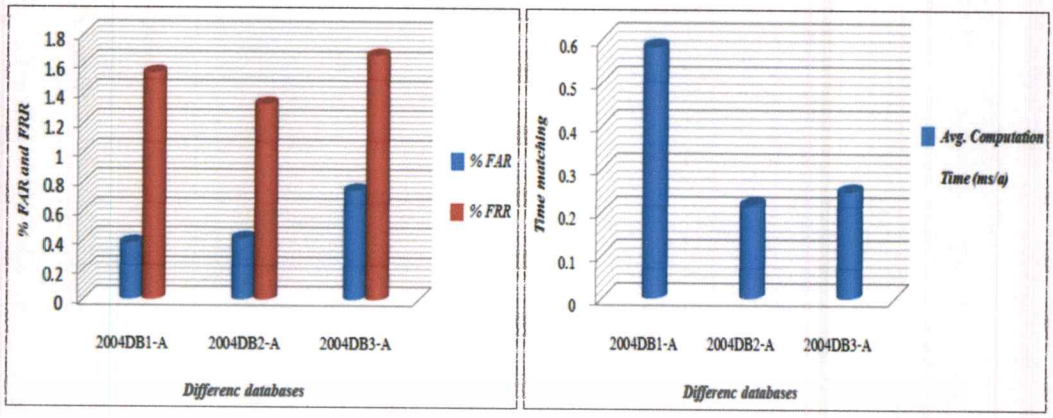
In the Table 4.3.2.4 we compare the performance of three databases. The performance result is shown in the Table 4.3.2.4 below.

TABLE 4.3.2.4. COMPARE THE PERFORMANCE RESULTS FROM DIFFERENCES DATABASE

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75 , *line angles* $\pm 0.5^o$		
			Avg. Computation Time (ms/a)	*% FAR*	*% FRR*
2004DB1-A	16	291	0.58	0.384	1.54
2004DB2-A	16	300	0.216	0.415	1.33
2004DB3-A	16	300	0.247	0.745	1.6625

Intel i5, 2.1 GHz, 4 GB RAM

From table 4.3.2.5 we can see the matching results in the Figure 4.3.6 a, and b, below.



(a) (b)

Figure 4.3.6 (a) Percent of FAR and FRR, (b) Average computation Time machine

In this experiment the fingerprint matching based on 2D-Discrete Fourier transform technique. In this technique we have to test three databases, i, e: FVC-2004-DB1-A, DB2-A, DB3-A database and each data have different scan and different sized. For a normal scanned fingerprint image, the core point has generally appeared at the center of the image. With such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a reference core point the 2D-Discrete Fourier transform is applied to 64 sub-image of 16×16 pixels. According to the symmetry properties of the DFT, some left side and right side image can offer the very similar spectrum values. That can lead to the wrong justification and the percents of FAR and FRR is increased if the core point cannot be located or incorrectly located and the fingerprint images have low quality. However, the DFT can offer slightly better FAR and FRR performance. The 8×8 tiny tiles of 16×16 pixels are fed to the transform machine before the spectrum of corresponding tile are correlated. The results shown in the Table 4.3.2.5 and the Figure 4.3.5, we can see the percentage of FAR from DB1-A is better than DB2-A and DB3-A and DB2-A the percentage of FRR is better than other data because the number of the Tent less than data1 and data3. For the time matching the DB2-A and DB3-A is faster than its DB1-A when compared.

4.3.3 EXPERMENT 3

In this evaluation we propose fingerprint matching techniques using the 2D- DCT features. And the FVC 2004 DB1-A database set has been employed in this experiment. This amount of images is large enough to check the consistency of the algorithm as well as to widen the testing domain. As detailed in the previous sections; the machine has involved 3 main steps, i.e., spectrum finding, spectrum matching and average value computation. The matching decision is made upon the obtained average value. The merit of the algorithm is basically stated by its fault acceptance rate and fault rejection rate. Given as an example, matching score average values of samples obtained from a DCT process (a certain template) are plotted as shown Fig. 4.3.6 The matching decision can be made upon the observation. In this case, somewhere the value around 0.75 seems to be a good choice.

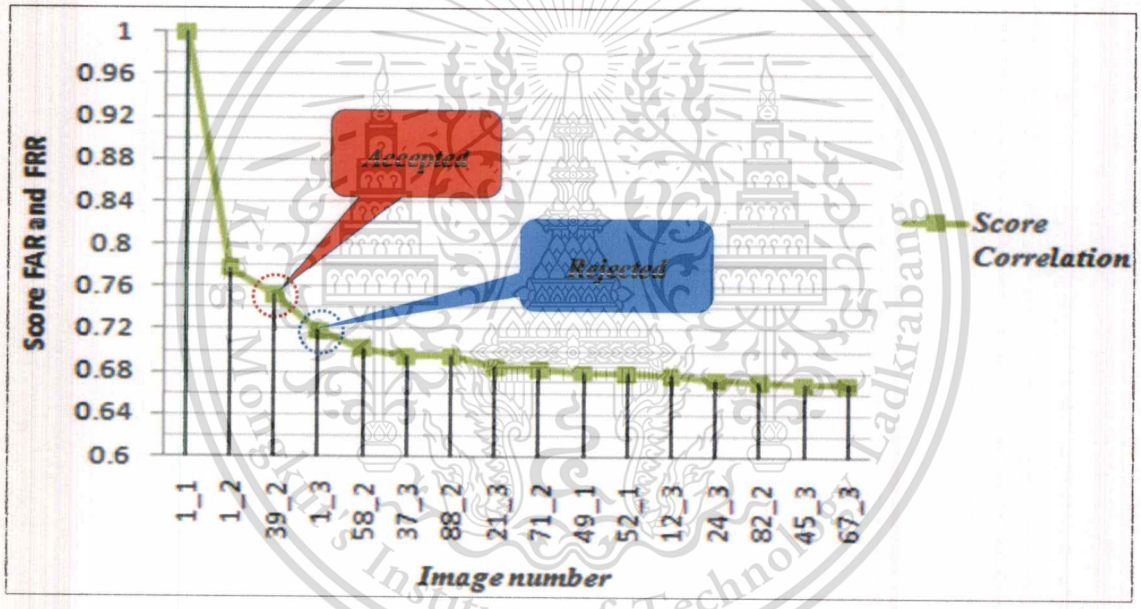


Figure 4.3.7 Example Average values of the correlation score of different images

The template is in fact the image 1_1. The decision on the value of 0.75 can result in image 1_2 and image 39_2 to be accepted. However, as the image 1_2 is a variation of the image 1_1. The decision is then wrong for the image 39._2. This is a case of faulty acceptance. From this algorithm the result shown in the Table 4.3.3 below.

TABLE 4.3.3 THE 2D-DCT RESULTS FROM FVC 2004-DB1-A

Pattern	Number of Tempiate	Number of Test image	*Avg. Values, spectrum* ≥ 0.75,		
			Avg. Computation Time (ms/a)	*% FAR*	*%FRR*
Whorl	4	66	0.394	0.67	1.34
Left loop	4	105	0.24	0.67	1.01
Right Loop	4	66	0.395	1.01	1.01
Tent	4	54	0.47	1.34	1.34
Avg%	16	291	0.37	0.9225	1.175

Intel i5, 2.1 GHz, 4 GB RAM

From table 4.3.3 we can see the matching results in the Figure 4.3.7 a, and b, below

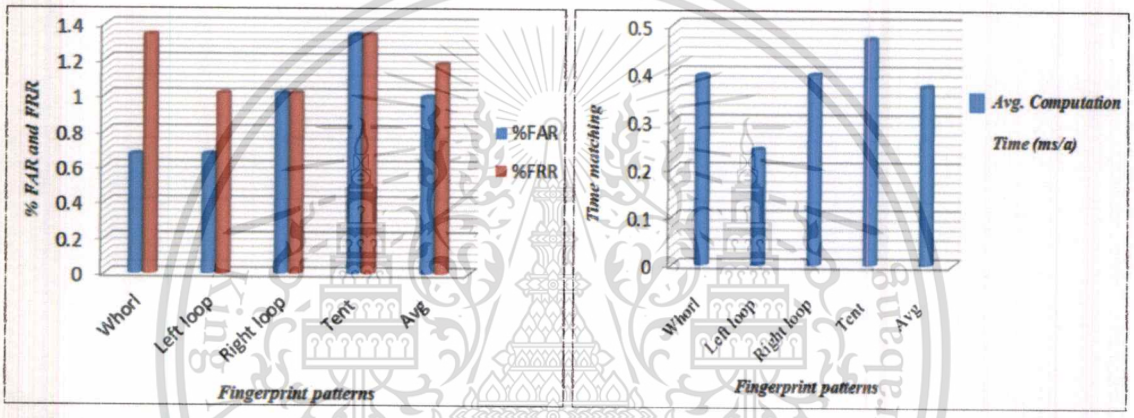


Figure 4.3.8 (a) Percentage of FAR and FRR, (b) Average computation Time machine

In this experiment we proposed the fingerprint matching by using 2D discrete cosine transform technique. In this technique the images under tested are those obtained in FVC-2004 (DB-1A). And this technique also similar whit 2D-DFT, for a normal scanned fingerprint image, the core point has generally appeared at the center of the image. With such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a reference core point the 2D-Discrete Fourier transform is applied to 64 sub-image of 16×16 pixels. According to the symmetry properties of the DCT, some left side and right side image can offer the very similar spectrum values. That can lead to the wrong justification and the percents of FAR and FRR is increased if the core point cannot be located or incorrectly

located and the fingerprint images have low quality. And The score given by 2 most similar sub-images can be close to +1, whilst that of the different images is very low. The average matching score can then be easily calculated based on the score of each sub-image matching. The highest average score implies the most similarity of those two cropped images. From this experiment the results shown in the table 4.3.3 and figure 4.3.8 we can improve the FAR 0.9225% and FRR 1.175%.

4.3.4 EXPERMENT 4

In this evaluation we have proposed a fingerprint matching using Normalized cross correlation (NCC) and two dimensional Discrete Fourier transform (2D-DFT). And the FVC 2004 DB1-A database set has been employed in this experiment. This amount of images is large enough to check the consistency of the as well as to widen the testing domain. As detailed in the previous sections; the machine has involved 3 main steps, i.e. NCC Score, spectrum finding, spectrum matching and average value computation. The decision is made upon the obtained average value. The merit of the algorithm is basically stated by its fault acceptance rate and fault rejection rate. Given as an , matching score average values of samples obtained from a DFT process (a certain) are plotted as shown Fig. 4.3.8 The matching decision can be made upon the observation. In this case, somewhere the value around 0.75 seems to be a good choice. Shown in the Fig . 4.3.8 Below.

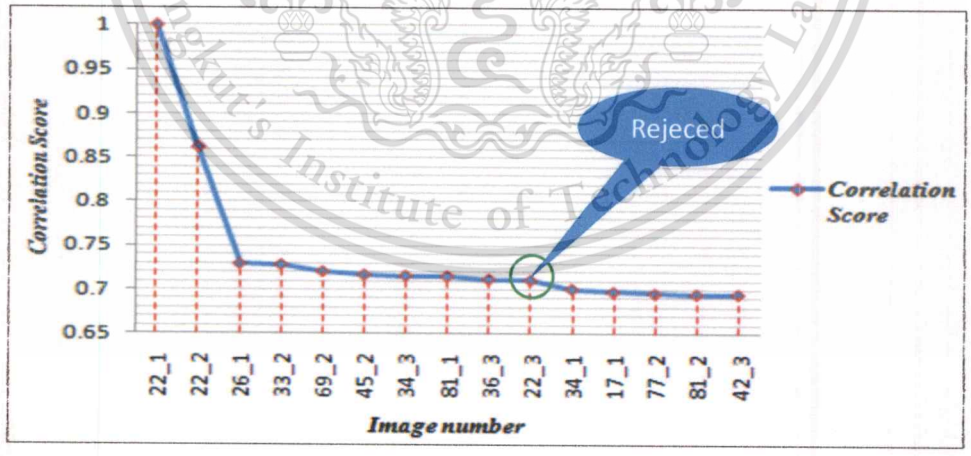
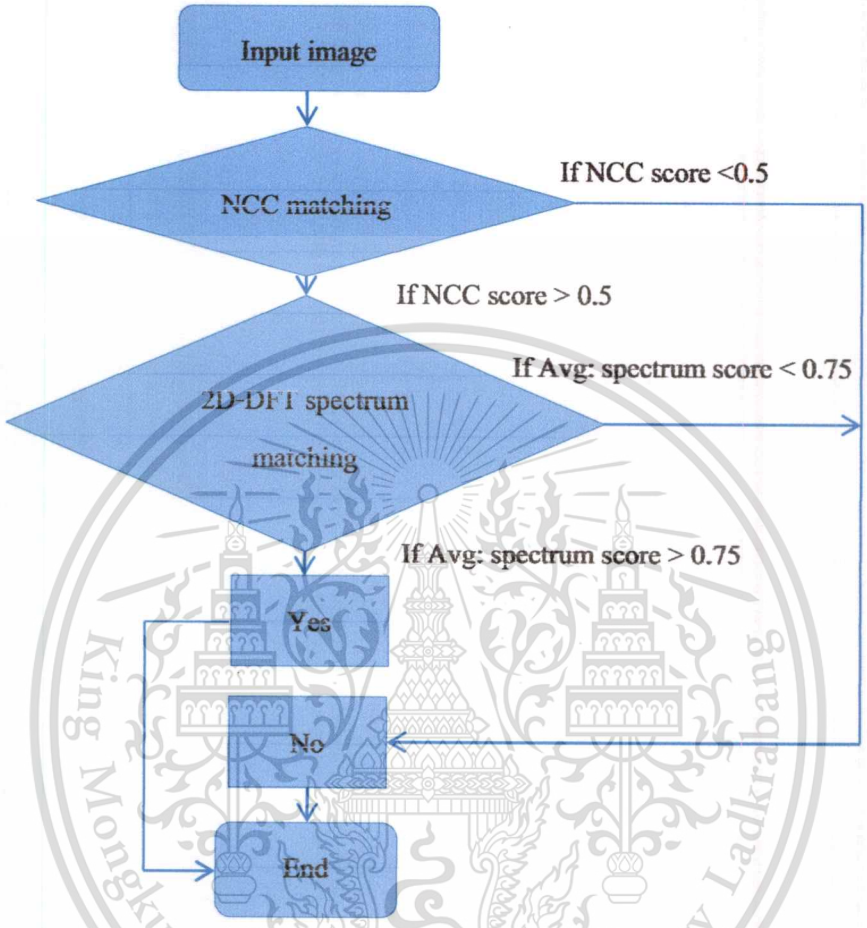


Figure 4.3.9 Example Average values of the correlation score of different images

The template is in fact the image 22_1. The decision on the value of 0.75 can result in image 22_2 and image 22_3 to be rejected . However, as the image 22_3 is a variation of the image 22_1. The decision

is then wrong for the image 22._3. This is a case of faulty rejected. And the Fig3.4.7 matching algorithm flowchart.



Finger 4.3.10 NCC and 2D-DFT matching algorithm flowchart

4.3.4.1 NCC Matching Result

The experiment we have set up 16 template images from 4 groups (4 images for each pattern). Those patterns are whorl, left loop, right loop, and tents. These are included in 97 individual images (35 left-loops, 22 right-loops, 18 tents, and 22 whorls). Each individual holds 3 images different scan. Therefore, there are 291 images involved in our test. Each

image has size 480×640 pixels. And if the two image similarity the NCC Score matching much more than 0.5. The evaluation result is shown in table 4.3.4.1 below.

TABLE 4.3.4.1 NCC MATCHING RESULTS FROM FVC 2004-DB1-A

Pattern	Number of Template	Number of Test image	*NCC. Error Matching score matching* > 0.5		
			Avg. Computation Time (ms/a)	*% FAR*	*%FRR*
Whorl	4	66	0.5	1.7	1.2
Left loop	4	105	0.378	1.6	1.2
Right Loop	4	66	0.6	1.6	1.4
Tent	4	54	0.58	1.7	1.6
Avg%	16	291	0.51	1.65	1.37

Intel i5, 2.1 GHz, 4 GB RAM

4.3.4.2 2D-DFT Matching Results

In this step we have to be cropped the test images and the template images from the 480×640 pixels into 128×128 pixels, and then divided into 64 sub-images and each sub-image with size 16×16 pixels. The result is shown in the table 4.3.4.2 below.

TABULAR 4.3.4.2 THE 2D-DFT MATCHING RESULTS FROM FVC 2004-DB1-A

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	66	0.62	0.336	1.56
Left loop	4	105	0.39	0.57	1.27
Right Loop	4	66	0.67	0.63	1.34
Tent	4	54	0.72	0	2.02
Avg%	16	291	0.58	0.384	1.54

Intel i5, 2.1 GHz, 4 GB RAM

4.3.4.3 Combination NCC and 2D-DFT Matching Results

In this experiment we measured the performance result by combination two steps the first step NCC matching step this step setup NCC Score matching more than 0.5 and the

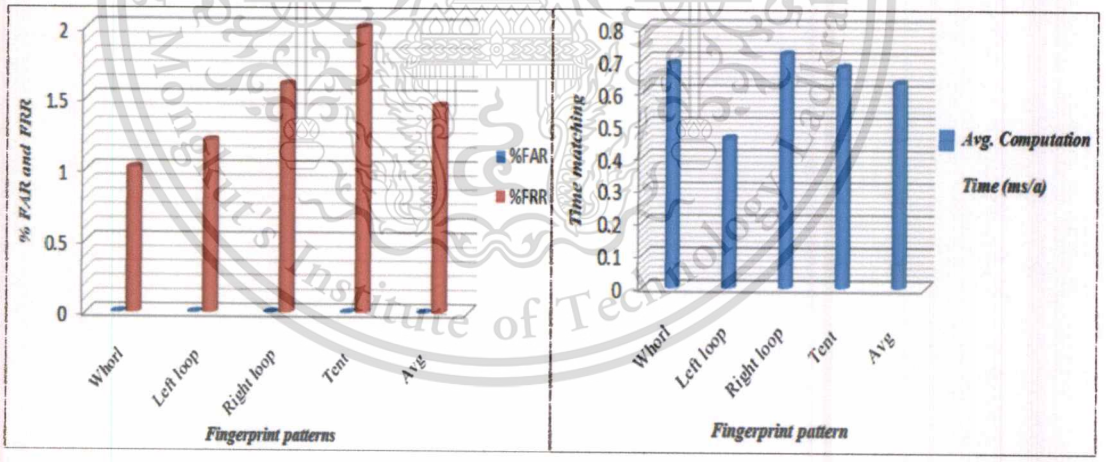
second step 2D-DFT step have sued the score who past the first step to process again and this step setup the score similarity more than 0.75. The experiment results shown in the table 4.3.4.3 below.

TABLE 4.3.4.3 COMBINATION NCC AND 2D-DFT MATCHING RESULTS

Pattern	Number of templates	Number of test image	*NCC Score* > 0.5, *Avg. Values, spectrum* ≥ 0.75		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	66	0.69	0	1.01
Left loop	4	105	0.46	0	1.2
Right Loop	4	66	0.72	0	1.6
Tent	4	54	0.68	0	2
Avg%	16	291	0.63	0	1.45

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

From table 4.3.4.3 we can see the matching results in the Figure 4.3.10 a, and b, below.



(a) (b)

Figure 4.3.11 (a) Percentage of FAR and FRR, (b) Average computation Time machine

In this experiment we combined two technique NCC and 2D-DFT technique. This technique can offer slightly better FAR and FRR performance. 4 pattern under tested, the Tent one holds rather high percents of FAR and FRR compared to others. This is because the core point cannot be

determined precisely and fingerprint scan has low quality. The ridge lines do not hold the sharp turn. Therefore the main drawback of the algorithm its dependency on the availability of the reference point (core point).

From the FAR and FRR result given in all our experiments , we can have some advantages compared to the methods reported in [51] has proposed the relative topological relationship among minutiae was used in fingerprint matching for its changeless characteristics in distorted fingerprints. Each minutia was defined by a characteristic record in which the minutia type and the relative topological relationship among the minutia and its 5 nearest neighbors are included. The fingerprints matched or not depend on the number of minutiae matched. And image rotation about $\pi/6$ degree. And FVC 2004DB1-A was used to test the algorithm in normal fingerprint matching. There are 100 fingerprints including 5 images from each 20 fingers. Each fingerprint was matched with the others using the algorithm given in this experiment. The matching rules are: the type ring of the neighbor minutiae must be the same and the difference of the numbers of the ridge between the neighbor and the minutia in two records is not more than 2. The obtained performances are shown in Table 4.3.4.4 below.

TABLE 4.3.4.4 MATCHING OF DIFFERENT WORKS

Techniques	Database	Number of Templates	Number of test images	*Avg. Values, spectrum* ≥ 0.75, NCC score >0.5		
				Avg. Computation Time (ms/a)	*% FAR*	*% FRR*
2D-DFT	2004DB1-A	16	291	0.58	0.384	1.54
	2004DB2-A	16	300	0.216	0.415	1.33
	2004DB3-A	16	300	0.247	0.745	1.6625
2D-DCT	2004DB1-A	16	291	0.37	0.9225	1.175
NCC and minutiae score	2004DB1-A	16	100	0.4992	0	1
NCC and 2D-DFT	2004DB1-A	16	291	0.63	0	1.45
Reference [51]	2004DB1-A	20	100	24	0.3	2.02

Intel i5, 2.1 GHz, 4 GB RAM

4.3.5 Summary

According to the results of our experiments given in this chapter shown in Table 4.3.4.4 we can see the experiments 4.3.1 NCC matching and 4.3.4.3 Combination NCC and 2D-DFT matching have obtained better results compared to other experiments. And from the proposed method is superior over those reported by [51]. The false reject rate and the average computation times of our method are better than the techniques noted in [51]. However the percents of FAR and FRR are increased if the core point cannot be determined precisely and the fingerprint images scan have low quality. The ridge lines do not hold the sharp turn. Therefore the main drawback of the algorithm is its dependency on the availability of the reference point (core point). And we hope we can find some alternative approaches to improve the precision of core point detection as well as seeking other alternatives that rely less on the availability of the reference point.

Chapter 5

Discussion, Conclusion & Future Prospects

5.1 Discussion

With the advancement of biometrics, due to increase in frauds and crimes, more and more biometric modalities are emerging. Fingerprints are widely used in many personal identification systems due to its permanence and uniqueness. Automatic fingerprint identification systems are being commercially deployed at many places. Hence, an error rate of just one percentage may prove to very disastrous. Currently, many researchers are trying to develop systems with one hundred percentage recognition rate. And one of the very important factors which can affect the performance of a fingerprint identification system is the quality of the input images. Several factors determine the quality of fingerprint image: skin conditions (e.g. Wetness, dryness, dirtiness, temporary or permanent cuts or bruises), sensor conditions (e.g. Dirtiness, noise, size), user cooperation, etc. The poor image quality leads to many pseudo-minutiae. This degrades the performance of fingerprint identification system. In a typical fingerprint identification system first of all acquisitions take place which means acquiring of fingerprint data from the user, then comes the feature extraction part which involves the use of various image processing applications and finally matching is done with template feature sets in the database.

5.2 Conclusion

In this thesis, we purpose of fingerprint matching by using normalized cross correlation , minutiae extraction, 2D discrete Fourier transforms and 2D discrete cosine transforms techniques. The normalized cross correlation technique to speed up the matching process, the template and the test images cropped to the size of 128×128 pixels and core point is assumed to be the center of this square. And the 2D discrete Fourier transforms and 2D discrete cosine transform, spectrum matching technique. The FAR and FRR results are better than the minutiae-based techniques proposed in the literatures. DCT based is faster than its DFT companion. However, the DFT can offer slightly better FAR and FRR performance. The 8×8 tiny tiles of 16×16 pixels are fed to the transform machine before the spectrum of corresponding tile are correlated. Of those 4 pattern under tested, the Tent one holds

rather high percents of FAR and FRR compared to others. This is because the core point cannot be determined precisely. The ridge lines do not hold the sharp turn.

The experiments are conducted on standard public databases FVC 2004 DB1-A , FVC 2004 DB2-A and FVC2004DB3_A. The three databases captures most of the problem that we have mentioned. However the percents of FAR and FRR are increased if the core point cannot be determined precisely and the fingerprint images scan have low quality. The ridge lines do not hold the sharp turn. Therefore the main drawback of the algorithm is its dependency on the availability of the reference point (core point). And we hope we can find some alternative approaches to improve the precision of core point detection as well as seeking other alternatives that rely less on the availability of the reference point.

5.3 Future Prospects

All of our techniques propose the main drawback of the algorithm is its dependence on the availability of the reference point (core point). To reduce with this problem we can find some alternative approaches to improve the precision of core point detection as well as seeking other alternatives that rely less on the availability of the reference point.

Reference

[1] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar , Second Editor "Handbook of Fingerprint Recognition", Springer, London, 2009

[2] Kamei T. "Image filter design for fingerprint enhancement", in Automatic Fingerprint Recognition Systems, Springer, New York, pp. 113–126,

[3] Xie, Su and CAI (2006). Xie X., Su F. And CAI A., "Ridge-Based Fingerprint Recognition", in Proc. International conference, on Biometrics, LNCS 3832, pp. 273–279, 2006.

[4] Anil K. Jain and David Maltoni. "Handbook of Fingerprint Recognition", Springer- Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[5] Mayank Vatsa , Richa Singh, "Biometric Technologies", Indian Institute of Technology Kanpur and Electronic , India

[6] Jain A.K, Chen Y, and Demirkus M. Pores and Ridges: "High-Resolution Fingerprint Matching Using Level 3 Features", PAMI, 29 (1):15–27, January 2007.

[7] Jain A.K., Hong L. and Bolle R., "On-line fingerprint verification", IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 19, no. 4, pp. 302–313, 1997.

[8] Raymond Thai "Fingerprint Image Enhancement and Minutiae Extraction", The University of Western Australia, 2003

[9] Hong, Y. Wan, and A. Jain. "Fingerprint image enhancement: Algorithm and performance evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8):777–789, August 1998.

[10] Grassley (1969). Grassley A., "On the automatic classification of fingerprints", in Methodologies of Pattern Recognition, S. Watanabe (Ed.), Academic, New York, 1969.

[11] Kass and Witkin (1987). Kass M. and Witkin A. "Analyzing oriented patterns", Computer Vision Graphics and Image Processing, vol. 37, no. 3, pp. 362–385, 1987

[12] Ratha, N., Chen, S., and Jain, A. "Adaptive flow orientation based feature extraction in fingerprint images", Pattern Recognition 28, 11 (1995), 1657–1672.

[13] Fang Yuen, Wangmeng Zuo, Kuanquan Wang "A Performance Evaluation of Filter Design and Coding Schemes for Palm print Recognition", 19th International Conference on Pattern Recognition, ICPR 20008, 8-11 Dec, 2008

[14] Burt P. J, and Shashua E. H. "The laplacian pyramid as a compact image code", IEEE Transactions on Communications, vol. Com-31 No. 4, April, 1983.

[15] Adelson E. H, Anderson C. H, J. R. Bergen, P. J. Burt, and J. M. Ogden. "Pyramid Methods in Image Processing", RCA Engineer, 33-41,29\6\ 1984.

[16] Jain A.K, S. Prabhakar and L. Hong, "A Multichannel Approach to Fingerprint Classification", IEEE Trans. On PAMI, Vol.21, No.4, pp. 348-359, April 1999

[17] Gonzales R.C. And Woods R.E. "Digital Image Processing, 3rd edition", Prentice-Hall, Englewood Cliffs, NJ, 2007.

[18] Ito K., Morita A, Aoki T, Nakajima H., Kobayashi K. and Higuchi T. "A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching", in Proc. Int. Conf. on Biometrics, LNCS 3832, pp. 316–325, 2006.

[19] Lindoso A., Entrena L, Liu-Jimenez J. and San Millan E., "Correlation-Based Fingerprint Matching with Orientation Field Alignment", in Proc. Int. Conf. on Biometrics, LNCS 4642, pp. 713–721, 2007.

[20] Sujan V.A. and Mulqueen M.P., "Fingerprint identification using space invariant transforms", Pattern Recognition Letters, vol. 23, no. 5, pp. 609–619, 2002.

[21] Ouyang Z., Feng J., Su F. and Cai A., "Fingerprint Matching with Rotation-Descriptor Texture Features", in Proc. Int. Conf. on Pattern Recognition (18th), vol. 4, pp. 417–420, 2006

[22] Wilson C.L., Watson C.I. and Paek E.G., "Combined optical and neural network fingerprint matching", Proc. of SPIE (Optical Pattern Recognition VIII), vol. 3073, pp. 373–382, 1997.

[23] Kryszczuk K.M., Morier P. and Drygajlo A., "Study of the Distinctiveness of Level 2 and Level 3 Features in Fragmentary Fingerprint Comparison", in Proc. Workshop on Biometric Authentication (in ECCV 2004), LNCS 3087, pp. 124–133, 2004.

[24] Chen J. and Moon Y.S, "A Minutiae-Based Fingerprint Individuality Model", in Proc. Conf. Computer Vision and Pattern Recognition, 2007.

[25] Jea T.Y. and Govindaraju V, "A minutia-based partial fingerprint recognition system", Pattern Recognition, vol. 38, no. 10, pp. 1672–1684, 2005.

[26] Bishnu A., Das S, Nandy S.C. and Bhattacharya B.B., "Simple algorithms for partial point set pattern matching under rigid motion", Pattern Recognition, vol. 39, no. 9, pp. 1662–1671, 2006.

[27] Ballard D.H., "Generalizing the Hough transform to detect arbitrary shapes", Pattern Recognition, vol. 3, no. 2, pp. 110–122, 1981.

[28] Ranade A. and Rosenfeld A, "Point pattern matching by relaxation", Pattern Recognition, vol. 12, no. 2, pp. 269–275, 1993.

[29] Baird H., Model Based Image Matching Using Location, MIT Press, Cambridge, MA,1984.

[30] Oh C. and Ryu Y.K., "Study on the center of rotation method based on minimum spanning tree matching algorithm for fingerprint recognition", Optical Engineering, vol. 43, no. 4, pp. 822–829, 2004.

[31] Tan X. and Bhanu B., "Fingerprint matching by genetic algorithms", Pattern Recognition, vol. 39, no. 3, pp. 465–477, 2006.

[32] Bazen A.M. and Gerez S.H., "Systematic methods for the computation of the directional fields and singular points of fingerprints", IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 24, no. 7, pp. 905–919, 2002.

[33] Jain A.K., Hong L. and Bolle R., "On-line fingerprint verification", IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 19, no. 4, pp. 302–313, 1997.

[34] Xudong Jiang and Wei-Yun Yau. "Fingerprint minutiae matching based on the local and global structures". In Proceedings of 15th International Conference on Pattern Recognition, volume 2, pages 1038–1041, 2000.

[35] Nalini Ratha Ibm, Nalini K. Ratha, Vinayaka D. Pandit, Ruud M. Bolle, and Vaibhav Vaish. "Robust Fingerprint Authentication Using Local Structural Sim- ilarity", In In Workshop on applications of Computer Vision, pages 29–34, 2000.

[36] Sharat Chikkerur, Alexander N. Cartwright, and Venu Govindaraju. K-plet and Coupled BFS: A Graph Based Fingerprint Representation and Matching Algorithm. In ICB, volume 3832 of Lecture Notes in Computer Science, pages 309–315. Springer, 2006.

[37] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. "Introduction to Algorithms", MIT Press and McGraw-Hill, 2001.

[38] Jain A.K., S. Prabhakar, Lin Hong, and S. Pankanti. Finger Code: "A filter bank for fingerprint representation and matching", In Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, volume 2, pages –193, 1999

[39] Loris Nanni and Alessandra Lumini. "Local binary patterns for a hybrid finger- print matcher", Pattern Recogn., 41(11):3461–3466, 2008.

[40] Jonathan D. Stosz and Lisa A. Alyea." Automated System for Fingerprint Au- thentication Using Pores and Ridge Structure", In Proc. of Automatic Systems for the Identification and Inspection of Humans, volume 2277, pages 210–223, 1994.

[41] Mayank Vatsa, Richa Singh, Afzel Noore, and Max M. Houck. "Quality- augmented fusion of level-2 and level-3 fingerprint information using DSm theory", Int. J. Approx. Reasoning, 51–61, 2009

[42] Marsh R. A., and G. S. Petty, "Optical Fingerprint Correlate, US Patent 5050220, 1991.A. Jain, L. Hong, and R. Boll, "On-line fingerprint verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4):302–313, April 1997

[43] Lindoso A, Entrena L., Liu-Jimenez J. and San Millan E, "Correlation-Based Fingerprint Matching with Orientation Field Alignment", in Proc. Int. Conf. on Biometrics, LNCS 4642, pp. 713–721, 2007.

[44] Chen, Tian and Yang (2006). Chen X, Tian J. and Yang X, "A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure", IEEE Transactions on Image Processing, vol. 15, no. 3, pp. 767–776, 2006.

[45] Tachphetpiboon S. and T. Amornraksa, "Applying FFT Features for Fingerprint Matching", IEEE Trans., 2006.

[46] Yuh-Ming Huang, ja-Ling Wu, and Chaou-TingHsu " A Refned Fast 2-D discrete cosine transform Algorithm with regular butterfly structure", PP 376-383.IEEE Transaction on Consumer Electronics, Vol.44,No.2, MAY,1998.

[47] Xiao-Yuan Jing and David Zhang, "A Face and Palmprint Recognition Approach Based on Discriminant DCT Feature Extraction", IEEE Transaction on Systems, Man and Cybernetics-Part B: Cybernetics, Vol. 34, No. 6, December 2004.

[48] Wang Y., J. Hu and D. Philips. "A Fingerprint Orientation Model. Based on 2D Fourier Expansion (FOMFE) and Its Application to Singular-Point Detection and Fingerprint Indexing", IEEE Trans. Pattern Anal. Mach. Intell., 573–585, 2007.

[49] Karthik Nandakumar, "Fingerprint Matching Based On Minutiae Phase Spectrum", Institute for Infocomm Research, A*STAR, Fusionopolis, Singapore, PP 216-221, 2/12/2012 IEEE.

[50] XunqiangTao, Xin Yang, Kai Cao, Ruifang Wang, Peng Li and Jie Tian, "Estimation of fingerprint orientation field by weighted 2D Fourier expansion model", DOI 10.1109/ICPR.2010.312, PP 1253 -1256.

[51] Wei-bo ZHONG, NING Xin- bao, WEI Chen-Jia, "A Fingerprint Matching algorithm based on the relative topological relationship among minutiae", IEEE Int. Conference Neural Networks & Signal Processing Zhenjiang, China, June 8-10, 2008 PP 225-228

Appendix A

Biography

Personal Information

Name & Surname:	Mr. Souksamay Insankeovilay
Nationality:	Lao
Birth of date:	July, 07, 1984
Place of birth:	Houephone province, Lao P.D.R

Education

High diploma

Field:	Electronics Engineering
Duration:	2004 - 2008
Institute:	Department of Electronics, Faculty of Engineering, National University of Laos.

Bachelor degree (Electronics Engineering, Bridging course)

Field:	Electronics Engineering
Duration:	2008 - 2010
Institute:	Department of Electronics, Faculty of Engineering, National University of Laos

Master degree

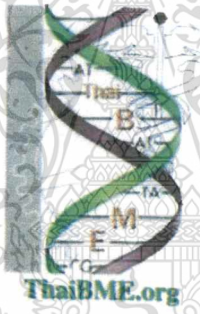
Field:	Electronics Engineering
Duration:	2011 – 2013
Institute:	International College, Department of Electronics, Faculty of Engineering, King Mongkut's Institute of Technology, Ladkrabang, Thailand

BMEiCON-2011

4th Biomedical Engineering International Conference

29-30-31 January 2012

Chiang Mai, Thailand



IEEE THAILAND SECTION

IEEJ

IJABME

BMEiCON 2011

IEEE EMB Thailand Chapter

Fingerprint Matching With Cross Correlation and Minutiae Scores

Souksamay Insankeovilay
International College,
King Mongkut's Institute of technology Ladkrabang,
Bangkok 10520, Thailand
Email: samay.84@hotmail.co.th

Poramate Prasarn, and Somsak Choomchuay
Department of Electronic Engineering, Faculty of Engineering,
King Mongkut's Institute of technology Ladkrabang,
Bangkok 10520, Thailand
Email: storm_thunderz@hotmail.com, kchsomsa@kmitl.ac.th

***Abstract*—This paper reports a combination technique for fingerprint identification (matching). The proposed method utilizes both Normalized cross correlation (NCC) template matching and minutiae matching. This method offers better performance when compared to each individual matching. Moreover, our method is less sensitive to rotational effect. The proposed technique is, however, based on the availability of core point. The technique fails if the core point cannot be located or incorrectly located. The first matching is performed based on the NCC score matching of the pattern around core point. Only few candidates are again matched based on the observed minutiae (i.e., bifurcate and end points with a particular range of pre-defined angle). Using this 2-step matching, we can improve the FAR and FRR. Images under tested are those obtained in FVC-2004 (DB-1A). There are 16 templates (4 groups of 4 patterns each). We have used 1,000 specimens (100 patterns for 10 times) in our experiment. Upon the investigation, we have obtained 0% FAR and 1% FRR.**

Keywords-component; formatting; style; styling; insert (key words)

I. INTRODUCTION

As biometric data processing becomes more and more important in the decade of information technology, there are several vital needs in data consistency and data security. Moreover, the important of the tracking (or tracing) is also extended to the person who is the owner of such data, no matter the one who sends it or the one who receives it. Personal identification by mean of fingerprint pattern is one of the most popular and reliable use biometric techniques. This is because fingerprint holds many desirable features such as universality, permanence, collectability, and distinctiveness. Personal identification based on fingerprint matching is now, therefore, popular in wide range of applications.

Fingerprint characteristics are basically divided into two groups, i.e., Local characteristics and Global characteristics. Global characteristics are general features of any fingerprint based on which classification of fingerprints into one of defined classes is performed before matching. This will cause the matching operation to be performed faster. Classes are generally classified into: Left loop, Right loop, Whorl (including dual loop), Arc, and Tent. Another important fingerprint feature is the local ridge characteristics there are two prominent local ridge characteristics: ridge ending and ridge bifurcation. Both of them are referred to as minutiae or minutiae points. These features are illustrated in Fig. 1

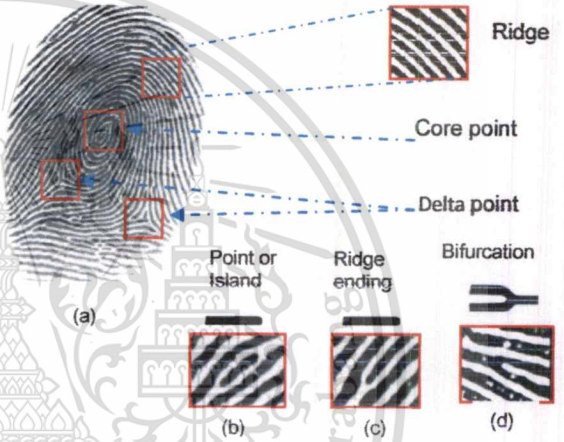


Figure 1. Fingerprint feature and definitions

There are two main streams in fingerprint pattern matching (or fingerprint matching); minutiae–based and images-based. Compared to the image-based technique, a minutiae-based matching relies on less information and offers better performance as the matching area is larger. Generic correlation matching [1] is less to relent according to to rotation and translational variances. Direct minutiae matching [2, 3] are certainly the most well-known and widely used method according to its higher recognition accuracy. Another matching technique is known as a spectrum matching which is based on a local texture analysis where the fingerprint area of interest is tessellated with respect to the core point [4]. Although the obtained spectrums are not as distinctive as minutiae, these features may be used in conjunction with minutiae to increase system accuracy and robustness.

Image-based matching on the other hands, offer good registration in particular when the matching area is fairly small. However, the technique consumes large storage and computing resources. The technique works regardless the availability of

This work is partially supported by AUN/SEED-Net program under the Research Collaboration scheme.

978-1-4577-2190-8/11/$26.00©2011 IEEE

the standard point neither core point nor minutiae point. Variance feature of orientation field matching has been proposed in [5]. Wavelet based matching methods proposed by [2] and [6] have shown their better recognition rates. Normalized cross correlation (NCC) has been applied together with group delay spectrum (GDS) and dynamic programming (DP) for line scan matching [7].

The performance of a fingerprint recognition method involves a tradeoff among different performance measures, i.e.; accuracy, efficiency, template size, and so on. Different applications may desire different properties in the fingerprint matching algorithms (e.g., template size, matching speed, memory requirements, and etc). With this regard, a combination of both image and minutiae could be an ideal that the pros of each and be utilized.

The rest of this paper is organized as follows. In the next section we will give a brief procedure of Normalized Cross Correlation matching (NCC). Al matching steps are given with certain details in section 3. Algorithm evaluations with some demonstrated results are elaborated in section 4. Finally the work is concluded in section 5.

II. A TEMPLATE MATCHING METHOD

The main purpose of using this procedure is to evaluate the coarse matching of two patterns, for best matching result; size and orientation of the detail image are assumed to be the same. Generally, a correlation method is a technique which can show how strongly pairs of variables are related. The result indexed by correlation coefficients value of which -1.0 to +1.0. The closer range of +1, the more closely one variable is related to the other. The correlation between two signals (cross-correlation) is a standard approach to find out how the two signals are related. It has shown its good applications in pattern recognition and cryptanalysis. Of its kinds, normalized cross correlation (NCC) has also been used extensively in machine vision for industrial inspection including defect detection in complicated images.

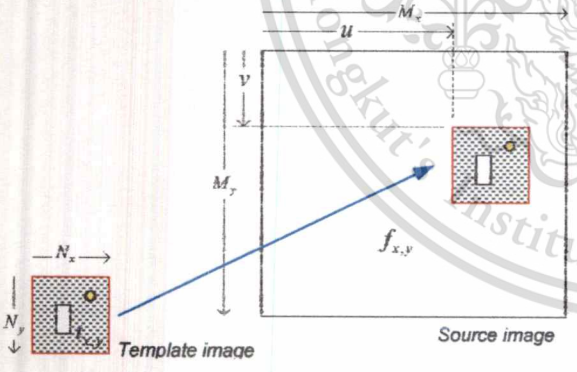


Figure 2. Matching of template t into the source image f

Shown in Fig. 2 Let f be a test image (source image) and t be a template image, we want to seek any similarity of the template t to any portion of test image f. In this particular case, the image size t is smaller or equal to f a simple method for measuring similarity or mismatch performed by taking the absolute difference between template image t and given test image f over a specific region.

If we take the sum of difference square between template t and give image f over a region offset by u and v in each dimension, then we can get:

$$d^2_{f,t}(u,v)=\sum_{x,y}\left[f(x,y)-t(x-u,y-v)\right]^2 \qquad (1)$$

The above equation (1) can be expanded to,

$$d^2_{f,t}(u,v)=\sum_{x,y}\begin{bmatrix} f^2(x,y)-2f(x,y)t(x-u,y-v) \\ +t^2(x-u,y-v)\end{bmatrix} \qquad (2)$$

The term $\sum_{x,y}\left[t^2(x-u,y-v)\right]$ is fixed for a given template image. Likewise, the term $\sum_{x,y}\left[f^2(x,y)\right]$ is also approximated to be fixed. Then the cross correlation expression given in (3) will give the degree of similarity.

$$c(u,v)=\sum_{x,y}\left[f(x,y)t(x-u,y-v)\right] \qquad (3)$$

Direct implementation of (3) leads to a problem that image intensity may vary from region to region. The obtained result is not consistent. To avoid such a problem, both means and variances are taken into account. The resulted (4) is known as normalized cross correlation (NCC).

$$\gamma(u,v)=\frac{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]\left[t(x-u,y-v)-\bar{t}\right]}{\sqrt{\sum_{x,y}\left[f(x,y)-\bar{f}_{u,v}\right]^2\sum_{x,y}\left[t(x-u,y-v)-\bar{t}\right]^2}} \qquad (4)$$

where

$\bar{f}_{u,v}$ and $\bar{t}$ are the means of $f(x,y)$ and t respectively.

$$\bar{f}_{u,v}=\frac{1}{N_xN_y}\sum_{x=u}^{u+N_x-1}\sum_{y=v}^{v+N_y-1}f(x,y)$$

and

$$\bar{t}=\frac{1}{N_xN_y}\sum_{x=u}^{u+N_x-1}\sum_{y=v}^{v+N_y-1}t(x,y)$$

In practice to avoid excessive computation, fast and approximated techniques are used to compute (4) [2], [3].

III. Fingerprint Matching Procedures

There are two folds in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. Details are given as follows:

A. Database Construction

In practice there could be a huge fingerprint patterns stored as database. To identify the case, an anonymous pattern must seek its most similarity to one or few database patterns. Storing those tons of patterns without loosing their originality is also a problem to be solved. In our approach database construction is as follows:

- The raw image is enhanced with Gabor filtering.
- The core point of the enhanced imaged is located using point care technique.
- Fingerprint orientation is determined.

In determining the pattern orientation we firstly did image binarization and thinning. Around the core point, the circle of interest with the radius of 100 pixels is drawn. An area of 15x15 pixels around the core point is assumed as a core point. Average angles of ridges line between this box to the circumference is considered to be the orientation of the pattern.

There could be some other directional filters, a Gabor filter one can be used nicely with reasonable computational cost. Likewise there are also some other methods, i.e. maximum curvature and geometric region that can be alternatively used in determining the location of the core point.

B. First Matching Step: Normallized Cross Correlation

The specimens (test images) are then compared to the template (database) using the following steps:

- Use the given above procedure to determine the core point and pattern orientation.
- For the aligned core point, the test image is rotated with the amount of degrees difference between the two images.
- Two images are then cropped with the size of 128x128 pixels (a core point is at the center).
- Each image is then divided in to 4 sub-image; 64x64 pixels.
- The corresponding sub-images are then matched with NCC template matching. Each region's matching score are summed up. Image with score above the set value (threshold) can pass this coarse matching.

C. Second Step Matching: Minutiae Matching

There could be few matching that give us high score. These candidates are then fed into the fed into minutiae investigation.

- Candidate images are fed into the binarization and minutiae extraction. The minutiae extraction offers us type of minutiae (bifurcate or end point) as well as the corresponding distance (from the core point) and the angle, i.e. distance from the core point and leverage angle, $g(r,\theta)$.
- The score is counted once the criteria is met, i.e. $r \pm 3$ pixel and $\theta \pm \frac{\pi}{12}$ radians.

IV. Evaluation and Results

To investigate the matching algorithm detailed in previous sections, we have set up 16 template images (16 individuals) from 4 group patterns (4 images for each pattern). Those patterns are whorl, left loop, right loop, and tent. 100 images including templates are primarily selected as test images. We have repeated the testing for 10 times. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 database DB1-A set has been employed in this experiment.

In depth; we have investigated 4 issues, namely; i) what should be the best threshold score to pass the proper candidates in the template matching step, ii) what would be the tolerance of the minutiae angle we should use in the minutiae matching step, iii) what kind of fingerprint pattern that prone to fail when the decision is made, and iv) when compared to other existing matching methods what kind of merits we can gain.

By varying the NCC matching score as FAR and FRR are observed, it is found that the score around 0.5 is ideal. This can be clearly noticed from the graph shown in Fig. 2. Too high score can help fault acceptance rate but destroying the fault rejection rate.

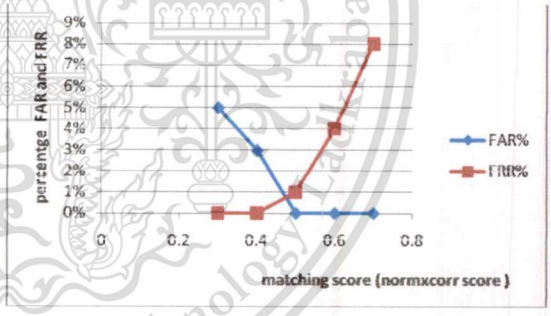


Figure 3. Matching score versus FAR and FRR

Although we have rotated the image before any other processing, the average angle obtained in orientation finding cannot be so accurate. We have investigated this by varying the constrain angle in the minutiae matching step. The (minutiae) candidates are considered if they hold the angle between $\pm 9^{\circ}$, $\pm 12^{\circ}$, $\pm 15^{\circ}$, and $\pm 18^{\circ}$. As shown in Table I, the matching still offers desirable result provided that we have kept the tolerance of 15 degree or less. When the angle grows larger, the nearby minutiae are main cause of the failure.

TABLE I. CONTRAIN ANGLES USED IN THE MINUTIAE MATCHING

Test	Corr. Matching Score ≥ 0.5 and $r \pm 3$		
	Constraint angle	*% FAR*	*% FRR*
1	$\frac{\pi}{20} = 9^{\circ}$	0	0
2	$\frac{\pi}{15} = 12^{\circ}$	0	0
3	$\frac{\pi}{12} = 15^{\circ}$	0	0
4	$\frac{\pi}{10} = 18^{\circ}$	4	0

For each investigated pattern, we found that the whorl pattern is sensitive to be a fault rejection one. This can be noted in Table II below. However we need few more investigations to check whether the case is strongly concerned the pattern or it just because of the image quality.

TABLE II. MATCHING RESULTS VERSUS FINGERPRINT PATTERN

Pattern	Corr. Matching Score ≥ 0.5, $\theta = \frac{\pi}{12}$, and $r \pm 3$		
	Avg. computation time (ms)[a]	*% FAR*	*% FRR*
Whorl	52.97	0	1
Left loop	52.97	0	0
Right Loop	52.97	0	0
Tent	52.97	0	0

a. Intel core i5, 4 GB RAM, 1000 images

Whether the proposed method can have some advantage compared to the methods reported in the literature, we did some comparisons. [15] used 8 images of 21 individuals. They have employed topology matching (Delaunay triangle edges, deformation model, and maximum bipartite matching scheme) in the matching procedure. [16] have used quite normal minutiae matching procedure. Maximum curvature was used for core point locating. [16] and ours used FVC2004-DB1A, but [16] used 5 images of 20 individuals and our used 100 individual images (35 left-loops, 22 right-loops, 21 tents, and 22 whorls). Our database is constructed with 16 individuals (lie in 100 individuals but different images). We have run the algorithm for 10 rounds. Results are shown in Table III.

TABLE III. FINGERPRINT MATCHING OF DIFFERENT WORKS

Matching Scheme	Results		
	Avg. computation time (ms)	*% FAR*	*% FRR*
Ref. [15]	29[a]	5.46	0.19
Ref. [16]	24	1.37	0.50
Proposed[c]	26[b]	0	1.00

a. Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

c. Corr. Matching Score ≥ 0.5, $\theta = \frac{\pi}{12}$, and $r \pm 3$

In term of FAR, our proposed method is superior over [15] and [16]. Of FRR we cannot compete both of them. The rejected image is basically poor and/or only some image portions are clearly available. This results in the failure of core point identification.

V. CONCLUSION

In this paper we have proposed an alternative method for fingerprint matching. Normalized cross correlation followed by minutiae matching has been proposed. The first step can be considered as a coarse matching whilst the second is a fine matching. To speed up the matching process, the images are cropped to the size of 128x128 pixels and core point is assumed to be the center of this square. With FVC2004-DB1A database, the 0% FAR and 1% FRR have been obtained. The main drawback of the algorithm is its dependency on the availability of the reference point (core point). We have obtained some high percentages of FRR because of this failure. We hope we can find some alternative approaches to improve the performance of this work further.

REFERENCES

[1] L Coetzee and E.C. Botha, "Fingerprint recognition in low Quality, images," Pattern Recognition, vol. 26, no.101993, pp. 1441–1460.

[2] R. A. Marsh, and G. S. Petty, "Optical Fingerprint Correlate, "US Patent 5050220, 1991.A. Jain, L. Hong, and R. Boll, "On-line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4):302–313, April 1997.

[3] M. Taco and P. Kuosmanen, "Fingerprint matching using an Orientation based minutia descriptor," IEEE Trans. on Patti. Analyst and Mach In tell, vol. 25, no. 8, 2003, pp. 1009–1014.

[4] Y. Jibe, Y. Yifang, Z .Rangie and S. Quaff, "Fingerprint minutiae Matching algorithm for real time system, " Pattern Recognition, 2006, pp. 143–146.

[5] A.K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filter bank Based fingerprint matching," IEEE Trans. Image Processing, 9(5):846–859, 2000.

[6] J. Koru and N. Apathy, "No minutiae Based Fingerprint Matching," Proc. of Int. Assoc. of Computer Science and Information Technology, Spring Conference, IACSIT, 2009.

[7] Z. Bauhaus, J. Yinchuan, Z. Jianfeng, Y.Dahua, and Z. Quentin, "Fingerprint template matching Algorithm Based on Daubechies Wavelet, Proc. of Int. Conf. on Communication Software and Networks, ICCSN-2009.

[8] S. Y. Tan, W.T. Huang, C.H. Chen, and Y.J. Chang, "Sweep Fingerprint Verification System Based on Template Matching, Journal of Recent Advances in Networking, VLSI, And Signal Processing, ISBN: 978-960-474-162-5.

[9] J. K. Kim, S.H. Chase, S.J. Lim, and S.B. Pan, "A Study on The Performance Analysis of Hybrid Fingerprint Matching Methods," Int. Journal of Future Generation Communication and Networking, pp. 23-28.

[10] S. D. Wei and S. H. Lai, "Fast Template Matching Based on Normalized Cross Correlation with Adaptive Multilevel Winner Update," IEEE Trans. Image. Proc., vole 17, no.11, Nov. 2008.

[11] J. P. Lewis, Fat Normalized Cross-Correlation, Industrial Light and magic.

[12] Kai Bristle and Use D. Han beck, Template Matching Using Fast Normalized Cross Correlation. Proc. of SPIE01, vol. 4387, March 2001.

[13] Y. He, J. Tina, X. Lou and T. Zhang, "Image enhancement and Minutiae matching in fingerprint verification", Patti. Reclog. Letts, no, 24, 2003, pp. 1349-1360.

[14] N.K. Ratha, K. Karu, S. Chen and A.K. Jain, "A Real-Time Matching System for Large Fingerprint Databases, " PAMI, vol.18, no. 8, 1996, pp. 799-813.

[15] C. Wang, M. Gavrilova, Y. Luo, and J. Rokne, "An efficient algorithm for fingerprint matching, " IEEE Conf. on Pattern Recognition, 2006.

[16] S. Mohammadi and A. Frajzadeh, "A Matching Algoritm of Minutiae for Real Time Fingerprint Identification System," Proc. of World Academy of Science, Engineering and Technology 60, 2009.

AUN/SEED-Net JICA KMITL DE LA SALLE UNIVERSITY

5th AUN/SEED-Net Regional Conference on Information and Communications Technology

"Leveraging ICT Research to Meet the Challenges of Establishing Secure, Equitable and Sustainable Communities for the 21st Century"

October 18-19, 2012 • Traders Hotel, Manila, Philippines

Fingerprint Matching based on 2D Fourier Transform Features

Souksamay Insankeovilay
International College
King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand
Email: souksamay.en@hotmail.com

Somsak Choomchuay and Kazuhiko Hamamoto
Department of Electronic Engineering, Faculty of Engineering,
King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand
Information Media Technology, School of Information
Technology and Electronics Tokai University, Tokyo, Japan
Email: kchsomsa@kmitl.ac.th; hama@keyeki.cc.u-tokai.ac.jp

Abstract—**In this paper, we proposed a fingerprint matching scheme based on 2D Fourier transform features. We use this technique for finding the magnitude value of the spectrum, as well as spectrum phase. Such the obtained matching score is then further processed for pattern classification. From the results, we can see that this method offers good performance when compared other individual matching techniques. In addition, this method is less sensitive to rotational effect. By using this technique, we can improve both the false accept rate (FAR) and false reject rate (FRR). For FVC-2004 (DB-1A), we can obtain 0.384% of the FAR and 1.54% of FRR, and from FVC-2002 (DB2-A) we can obtain 0.88% of FAR and 1.75% of FRR. On its drawback, the proposed technique is still based on the availability of core point. Therefore, this technique can introduce some errors if the core point cannot be located or improperly located.**

Keywords-component; Biometric; fingerprint matching; fingerprint classification, 2D Fourier transform

I. INTRODUCTION

As machine based data processing becomes more and more important in the decade of information technology, there are several vital needs in data consistency and data security. Moreover, the importance of the tracking (or tracing) is also extended to the person who is the owner of such data, no matter the one who sends it or the one who receives it. Personal identification by mean of fingerprint pattern is one of the most popular and reliable use Biometric techniques. This is because fingerprint holds many desirable features such as universality, permanence, collect ability, and distinctiveness. Personal identification based on fingerprint matching is now, therefore, popular in a wide range of applications. Fingerprint characteristics are basically divided (classified) into four patterns, namely: Left loop, Right loop, Whorl (including dual loop), Arc, or Tent. These features are illustrated in Fig. 1. The classification process tries to clarify out the input fingerprints into one of defined classes before matching procedure. This will result that the matching operation to be performed faster.

This work is partially supported by AUN/SEED-Net program under the Research Collaboration scheme.

a. Left Loop b. Right Loop d. Whorl d. Tent or Arc

Fig. 1 Fingerprint Pattern features

Image-based matching, in general, offer good registration in particular when the matching area is fairly small. However, the technique consumes large storage and computing resources. The technique also works regardless the availability of the standard point neither core point. Variance feature of orientation field matching has been proposed in [1], wavelet based matching methods proposed by [2] and [3] The performance of a fingerprint recognition method involves a tradeoff among different performance measures, i.e.; accuracy, efficiency, spectrum, angles, and so on. Minutiae-based matching, on one hand, can offer a very accurate matching result but on the other hand, it does require a clear fingerprint pattern (i.e., valley, ridge, and minutiae points). In some cases, reference point (such as core and/or delta point) is also needed. In this paper, the matching procedure requires both the core point and the spectrum magnitude of the pattern around the core point. The rest of this paper is organized as follows. In the next section we will give a brief procedure of 2D Fourier transform matching (DFT). Matching steps are given to certain details in section III. Algorithm evaluations with some demonstrated results are elaborated in section IV. Finally the work is concluded in section V.

II. 2D FOURIER TRANSFORM

The term image transform refers to a class of unitary matrices used for representing images. Images are expanded in terms of a discrete set of basis arrays called basis images [4]. Energy conservation, energy compaction, decoration is the important properties of these transforms. Image transforms like Discrete Fourier Transform (DFT) to digital image data is well studied and extensively used for many years.

The two dimensional DFT of an $M \times N$ image f (x, y) is a separable transform defined as:

$$F(u,v) = \mathrm{F}[f(x,y)] = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\left\{-2j\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad (1)$$

The u and v are frequency component of each dimension, and we can find a Fourier spectrum as: (2)

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)}$$

And spectrum angles by $\varphi(u,v) = \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right]$ (3)

After transformation, the phase values provide little information, only magnitudes are further considered for our application

This method we measure the performance by correlation-based fingerprint matching. Use the value of the spectrum, spectrum phase and the value of the line angles between the template images and test images, we can define as.

$$r = \frac{\sum_m\sum_n \left(A_{mn}-\overline{A}\right)\left(B_{mn}-\overline{B}\right)}{\sqrt{\left(\sum_m\sum_n \left(A_{mn}-\overline{A}\right)^2\right)\left(\sum_m\sum_n \left(B_{mn}-\overline{B}\right)^2\right)}} \quad (4)$$

Where $\overline{A} = mean2(A)$, *and* $\overline{B} = mean2(B)$

In our experiment, we started fingerprints images from database FVC2004 DB1_A where each image hold's the size of 480×640 *pixles* .Around the core point, the image is cropped into into 128×128 *pixles*, and further divided into 64 sub- images, of the size 16×16 *pixles* .The 2D Fourier transform is then applied to each sub-image. These are illustrated in Fig.2.

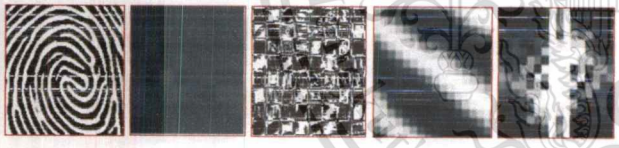


Fig. 2 (a) Fingerprint image cropped to size 128x128 pixels. (b) 64sub-image cropped with size 16x16 pixels. (c) 64 sub-image is 2D Fourier transforms. (d) One sub-image with size 16x16 pixels. (e) Spectrum of one sub-image transforms

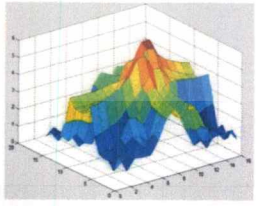


Fig.3 the magnitude Fourier transform of one sub_image with size (16x16 pixels).

As common to many others, in our method there are two folds in the fingerprint matching procedure, database construction and matching algorithm. Steps are illustrated in Fig 4.

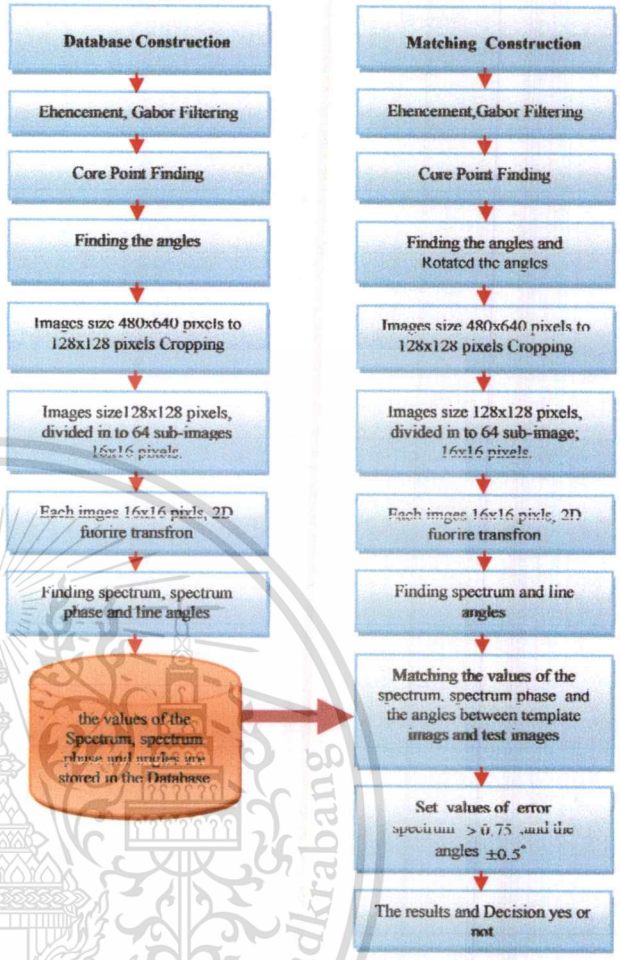


Fig.4 Algorithm matching steps

Database construction and matching algorithm hold most common steps since the sampled image has to be compared with what's stored in the database. Images are firstly enhanced with several sub-steps, i.e., normalization and filtering. Gabor filter proposed by [6,7] is an effective directional filter tool. Core point detection using point care, the method detailed by [8], is evoked afterward. With the obtained core point we can find a different angle that enables us to rotate the sampled image to the same orientation as that of the referenced non-rotate image [9]. Given in Fig. 4, θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled) image, then θ_3 is the angle differences between those two images. We then have to rotate the test image by (θ_3) degree, ($\theta_3 = \theta_2 - \theta_1$). For a normal scanned fingerprint image, the core point has generally

appeared at the center of the image. With such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a reference core point the 2D Fourier transform is applied to 64 sub-image of 16x16 pixels. Details of this 2D transform can be found in [10, 11]. Spectrum feature as well as angle is then stored for the matching purpose. More details are elaborated in the next section.

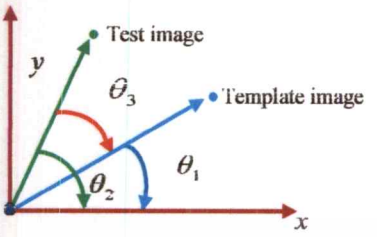


Fig .5 Angle of the template rotated

III. FINGERPRINT MATCHING ALGORITHM

There are two folds in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. Details are given as follows:

A. Database Construction.

In practice there could be a huge fingerprint pattern stored as database. To identify the case an anonymous pattern must seek its most similar to one or few database patterns. Storing those tons of patterns without losing their originality is also a problem to be solved. In our approach database construction is as follows:

- Including the images from FVC-2004 (DB1-A) and FVC-2002 (DB2-A) database.
- The raw image is enhanced with Gabor filtering.
- Mark the core point of the enhanced imaged is located using point care technique and Core point is a center.
- Images are cropped into the size of 128x128 pixels (a core point is at the center).
- Images, size 128x128 pixels divided into 64 sub-images, with the size 16x16 pixels.
- Apply the 2D Fourier transform to that sub-image.
- Determine the value of the spectrum, spectrum phase and the value of the line angle of each sub-image.
- Each image value is stored in the local database.

B. Two Dimensional Fuoriertansfrom Matching steps.

The specimens (template) are then compared to the test images (database) using the following steps:

- The same step 1 to step 3 in database construction.
- An image must be rotated by the angle difference between Template image and test images.
- Images are cropped to the size of 128x128 pixels (a core point is at the center).
- Images, size 128x128 pixels, divided into 64 sub-images, with the size 16x16 pixels.
- Each image is transformed via a 2D-DFT.
- Determine the values of the spectrum,spectrum phase and the line angles of each sub-image.
- Matching each value of the templates with values of the test images by correlation or corr2 technique.
- Find the values of the spectrum,spectrum phase and the line angles of each sub-image.
- Matching each value of the templates with values of the test images by correlation or corr2 technique.
- The value the similarity average of spectrum between the template image and test images between 0.75 to 1, and the angle line value equal or less than $\pm 0.5^{\circ}$

IV. EVALUATION AND RESULTS

We have set up 16 template images from 4 group patterns (4 images for each pattern). Those patterns are whorl, left loop, right loop, and tents. As such we have 97 individuals including test images and one individual. There are in fact 3 images come from the same image, each image is difference angle or difference position. All of images in the database to test images 291 images. This is to check the consistency of the algorithm as well as to widen the testing domain. The FVC 2004 DB1-A database set has been employed in this experiment. To measure our algorithm performance, we also have the FVC2002 DB2- A. We have set up 10 template's images from 3 group pattern and we have to test all, and each template is a 4 templates from left loop, 4 templates from right loop, and 2 templates come from the whorl, and we have to include 3 images come from the same template and each image they have difference position or different angles. In depth, we have investigated 2 issues, namely; I) find the values of the spectrum , spectrum phase and values of the line angles after transforming images, II) Find average the value of the angles of the template and the test images, III) Correlation the value of the spectrum, spectrum phase and average subtracts the value of the angle between the two images. From this evaluation the results are shown in table I and II respectively.

TABLE I. FVC 2004-DB1-A MATCHING RESULTS

Pattern	*Avg. Values, spectrum* > 0.75 , *angles* ≤ ±0.5°		
	Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	41.15	0.336	1.56
Left loop	41.82	0.57	1.27
Right Loop	44.61	0.63	1.34
Tent	39.11	0	2.02
Avg%	41.67	0.384	1.54

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

TABLE II. FVC 2002-DB2-A MATCHING RESULTS

Pattern	*Avg. Values, spectrum* > 0.75, *line angles* $\leq \pm 0.5°$		
	Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	9.53	0	0
Left loop	8.67	1.66	1.66
Right Loop	7.67	1	1.66
Avg%	8.62	0.88	1.75

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

To demonstrate that the proposed a fingerprint matching scheme based on 2D Fourier transform method. We can have some advantages compared to the methods reported in the literature [13]. [13] have used FVC 2002 DB2 and DB3, as their database. 10 individuals and 8 images per person are deployed. Their matching method is based on the minimum Euclidean distance between two feature vectors. The method proposed by [14] used FVC2004 DB1-A as their work bench. There are 800 fingerprints from 100 different fingers. The technique to measure the algorithm performance has employed fingerprint orientation model based on weighted 2D Fourier expansion (W-FOMFE). The gradient-based algorithm was the the main tool, and the error from the noise can be eliminated using the Harris-corner strength. To make a comparison, we used 97 individual images (35 left-loops, 22 right-loops, 18 tents, and 22 whorls), and included three images come from the same individual all of the images in the database. Likewise, we have tested 291 images constructed with 16 individuals from FVC2004-DB1A. Secondly, to invcstigatc the rotation sensitivity, we used 10 individual images, (4 left-loops, 4 right-loops, and 2 whorls), including three images come from the same individual, each image has difference angles or difference position. We applied the test to two databases with the same algorithm. The results are shown in table III.

TABLE III. MATCHING OF DIFFERENT WORKS

Matching Scheme	Results		
	Avg. Computation time (ms)	*% FAR*	*% FRR*
Ref. [13]	38[a]	1	3.6
Ref. [14]	24[a]	3.6	6.57
Proposed FVC2004-DB1-A	8,11[a]	0,384	1.54
Proposed FVC2002-DB2-A	5,22[a]	0,88	1,75

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

According to the results shown in table III, we can see that we have obtained is fairly good. Our proposed method is superior over [13] and [14]. The false reject rate is not so severe and considered to be a positive error, since those reject samples could be re-examined by some other methods even by using an expert.

Our method is superior over the techniques [13,14], and when we compare the recluse from two databases first data fairly better than second databases. We hope that we can improve the FRR after patient fine tuning the threshold as well as increasing the total matching number.

V. CONCLUSION

In this paper we proposed an alternative method for fingerprint matching by using 2D Fourier transform features. We have applied our technique to two databases (FVC2004-DB1-A and FVC2002-DB2-A). The result confirms to us that ours works well and offers considerably better performance compared to the similar publication. The main weak point of our method is that it has assumed the availability of core point which may be not exist in some types of the supplied image. We hope we can find some alternative approaches to further improve the performance of this work further.

ACKNOWLEDGEMENT

We would like to acknowledge to the Asian University Network (AUN/SEED-Net) for the financial support of one of the authors (Mr. Souksamay Insankeovilay) from National University of Laos (NUOL), LAO PDR for his graduate study at King Mongkut's Institute of Technology Ladkrabang (KMITL), THAILAND.

REFERENCES

[1] Jayant V. Kulkarni, Bhushan D. Patil, Raghunath S.Holambe "Orientation feature for fingerprint matching"J.V. Kulkarni et al./ Pattern Recognition 39 (2006) 1551 – 1554

[2] Yan Xia Anthony Tung Shuen Ho YanWen Ji"A Novel Wavelet Stereo Matching Method to Improve DEM Accuracy"

[3] Line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4): 302–313, April 1997. A.K. Jain, S. Prabhakar,L. Hong and S. Pankanti, "Filter bank Based fingerprint matching," IEEE Trans. Image Processing, 9(5):846–859, 2000

[4] Y. He, J. Tina, X. Lou and T. Zhang, "Image enhancement and Minutiae matching in fingerprint verification", Patti. Reclog. Letts, no, 24, 2003, pp. 1349-1360.

[5] L. Hong, Y. Wan and A. K. jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", IEEE Transaction on PAMI, Vol. 20,No. 8, pp. 777-789, August 1998

[6] Muhammad Umer Munir and Mohammad Younas Javed, "Fingerprint Matching using Gabor Filters", National Conference on Emerging Technologies 2004

[7] M. Taco and P. Kuosmanen, "Fingerprint matching using an Orientation based minutia descriptor," IEEE Trans. On Patti. Analyst and Mach In tell, vol. 25, no. 8, 2003, pp. 1009–1014.

[8] S. Tachaphetpi boon and T. Amornraksa, "A Fingerprint Matching Method Using DCT Features", Proceedings of ISCIT2005, pp. 446-449.

[9] S. Tachphetpiboon and T. Amornraksa, "Applying FFT Features for Fingerprint Matching," IEEE Trans., 2006.

[10] Xiao-Yuan Jing and David Zhang, "A Face and Palmprint Recognition Approach Based on Discriminant DCT Feature Extraction", IEEE Transaction on Systems, Man and Cybernetics-Part B: Cybernetics, Vol.

[11] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar "Fingerprint Template Protection: From Theory to Practice"

[12] Sharat Chikkerur, Alexander N. Cartwright, Venu Govindaraju "Fingerprint enhancement using STFT analysis" Received 16 August 2005; received in revised form 2 May 2006; accepted 25 May 2006

[13] A Fingerprint Orientation Model Based on 2D Fourier Expansion (FOMFE) and Its Application to Singular-Point Detection and Fingerprint Indexing Yi Wang, Student Member, IEEE, Jiankun Hu,

[14] Xunqiang Tao, Xin Yang, Kai Cao, Ruifang Wang, Peng Li and Jie Tian "Estimation of fingerprint orientation field by weighted 2D fourier expansion model"

The 5th Biomedical Engineering International Conference

BMEiCON 2012

December 5 - 7, 2012
UbonRatchathani, Thailand
& Champasak, Laos

Fingerprint Matching Using the 2D-DCT and 2D-DFT

Souksamay Insankeovilay
International College
King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand
Email: souksamay.en@hotmail.com

Somsak Choomchuay and Kazuhiko Hamamoto
Department of Electronic Engineering, Faculty of Engineering,
King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand
Information Media Technology, School of Information
Technology and Electronics Tokai University, Tokyo, Japan
Email: kchsomsa@kmitl.ac.th; hama@keyeki.cc.u-tokai.ac.jp

***Abstract*- In this paper, we propose fingerprint matching techniques using the 2D DFT features as well as 2D DCT features. In the procedure, we crop input images from the size of 480x640 pixels into 128x128 pixels, and then divide the image into 64 sub-images. Each sub-image (a tile) holds the size of 16x16 pixels. Each tile is transformed, and its spectrums are obtained. The achieved spaectrums are then compared between those of a test tile and those of a template tile. A commonly known FVC-2004 (DB-1A) database has been used in our investigation. Upon the results, can see that this method offers better performances (FAR, FAR, and computation times) when compared to other individual matching reported in the literatures. Our method is not sensitive to the rotational effect. However, the proposed technique is still based on the availability of core point. Therefore, the performance can be deterior if the core point cannot be located or improperly located.**

***Index Terms*[1]—Fingerprint matching, 2D DCT, 2D DFT**

I. Introduction

The Biometrics are used to recognize a person and the term is derived from the Greek word bio (life) and metric (measurement). The biometric parameters are broadly classified as Physiological characteristics of a person such as face, fingerprint, palm print, Iris, DNA etc. and behavioral characteristics of human beings like signature, voice, keystroke, gait etc. The biometric system operates as verification mode or an identification mode depending on the requirement. The verification mode validates a person with the template. The identical model recognizes an identity by performing matching against multiple templates. The biometrics are more secure compared to the traditional methods such as PIN (Personal Identification Number), for verifying a person.

Fingerprints have been used as most popular biometric authentication and verification measure because of high acceptability and immutability refers to the persistence of the fingerprints over time whereas uniqueness is related to the individuality of ridge details across the whole fingerprint image. Fingerprint classification is an important step in any fingerprint identification system because it reduces the time taken in identification of fingerprints. Classification allows test fingerprint to be coarse matched against a database. The fine matching can be performed by examining the fine feature of a fingerprint .These are, for instance, singular point, minutiae and so on. Direct measuring the minutiae features technique is quite popular according to its accurate and reliable result. However, on the dim side, such a technique requires large database as well as computational workload.

In our method we have investigated the fingerprint fine feature in the transform domain. 2D-DFT and 2D-DCT are 2 transforms that we were looking at. A bigger image have been cropped around the center suggested by the corepoint location. Further divided tiny tiles were applied to the 2D transform. The spectrum of the corresponding tiles are compared via normalized cross correlation process.

The rest of this paper is organized as follows. In the next section we will give a brief procedure of 2D discrete cosine transform (DCT) and 2D discrete Fourier transforms (DFT) matching. Followingly, matching steps are given to certain details in section III. Algorithm evaluations with some demonstrated results are elaborated in section IV. Finally the work is concluded in section V.

II. 2D-DFT and 2D-DCT

A. Two Dimensional Fourier Transforms (2D-DFT)

Direct minutiae matching is certainly the most well-known and widely used method according to its higher recognition accuracy

The term image transform refers to a class of unitary matrices used for representing images. Images are expanded in terms of a discrete set of basis arrays called basis images [4]. Energy conservation, energy compaction, decoration is the important properties of these transforms. Image transform is basically a higher dimension Discrete Fourier Transform (DFT).

The two dimensional DFT of an $M \times N$ image $f(x,y)$ is a separable transform defined as

$$F(u,v) = \mathbb{F}[f(x,y)] = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp\left\{-2j\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (1)$$

The u and v are frequency component of each dimension. Although the input is a real sequence, the transformed sequence is a complex sequence that holds both real part and

This work is partially supported by AUN/SEED-Net program under the Research Collaboration (RC) scheme.

978-1-4673-4892-8/12/$31.00 ©2012 IEEE

imaginary part. The Fourier spectrum magnitude and spectrum phase can be given by eq. (2.1) and eq. (2.2) respectively.

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \tag{2.1}$$

$$\varphi(u,v) = \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \tag{2.2}$$

After transformation, the phase values provide little information, only magnitudes are further considered for our application.

B. Two Dimensional Discrete Cosine Transform (2D-DCT)

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG (The Joint Photographic Experts Group). The discrete cosine transform (DCT) is closely related to the discrete Fourier transform. It is a separable linear transformation; that is, the two-dimensional transform is equivalent to a one-dimensional DCT performed along a single dimension followed by a one-dimensional DCT in the other dimension. With the dimension of $M \times N$, the definition of the type-II two-dimensional DCT of an input image A and output image B can written as shown in Eq. (5). Here m,n and p,q are index along each dimension of A and B respectively.

$$B(p,q) = C_p C_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A(m,n)\cos\left\{\frac{p\pi}{2N}(2m+1)\right\} \left\{\cos\frac{q\pi}{2M}(2n+1)\right\} \tag{3}$$

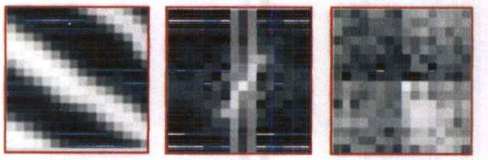
Where

$$C_p = \begin{cases} \dfrac{1}{\sqrt{M}}, & \text{for} \quad p = 0 \\ \sqrt{\dfrac{2}{M}}, & \text{for} \quad 1 \le p \le M-1 \end{cases} \tag{4}$$

And likewise C_q.

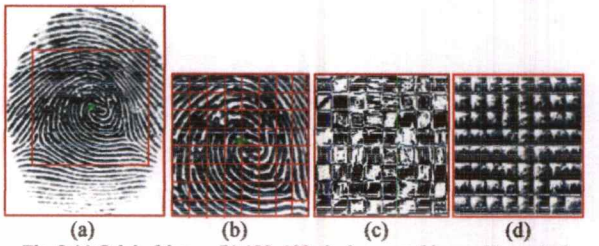
If the DCT is applied to the real data, the result is also real. The DCT tends to concentrate information, making it useful for image compression applications. We have also considered the transformed information as a feature for fingerprint matching.

The cropped 128×128 pixel image is further divided into 64 sub-images of each with the dimension of 16×16 pixels. Both DFT and DCT are applied to each sub-image. The resulted transformed images are illustrated below.



(a) (b) (c)

Fig. 1 (a) A portion of fingerprint images, size 16x16 pixels. (b) Resulted 2D Fourier transform and (c) Resulted 2D discrete cosine transform



(a) (b) (c) (d)

Fig. 2 (a) Original image (b) 128x128 pixels cropped image (c) resulted 2D DFT and (d) resulted 2D DCT

The feature of a sub-image is in fact defined alternatively in its DFT or its DCT domain. To make a justification whether the sub-image of the test image is actually the same with its corresponding of the template sub-image. At this stage, to examine their similarity, we are focusing to the cross correlation.

For the image "A" with the dimension $M_a \times N_a$ and the image "B" with the dimensions $M_b \times N_b$, the equation for the two-dimensional discrete cross-correlation can be given by:

$$r(i,j) = \sum_{m=0}^{M_a-1}\sum_{n=0}^{N_a-1} A(m,n)\,B(m+i,n+j) \tag{5}$$

Where $0 \le i < M_a + M_b - 1$ and $0 \le j < N_a + N_b - 1$. It should be noted that the resulted image is with the dimensions of twice larger compared to the original images. We also do not want to use all available value. In addition, the resulted minimum peak can be affected by the brightness level of the original images. Instead, we just need the maximum value that the brightness levels have been taken into account. Fortunately, a normalized cross correlation operation given by the eq. (6), below can offer what we need.

$$r = \frac{\sum_m\sum_n \left(A_{mn} - \overline{A}\right)\left(B_{mn} - \overline{B}\right)}{\sqrt{\left(\sum_m\sum_n \left(A_{mn} - \overline{A}\right)^2\right)\left(\sum_m\sum_n \left(B_{mn} - \overline{B}\right)^2\right)}} \tag{6}$$

The score given by 2 most similar sub-images can be close to +1, whilst that of the different images is very low. The average matching score can then be easily calculated based on the score of each sub-image matching. The highest average score implies the most similarity of those two cropped images.

$$S_{Avg} = \frac{1}{64}\sum_{i=1}^{64} r_i \qquad (7)$$

Doing the transformation to the image is in fact trying to look into the image in the different point of view. In the transformed domain, the spectrum feature can define well the uniqueness of the fingerprint that is hard to be of served in the spatial domain. However, under this assumption, the orientation as well as the resolution of the images must be the same. The resolution can be controlled in the acquiring process. Although the orientation of the finger can be controlled during the scanning process, the exact orientation of the acquired fingerprint is still not ensured. To overcome the rotation problem, the raw image must be rotated before segmentation or transformation. Obtained with the core point we can find a different angle between the two images. That enables us to rotate the sampled image to the same orientation as that of the referenced non-rotate image [9]. We can find the raw image angle or image position by step 3 to step 5 in database construction. If given θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled) image, then θ_3 is the angle differences between those two images. We then have to rotate the template image by (θ_3) degree, ($\theta_3 = \theta_2 - \theta_1$). Shown in the Fig.3 below.

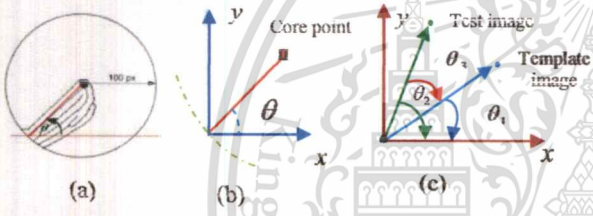


Fig3.(a) and (b) Image angle or image position ($\theta = 43.76°$), (c) Angle of the template rotated

For a normal scanned fingerprint image, the core point has generally appeared at the center of the image. With such an assumption, the major ridge and valley information are seemed to be around the core point. We were then trying to find the spectrum feature of those areas. To such a reference core point the 2D-Discrete Fourier transform and 2D discrete cosine transforms is applied to 64 sub-image of 16x16 pixels.

According to the symmetry properties of the DFT and DCT, some left side and right side image can offer the very similar spectrum values. That can lead to the wrong justification. To avoid the ambiguous, the line angle must be computed and store for further use. We find the value of the line angle from 64sub-image and then find Average value from 64-sub-image. And we compare the similarity of two images by subtraction the average value of the template image and the average value of the test image.

In a clever way, we also can avoid the the said above line angle computation. If the sub_image are stored in sequence the matching sequential with no need of line angle information.

III. Fingerprint Matching Procedure

There are two folds in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. Details are given as follows:

A. Database Construction.

In practice there could be a huge fingerprint pattern stored as database. To identify the case an anonymous pattern must seek its most similar to one or few database patterns. In our approach database construction is as follows:

1) The raw image is enhanced with Gabor filtering
2) Mark the core point of the enhanced imaged using point care technique
3) Define the circle of interest of which the radius of100 pixel. The core point is taken as a center of this circle.
4) Draw a box of 15x15 pixels around the core point.
5) The lines connected between the box and the circumstance of the circle are considered for angle measurement. Average values were taken
6) Determine the main ridge angle (respective to the vertical line). The obtained angle is stored in the database together with the image name.
7) Images are cropped to the size 128x128 pixels (a core point is at the center).
8) The 128x128 pixel image is divided into 64 sub-images, each is with the size of 16x16 pixels.
9) Each sub-image is transformed via a 2D-DFTand 2D-DCT
10) Determine the value of the spectrum components. There are 256 components for each sub-image. For the DFT transformation, spectrum magnitude is stored.
11) The location where it is in the 8x8 sub-image grid, together with its spectrum values are additionally stored. This is how the database is formed.

B. 2D-DFT and 2D-DCT Matching steps .

The specimens (test) are then compared to the test images (template) using the following steps:

1) Image occurring.
2) Enhancement and core point determination. This is the same as step 1 to step 5 in database construction.
3) Determine the angle of this test (respect to the vertical line) image. Compute the different angle between the template image and the test image. Rotate the test image by the degree of the angle difference.
4) Images are cropped to the size 128x128 pixels (a core point is at the center).
5) This 128x128 pixel image is then also divided into 64 sub-images, each of with 16x16 pixels in size.
6) Perform both 2D-DFT and 2D-DCT to the sub-image

7) Find the the spectrum values (256 values).

8) Matching the value of the spectrum, via normalized cross correlation. The matching score is obtained.

9) Average matching score of those 64 sub-images can tell us how similar those 2 images.

IV. Evaluation and Results

The FVC 2004 DB1-A database set has been employed in this experiment. We have set up 16 template images from 4 group patterns (4 images for each pattern). Those patterns are whorl, left loop, right loop, and tents. These are included in 97 individual images (35 left-loops, 22 right-loops, 18 tents, and 22 whorls). Each individual holds 3 different scans. Therefore, there are 291 images involved in our test. This amount of images is large enough to check the consistency of the algorithm as well as to widen the testing domain. As detailed in the previous sections; the matching has involved 3 main steps, i.e., spectrum finding, spectrum matching and average value computation. The matching decision is made upon the obtained average value. The merit of the algorithm is basically stated by its fault acceptant rate and fault rejection rate. Given as an example, matching score averarage values of samples obtained from a DFT process (a certain template) are plotted as shown In Fig. 5. The matching decision can be made upon the observation. In this case, somewhere the value around 0.75 seems to be a good choice.

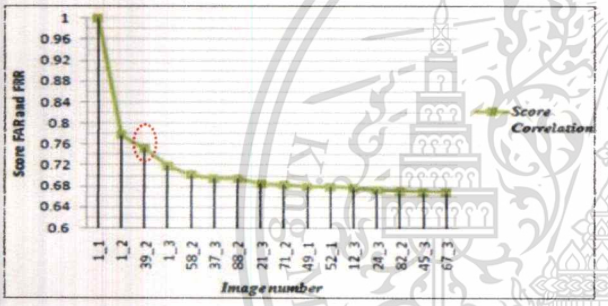


Fig.5 Average values of the correlation score of different images

The template is infact the image 1_1. The decision at the value of 0.75 can result in image 1_2 and image 39_2 to be accepted. However, as the image 1_2 is a variation of the image 1_1. The decision is then wrong for the image 39_2. This is a case of fault acceptance. For the whole testing, the evaluation result is shown in table I, II below.

TABLE I. FVC 2004-DB1 WITH 2D-DFT

Pattern	Number of Templates	Number of test images	*Avg. Values, spectrum* > 0.75 , *line angles* ± 0.5°		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	66	41.15	0.336	1.56
Left loop	4	105	41.82	0.57	1.27
Right Loop	4	66	44.61	0.63	1.34
Tent	4	54	39.11	0	2.02
Avg%	16	291	8.59	0.384	1.54

TABLE II. FVC-2004DB1-A WITH 2D-DCT

Pattern	Number of Template	Number of Test image	*Avg. Values, spectrum* > 0.75 , *line angles* ± 0.5°		
			Avg. Computation Time (ms)	*% FAR*	*% FRR*
Whorl	4	66	26.01	0.67	1.34
Left loop	4	105	25.59	0.67	1.01
Right Loop	4	66	26.11	1.01	1.01
Tent	4	54	25.44	1.34	1.34
Avg%	16	291	5.22	0.9225	1.175

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

From the FAR and FRR result given in table I and II above, it is quite clear that the spectrum observation technique proposed in this investigation is paractically good. It can have some advantages compared to the methods reported in [15]. In such a literature, the matcher has been evaluated on similar public-domain databases, namely, FVC2002 DB1, DB2 and FVC2006 database DB2. 100 fingers with 8 impressions per finger were taken from FVC2002. Likewise, 140 fingers with 12 impressions per finger were taken form FVC2006-DB2. The following parameters are set: v_{min}=0.01, v_{max}=0.25, N_v=64, N_θ=32, R=100 pixels, η=0.55 and K=5. The performance of the matcher is based on both global and local minutiae phase spectrums. Reported by [16], they use FVC 2002 DB2 and DB3, database consisted of fingerprints of 10 individuals and 8 images per person. The matching is based on the minimum Euclidean distance between two feature vectors. In short, [15] and [16] have proposed a minutiae-based matching while we are working on spectrum matching. The obtained performances are shown in Table III below.

TABLE III. MATCHING OF DIFFERENT WORKS

Matching Scheme	Performance		
	Avg. Computation time (ms) /image	*% FAR*	*% FRR*
Ref. [15]	22	2.6	4.9
Ref. [16]	38	1	3.6
2D-DFT	8.59	0.384	1.54
2D-DCT	5.22	0.9225	1.751

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

According to the results shown in table III, we can see that we have obtained better results compared to others. The proposed method is superior over those reported by [15] and [16]. The false reject rate is not so severe and considered to be a positive error, since those reject samples could be re-examined by some other methods even by using an expert. We can also use the given below evaluating equation to compare our technique with other proposed algorithm that is:

$$FAR = \frac{false\_accepted\_num}{total\_matching\_num} \times 100\%$$

$$FRR = \frac{false\_rejected\_num}{total\_matching\_num} \times 100\ \%$$

From table III. We can see the comparison results in the Fig.6 below.

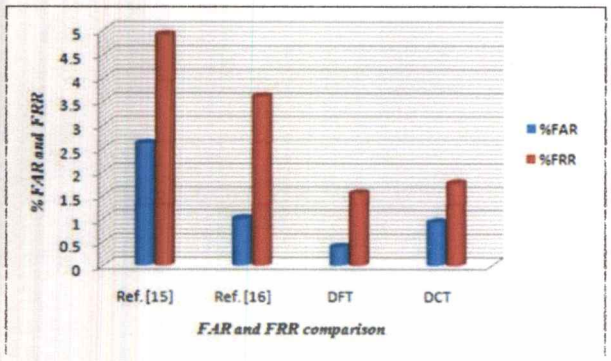


Fig.6 FAR and FRR comparison

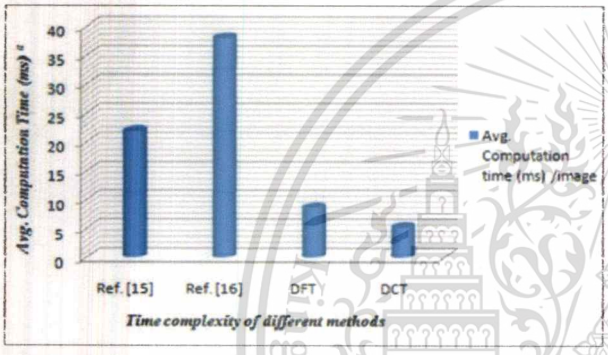


Fig.7 Time complexity of different methods

The average computation times of our method is faster than the techniques noted in [15 and 16]. In our case we also found that the DCT is about twice faster than DFT. However DFT is superior over DCT for FAR and FRR justification.

IV. Conclusion

In this paper we proposed an alternative method for fingerprint matching, spectrum matching technique. 2D discrete Fourier transforms and 2D discrete cosine transform were investigated. The FAR and FRR results are better than the minutiae-based techniques proposed in the literatures. DCT based is faster than its DFT companion. However, DFT can offer slightly better FAR and FRR performance. The 8x8 tiny tiles of 16x16 pixels are fed to the transform machine before the spectrum of corresponding tile are correlated. Of those 4 pattern under tested, the tent one holds rather high percents of FAR and FRR compared to others. This is because the core point cannot be determined precisely. The ridge lines do not hold the sharp turn. Therefore the main drawback of the algorithm is its dependency on the availability of the reference point (core point). We hope we can find some alternative approaches to improve the precision of core point detection as well as seeking other alternatives that less rely on the availability of the reference point.

Acknowledgement

We would like to express our gratitude to the Asian University Network (AUN/SEED-Net) for the financial support of one of the authors (Mr: Souksamay Insankeovilay) from National University of Laos (NUOL), LAO PDR for his graduate study at King Mongkut's Institute of Technology Ladkrabang (KMITL), THAILAND.

References

[1] Jayant V. Kulkarni, Bhushan D. Patil, Raghunath S.Holambe "Orientation feature for fingerprint matching"J.V. Kulkarni et al./ Pattern Recognition 39 (2006) 1551 – 1554

[2] Yan Xia Anthony Tung Shuen Ho YanWen Ji"A Novel Wavelet Stereo Matching Method to Improve DEM Accuracy"

[3] Line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, 19 (4): 302–313, April 1997. A.K. Jain, S. Prabhakar,L. Hong and S. Pankanti, "Filter bank Based fingerprint matching," IEEE Trans. Image Processing, 9 (5):846–859, 2000.

[4] Y. He, J. Tina, X. Lou and T. Zhang, "Image enhancement and Minutiae matching in fingerprint verification", Patti.Reclog. Letts, no. 24, 2003, pp. 1349-1360.

[5] L. Hong, Y. Wan and A. K. jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", IEEE Transaction on PAMI, Vol. 20,No. 8, pp. 777-789, August 1998

[6] Muhammad Umer Munir and Mohammad Younas Javed. "Fingerprint Matching using Gabor Filters", National Conference on Emerging Technologies 2004

[7] S. Tachaphetpiboon and T. Amornraksa, "A Fingerprint Matching Method Using DCT Features", Proceedings of ISCIT2005, pp. 446-449.

[8] S. Tachphetpiboon and T. Amornraksa, "Applying FFT Features for Fingerprint Matching," Proc. of Wireless Pervassive Computing Int. Symposium. 2006.

[9] Yuh-Ming Huang, ja-Ling Wu, and Chaou-TingHsu " A Refined Fast 2-D discrete cosine transform Algorithm with regular butterfly structure". Pp 376-383.IEEE Transaction on Consumer Electronics, Vol.44, No.2, May, 1998.

[10] Xiao-Yuan Jing and David Zhang. "A Face and Palmprint Recognition Approach Based on Discriminant DCT Feature Extraction", IEEE Transaction on Systems, Man and Cybernetics-Part B: Cybernetics, Vol. 34, No. 6, December 2004.

[11] S. Tachaphetpi boon and T. Amornraksa, "A Fingerprint Matching Method Using DCT Features", Proceedings of ISCIT2005, pp. 446-449.

[12] D. Bennet , Dr. S. Arumuga Perumal" Fingerprint Matching Using Hierarchical Level Features" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011.

[13] Sharat Chikkerur, Alexander N. Cartwright, Venu Govindaraju "Fingerprint enhancement using STFT analysis" , Elsever Ltd. (for the pattern recognition society), pp. 198-211, 2006.

[14] XunqiangTao, Xin Yang, Kai Cao, Ruifang Wang, Peng Li and Jie Tian, "Estimation of fingerprint orientation field by weighted 2D Fourier expansion model". DOI 10.1109/ICPR.2010.312, pp. 1253 -1256.

[15] Karthik Nandakumar, "Fingerprint Matching Based On Minutiae Phase Spectrum" Institute for Infocomm Research, A*STAR, Fusionopolis, Singapore, pp 216-221, 978-1-4673-0397-2/12, 2012 IEEE.

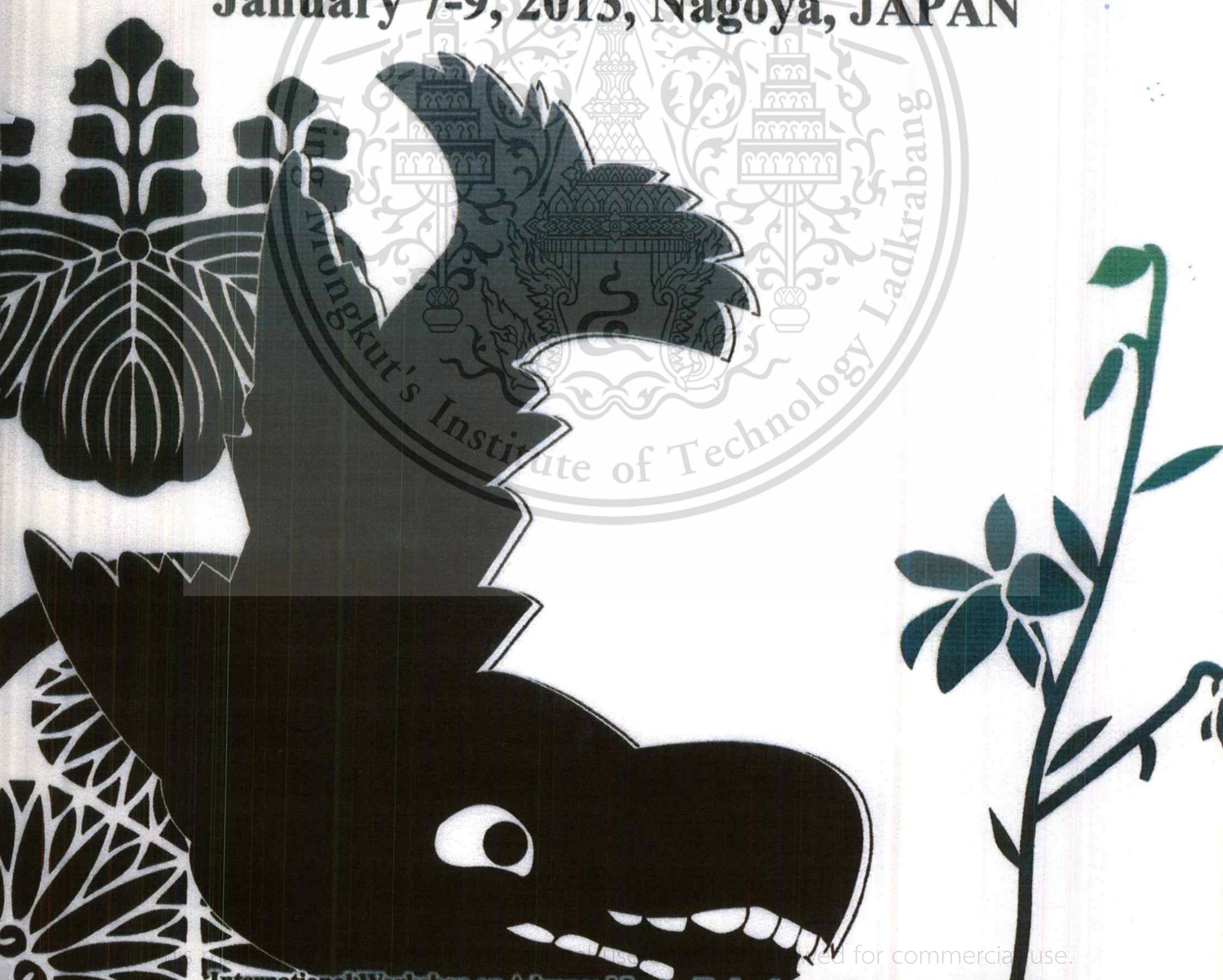
[16] Y. Wang, J. Hu and D. Philips. A Fingerprint Orientation Model. Based on 2D Fourier Expansion (FOMFE) and Its Application to Singular-Point Detection and Fingerprint Indexing. *IEEE Trans. Pattern Anal. Mach. Intell.*, 573–585, 2007.

Abstracts of

IWAIT 2013

International Workshop on Advanced Image Technology

January 7-9, 2013, Nagoya, JAPAN



International Workshop on Advanced Image Technology Organizing Committee
Furo-cho, Chikusa-ku, Nagoya, 464-8601, Japan

Fingerprint Matching Using NCC and 2D-DFT

Souksamay Insankeovilay
International College, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, THAILAND
Email:souksam.en@hotmail.com

Somsak Choomchua
Department of Electronics, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, THAILAND
Email:kchsomsa@kmitl.ac.th

Kazuhiko Hamamoto
Information Media Technology, School of Information Technology and Electronics Tokai University, Tokyo, JAPAN Email: hama@keyeki.cc.u-tokai.ac.jp

Abstract _ **this paper we have proposed a fingerprint matching using Normalized cross correlation (NCC) and two dimensional Discrete Fourier transform (2D-DFT). In this method to measure the performance of the algorithm we have to test two step NCC step and second step we used high score or who past the first step to process with 2d-DFT again. Moreover, our method doesn't sensitive to rotational effect. The proposed technique is, however, based on the availability of core point. The technique fails if the core point cannot be located or incorrectly located. The matching is performed based on the NCC score and two dimensional Discrete Fourier transforms magnitude, matching of the pattern around core point. Using this matching, we can improve the FAR and FRR. Images under tested are those obtained in FVC-2004 (DB-1A). There are 16 templates (4 groups of 4 patterns each). We have included 3 images come from the same individual each image has difference position or a different angle, in our experiment. Upon the investigation, we have obtained 0% FAR, 1.45% FRR .**

Keywords-component, formatting, NCC matching, 2D-DFT.

I. NCC INTRODUCTION

Normalized cross-correlation is computed in between the two resultant common regions t and f from the template fingerprint t and registered testing fingerprint f respectively using the Matlab function normxcorr2 to get the normalized cross-correlation coefficients as the result.

Machine–based data processing becomes more and more important in the decade of information technology, there are several vital needs in data consistency and data security. Moreover, the importance of the tracking (or tracing) is also extended to the person who is the owner of such data, no matter the one who sends it or the one who receives it. Personal identification by mean of fingerprint pattern is one of the most popular and reliable use Biometric techniques. This is because fingerprint holds many desirable features such as universality, permanence, collect ability, and distinctiveness. Personal identification based on fingerprint matching is now, therefore, popular in a wide range of applications. Fingerprint characteristics are basically divided into five patterns, are of them is generally features of any fingerprint based on which Classification of fingerprints into one of defined classes is performed before matching.

This work is partially supported by AUN/SEED-Net program under the Research Collaboration scheme

This will cause the matching operation to be performed faster. Classes are generally classified into: Left loop, Right loop, Whorl (including dual loop), Arc, and Tent. These features are illustrated in Fig. 1

(a) Left Loop (b) Right Loop (c) Whorl (d) Tent or Arc

Fig 1. Fingerprint Patterns

NCC matching on the other hands, offer good registration in particular when the matching area is fairly small. However, the technique consumes large storage and computing resources. The technique works regardless the availability of the standard point neither core point. Variance feature of orientation field matching has been proposed in [1,2]. based matching methods proposed by [5,6] have shown their better recognition rates. Normalized cross correlation (NCC) has been applied together with group delay spectrum (GDS) and dynamic programming (DP) for line scan matching [7] The performance of a fingerprint recognition method involves a trade off among different performance measures, i.e.; accuracy, efficiency, template size, and so on. Different applications may desire different properties in the fingerprint matching algorithms (e.g., Template size, matching speed, memory requirements, and etc.).

Fingerprints have been used as most popular biometric authentication and verification measure because of high acceptability and immutability refers to the persistence of the fingerprints over time whereas uniqueness is related to the individuality of ridge details across the whole fingerprint image. Fingerprint classification is an important step in any fingerprint identification system because it reduces the time taken in identification of fingerprints. Classification allows test fingerprint to be coarse matched against a database. The fine matching can be performed by examining the fine feature of a fingerprint .These are, for instance, singular point, minutiae and so on. Direct measuring the minutiae features technique is

quite popular according to its accurate and reliable result. However, on the dim side, such a technique requires large database as well as computational workload.

II. NCC MATCHING ALGORITHM

The main purpose of using this procedure is to evaluate the coarse matching of the patterns, for best matching result; size and orientation of the detail image are assumed to be the same. Generally, a correlation method is a technique which can show how strongly pairs of variables are related. The result indexed by a correlation coefficient value of which -1.0 to +1.0. The close range of +1, the more closely one variable is related to the other. The correlation between two signals (cross-correlation) is a standard approach to find out how the two signals are related. It has shown its best applications in pattern recognition and cryptanalysis. Of its kinds, normalized cross correlation (NCC) has also been used extensively in machine vision for industrial inspection including defect detection in complicated images

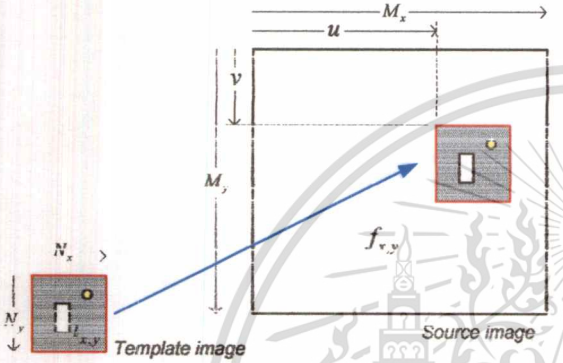


Fig2. Matching of template t into the source image f

Shown in Fig. 2. Let f be a test image (source image) have the size, ($M_x \times M_y = 640 \times 480$ *Pixels*) and t be a template image have the size, ($N_x \times N_y = 128 \times 128$ *Pixels*), we want to seek any similarity of the template t to any portion of test images f. In this particular case, the image size t is smaller or equal to f a simple method for measuring similarity or mismatch performed by taking the absolute difference image over template image t and given the test image f over a specific region.

If we take the sum of difference square between template and give image f over a region offset by u and v in each dimension, then we can get:

$$d^2_{f,t}(u,v) = \sum_{x,y} \left[f(x,y) - t(x-u,y-v) \right]^2 \qquad (1)$$

The above equation (1) can be expanded to,

$$d^2_{f,t}(u,v) = \sum_{x,y} \begin{bmatrix} f^2(x,y) - 2f(x,y)t(x-u,y-v) \\ +t^2(x-u,y-v) \end{bmatrix} \qquad (2)$$

The term $\sum_{x,y} \left[t^2(x-u,y-v) \right]$ is fixed for a given template image. Likewise, the term $\sum_{x,y} \left[f^2(x,y) \right]$ is also approximated to be fixed. Then the cross correlation expression given in (3) will give the degree of similarity.

$$c(u,v) = \sum_{x,y} \left[f(x,y)t(x-u,y-v) \right] \qquad (3)$$

From implementation of (3) the problem is to determine the position of a given pattern in a two dimensional image f. Let $f(x,y)$ denote the intensity value of the image f of the size $M_x \times M_y$ at the point $(x,y), x \in \{0,\ldots,M_x - 1\}$ and $y \in \{0,\ldots,M_y - 1\}$ the pattern is represented by a given template t of the size $N_x \times N_y$. A common way to calculate the position u,v of the pattern in the image f is to valuate the normalized cross correlation value γ at each point u,v for f and the template t, which has been shifted by u steps in the x direction and by v steps in the y direction Equation (4), gives a basic definition for the normalized cross correlation coefficient.

$$\gamma(u,v) = \frac{\sum_{x,y} \left[f(x,y) - \bar{f}_{u,v} \right] \left[t(x-u,y-v) - \bar{t} \right]}{\sqrt{\sum_{x,y} \left[f(x,y) - \bar{f}_{u,v} \right]^2 \sum_{x,y} \left[t(x-u,y-v) - \bar{t} \right]^2}} \qquad (4)$$

Where $\bar{f}_{u,v}$ And $\bar{t}$ are the means of $f(x,y)$ and t respectively.

$$\bar{f}_{u,v} = \frac{1}{N_x N_y} \sum_{x=u}^{u+N_x-1} \sum_{y=v}^{v+N_y-1} f(x,y) \qquad (5)$$

With similar notation $\bar{t}$ is the mean value of the template t the denominator in (4) is the variance of the zero mean image function $f(x,y) - \bar{f}_{u,v}$ and the shifted zero mean template function $t(x-u,y-v) - \bar{t}$ due to this normalization $\gamma(u,v)$ is independent of changes in brightness or contrast of the image, which are related to the mean value and the standard deviation.

And

$$\bar{t} = \frac{1}{N_x N_y} \sum_{x=u}^{u+N_x-1} \sum_{y=v}^{v+N_y-1} t(x,y) \qquad (6)$$

In practice to avoid excessive computation, fast and approximated techniques are used to compute (4) by [9,10].

III. 2D-DFT Introduction

In 2D-DFT we have investigated the fingerprint fine feature in the transform domain. 2D-DFT is transformed that we were looking at. A bigger image has been cropped around the center suggested by the core point location. Further divided tiny tiles were applied to the 2D transform. The spectrum of the corresponding tiles is compared via cross-correlation process. The two dimensional DFT of an $M \times N$ image $f(x,y)$ is a separable transform defined as.

$$F(u,v) = \mathbb{F} \qquad \mathbb{F} = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp\left\{-2j\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \qquad (7)$$

The u and v is a frequency component of each dimension. Although the input is a real sequence, the transformed sequence is a complex sequence that holds both real part and imaginary part. As such the Fourier spectrum (magnitude) can be computed.

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \qquad (8.1)$$

And spectrum angles can be computed by

$$\varphi(u,v) = \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \qquad (8.2)$$

After transformation, the phase values provide little information, only magnitudes are further considered for our application.

This step we measure the performance by Cross-correlation-based fingerprint matching. Use the value of the spectrum, and the value of the line angles between the template images and test images. If the matrix A has dimensions (Ma, Na) and matrix B has dimensions (Mb, Nb). The equation for the two-dimensional discrete cross-correlation is.

$$C(i,j) = \sum_{m=0}^{Ma-1} \sum_{n=0}^{Na-1} A(m,n).conj(Bm+i, n+j) \qquad (9)$$

where $0 \le i < Ma + Mb - 1$ *and* $0 \le j < Na + Nb - 1$.

Illustration of 2 images cross-correlation results should be noted that the resulted image is with the dimensions of twice larger compared to the original images. We also do not want to use all available value. In addition, the resulted minimum peak can be affected by the brightness level of the original images. Instead, we just need the maximum value that the brightness levels have been taken into account. Fortunately, a normalized cross correlation operation given by the equation . (10) , below can offer what we need.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \qquad (10)$$

The score given by 2 most similar sub-image can be close to +1, whilst that of the different images is very low. For 2 images with each of 64 sub-image the correlation scores are illustrated in Fig. 4. The average matching score can then be easily calculated based on the score of each sub-image matching. The highest average score implies the most similarity of those two cropped images.

$$Avg = \frac{\sum_{i=1}^{64} xi}{64} \qquad (11)$$

The transformation of the image is intact trying to look into the image in the different point of view. In the transformed domain, the spectrum feature can define well the uniqueness of the fingerprint that is is hard to be of serve in the spatial domain. However with is an assumption, the orientation as well as the registration of the image must be the same. To overcome the rotation problem, the raw image must be rotated before segmentation or transformation. Obtained with the core point we can find a different angle between the two images. That enables us to rotate the sampled image to the same orientation as that of the referenced non-rotate images . We can find the raw image angle using the following steps below:

1) Define the circle of interest of which the radius of 100 pixels. The core point is taken as a center of this circle.
2) Draw a box of 15x15 pixels around the core point.
3) The lines connected between the box and the circumstance of the circle are considered for angle measurement. Average values were taken.

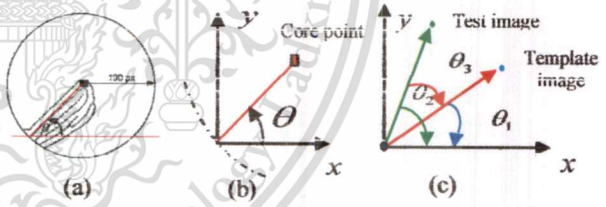
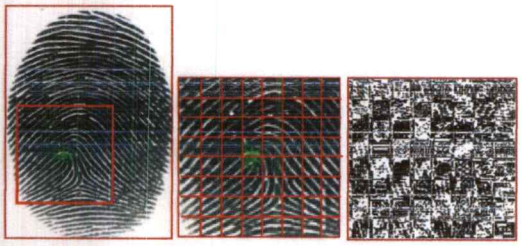


Fig3. (a) And (b) Image angle or image position ($\theta = 43.67°$), (c) Angle of the template rotated.

From Fig3, (c). If given θ_1 is an angle of a template image, θ_2 is an angle of a test (sampled) image, then θ_3 is the angle differences between those two images. We then have to rotate the template image by (θ_3) degree, ($\theta_3 = \theta_2 - \theta_1$).

In the fingerprint matching proceeding using 2D-Discrete Fourier transform. This step there could be few matching that give us high score or who past the first step, Normalization cross-correlation step, These candidates are then fed into the

2D-DFT, investigation to file the values of the spectrum, spectrum phase and line angles.



(a) (b) (c)

Fig. 4 (a) Original image , (b) 128x128 pixels cropped image and divide into 64sub-image with size 16x16 pixels, (c) 2D-Discrete Fourier transforms resulted.

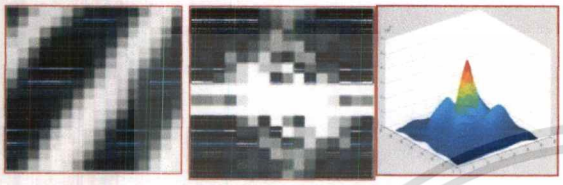


Fig. 5 (a) A portion of fingerprint images, size 16x16 pixels, (b) Resulted 2D-Discrete Fourier transforms, (c) Cross-Correlation Resulted between 2 sub-image.

IV. Fingerprint Matching Procedures

In this ageratum there are two constructions in the fingerprint matching procedure, database construction and matching algorithm. The procedure tries to find out the most similar pairs of the test image and the one in the database. The total process can be seen through the procedure are given as follows:

A. Database Construction

In practice there could be a huge fingerprint pattern stored as database. To identify the case an anonymous pattern must seek its most similar to one or few database patterns. Storing those tons of patterns without losing their originality is also a problem to be solved. In our approach database construction is as follows:

1) Including Test images from FVC 2004 DB1_A, database
2) The raw image is enhanced with Gabor filtering.
3) Mark the core point of the enhanced imaged is located using point care technique and Core point is a center.
4) Define the circle of interest of which the radius of 100 pixels. The core point is taken as a center of this circle.
5) Draw a box of 15x15 pixels around the core point.
6) The lines connected between the box and the circumstance of the circle are considered for angle measurement. Average values were taken.
7) Determine the main ridge angle (respective to the vertical line). The obtained angle is stored in the database together with the image name.
8) Tests images are cropped into the size of 128x128pixels a core point is at the center.
9) Images, size 128x128 pixels, are divided into 64 sub images with the size 16x16 pixels.
10) Each image is transformed via a 2D-DFT.
11) Determine the value of the spectrum, and the value of the line angle of each sub-image.
12) Enhance images, and the value of the spectrum angle line, and angle of each image are stored in the database.

B. Fingerprint Matching Step

The specimens (template) are then compared to the test images (database) using the following steps:

1) Follow from steps 1 to step 6 in the database construction
2) To the aligned core point, the template is rotated by

   Amount of degrees difference between the two images
3) Template is cropped with the size of 128x128 pixels (a core point is at the center).
4) The corresponding two images are matched with NCC template matching. If the same image must have Score more than 0.5.
5) Images, size 128x128 pixels, divided into 64 sub-images. with the size 16x16 pixels.
6) Each image is transformed via a 2D-DFT.
7) Determine the value of the spectrum and the value of the line angle of each sub-image.
8) Matching each value of the templates with values of the test images by correlation (corr2) technique.
9) The average value similarity of the spectrum the template image and test images between ≥ 0.75 to 1, and the angle line value equal or less than $\pm 0.5^{\circ}$

V. Evaluation and Results

The FVC 2004 DB1-A database set has been employed in this experiment. We have set up 16 template images from 4 groups (4 images for each pattern). Those patterns are whorl, left loop, right loop, and tents. These are included in 97 individual images (35 left-loops, 22 right-loops, 18 tents, and 22 whorls). Each individual holds 3 different scans. Therefore, there are 291 images involved in our test. This amount of images is large enough to check the consistency of the as well as to widen the testing domain. As detailed in the previous sections; the machine has involved 3 main steps, i.e.NCC Score, spectrum finding, spectrum matching and average value computation. The decision is made upon the obtained average value. The merit of the algorithm is basically stated by its fault acceptance rate and fault rejection rate. Given as an , matching score average values of samples obtained from a DFT process (a certain) are plotted as shown Fig. 6. The matching decision can be made upon the observation. In this case, somewhere the

value around 0.75 seems to be a good choice. Shown in the Fig.6 below.

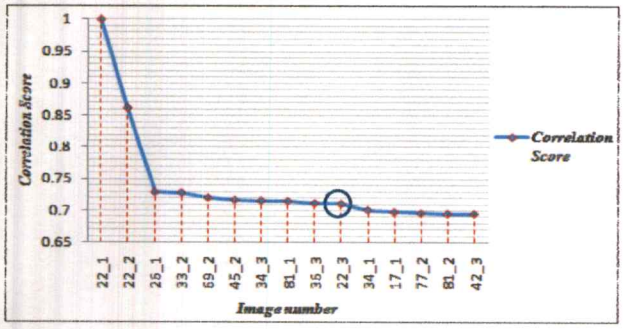


Fig .6 Average values of the correlation score of different images

The template is in fact the image 22_1. The decision at the value of 0.75 can result in image 22_2 and image 22_3 to be rejected . However, as the image 22_3 is a variation of the image 22_1. The decision is then wrong for the image 22._3. This is a case of faulty rejected. For the whole testing, the evaluation result is shown in table I below.

TABLE I. EVALUATION AND RESULTS

Pattern	Number of templates	Number of test image	NCC Score > 0.5, Avg.Values, spectrum > 0.75, line angles ≤ ±0.5°		
			Avg. Computation Time (ms)	% FAR	% FRR
Whorl	4	66	46.15	0	1.01
Left loop	4	105	48.82	0	1.2
Right Loop	4	66	47.61	0	1.6
Tent	4	54	37.11	0	2
Avg%	16	291	45.0	0	1.45

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

From table I. We can see the results in the Fig.7 below.

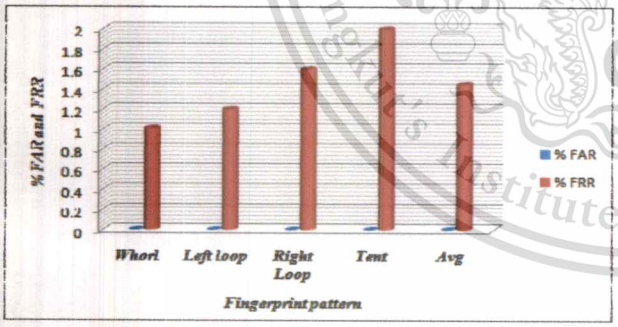


Fig. 7 FAR and FRR of each pattern

To demonstrate that the proposed a fingerprint matching scheme based on normalized cross correlation and 2D-Discrete Fourier transform method can have some advantage compared to the methods reported in the literature [17], They use FVC 2002-DB2A, the database consisted of fingerprints of 100 individuals and 8 images per person. They matching is based on the minimum Euclidean distance between two feature vectors. And in the reference [18], they used FVC2004 fingerprint database DB-A. There are 100 fingerprints including 5 images from each 20 fingers. First of all , for every fingerprint in the database, it considered as an input fingerprint image and it matched with other 4 coming from the same finger, and they measure performed based on the minutiae extracted features. To make a comparison, we used 97 individual images (35 left-loops, 22 right-loops, 18 tents, and 22 whorls), and included three images come from the same individual all of the images in the database. Likewise, we have tested 291 images constructed with 16 individuals from FVC2004-DB1A. Including three images come from the same individual, each image has difference angles or difference position. From this result are shown in table II.

Table II. Matching of different works

Matching Scheme	Results		
	Avg. Computation time (ms) /image	% FAR	% FRR
Ref. [17]	38	1	3.6
Ref. [18]	24	1.37	0.5
Proposed: Algorithm	45.05	0	1,45

Intel 1.4 GHz, 512 MB RAM, b. Intel i5, 2.1 GHz, 4 GB RAM

According to the results shown in table II, we can see that we have obtained is fairly good. Our technique proposed method is superior over [17] but cannot compete the one proposed in [18] for FRR. The false reject rate is not so severe and considered to be a positive error, since those reject samples could be re-examined by some other methods even by using an expert. We can also use the given below evaluating equation to compare our technique with other proposed algorithm that is.

$$FAR = \frac{false\_accepted\_num}{total\_matching\_num} \times 100\%$$

And

$$FRR = \frac{false\_rejected\_num}{total\_matching\_num} \times 100\%$$

From table II. We can see the comparison results in the Fig.8

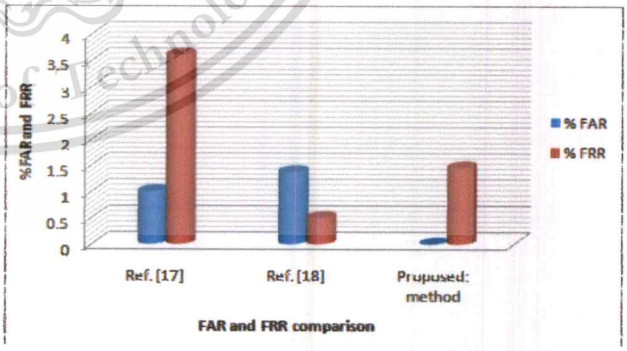


Fig. 8 FAR and FRR comparison of different methods

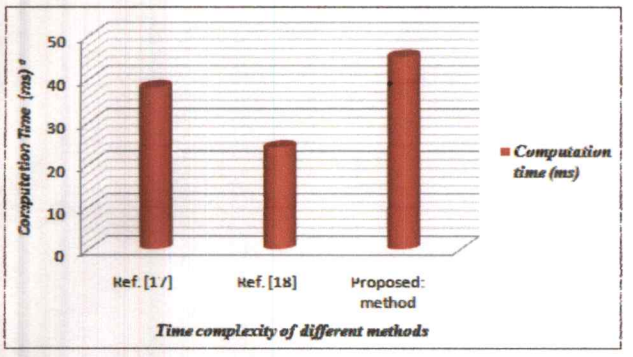


Fig.9 Time complexity of different methods

The average computation times of our method cannot complete, our algorithm use time for matching is longer than the techniques in [17 and 18].

VI. CONCLUSION

In this paper we have proposed a technique for fingerprint matching by using Normalized cross correlation and 2D-DFT. From NCC leaf *f*, the test images have the size 480x640 pixels and *t*, the template's images, to speed up the matching process crop the template images with the size (128x128 pixels). And second step we use high score or who past NCC steps to proposed by using 2D-DFT. This step in the template image and the test image are cropped with size 128x128 pixels and then divide 64 sub- images with size 16x16 pixels, and core point is assumed to be the center of this square. With FVC2004-DB1-A database, the 0% FAR, 1.45% FRR. The main drawback of the algorithm is its dependency of the core point. We hope we can fine some alternative approaches to further improve the performance of this work.

ACKNOWLEDGEMENT

We would like to acknowledge to the Asian University Network (AUN/SEED-Net) for the financial support of one of the authors (Mr. Souksamay Insankeovilay) from National University of LAOS (NUOL), LAO PDR for his graduate study at King Mongkut's Institute of Technology Ladkrabang (KMITL), THAILAND.

REFERENCES

[1] Jayant V. Kulkarni, Bhushan D. Patil, Raghunath S.Holambe "Orientation feature for fingerprint matching"J.V. Kulkarni et al./ Pattern Recognition 39 (2006) 1551 – 1554

[2] M. Taco and P. Kuosmanen, "Fingerprint matching using an Orientation based minutia descriptor," IEEE Trans. on Patt. Analyst and Mach In tell, vol. 25, no. 8, 2003, pp. 1009–1014.

[3] R. A. Marsh, and G. S. Petty, "Optical Fingerprint Correlate, "US Patent 5050220, 1991.A. Jain, L. Hong, and R. Boll, "On-line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4):302–313, April 1997.

[4] A.K. Jain, S. Prabhakar, L. Hong and S.Pankanti,"Filter bank Based fingerprint matching," IEEE Trans. Image Processing, 9(5): 846–859, 2000.

[5] Z. Bauhaus, J. Yinchuan, Z. Jianfeng, Y.Dahua, and Z. Quentin, "Fingerprint template matching Algorithm Based on Daubechies Wavelet, Proc. Of Int.Conf. On Communication Software and Networks, ICCSN-2009.

[6] S. Y. Tan, W.T. Huang, C.H. Chen, and Y.J. Chang, "Sweep Fingerprint Verification System Based on Template Matching, Journal of Recent Advances in Networking, VLSI, And Signal Processing, ISBN: 978-960-474-162-5.

[7] A.K.Jain, L. Hong and R. Bolle, "On-line fingerprint verification, " IEEE Trans Patt Anal Mach Intell, vol. 19, no. 4, 1997, pp.302–314.

[8] Y. He, J.Tian, X.Luo and T.Zhang, " Image enhancement and minutiae matching in fingerprint verification"Patt. Recog.Lett. no.24, 2003, pp.1349-1360.

[9] S. D. Wei and S. H. Lai, "Fast Template Matching Based on Normalized Cross Correlation with Adaptive Multilevel Winner Update," IEEE Trans. Image. Proc., vole 17, no.11, Nov. 2008.

[10] Kai Bristle and Use D. Han beck, Template Matching Using Fast Normalized Cross Correlation. Proc. Of SPIE01, vol. 4387, March 2001.

[11] C. Wang, M. Gavrilova, Y. Luo, and J.Rokne, "An efficient algorithm for fingerprint matching,"Proceedings of the 18th International Conference on Pattern Recognition (ICPR'06).0-7695-2521-0/06 $20.00 © 2006.

[12] J. K. Kim, S.H. Chase, S.J. Lim, and S.B. Pan, "A Study on The Performance Analysis of Hybrid Fingerprint Matching Methods," Int. Journal of Future Generation Communication and Networking pp. 23-28

[13] S.Dass, "Markov Random Field Models for Directional Field and Singularity Extraction in Fingerprint Images," IEEE Trans. Image Processing, vol. 13, no. 10, pp. 1358-1367, 2004.

[14] S.Tachaphetpiboon and T. Amornraksa, "Applying FFT Features for Fingerprint Matching," Proc. of Wireless Pervasive Computing Int.Symposium. 2006. O-7803-9410-O/06/$20.OO ©2006 IEEE.

[15] Xiao-Yuan Jing and David Zhang, "A Face and Palmprint Recognition Approach Based on Discriminant DFT Feature Extraction", IEEE Transaction on Systems, Man and Cybernetics-Part B: Cybernetics, Vol.

[16] Sharat Chikkerur, Alexander N. Cartwright, Venu Govindaraju "Fingerprint enhancement using STFT analysis". Elsever Ltd. (for the pattern recognition society), pp. 198-211, 2006.

[17] Yi Wang, Jiankun HuA, and Damien Phillips, "A Fingerprint Orientation Model Based on 2D Fourier Expansion (FOMFE) and Its Application to Singular-Point Detection and Fingerprint Indexing". IEEE transforms on pattern analysis and machine intelligence,Vol.29, NO.4, April 0162-8828/07/$25.00 _ 2007 IEEE.PP. 575-585.

[18] Shahram Mohammadi, Ali Frajzadeh "A Matching Algorithm of Minutiae for Real Time Fingerprint Identification System" World Academy of Science, Engineering and Technology 60 2009. PP.595-599