THE COMPARATIVE STUDY OF CANNY FILTER AND MORPHOLOGICAL OPERATOR IN FINGERPRINT RECOGNITION

ABDULGADER AB SINUSI

A thesis submitted in
fulfilment of the requirements for the award of Master of Computer Science
(Software Engineering)

The Department of Software Engineering
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

APRIL 2014

ABSTRACT

Fingerprint verification is one of the most reliable personal identification methods and it plays an important role in commercial and forensic applications. Designing a recognition system that will increase the accuracy is required. This thesis proposed a fingerprint recognition system using canny filter and morphological operator through path analysis test case. Steps involved in the recognition system include; image acquisition, pre-processing, features extraction and matching. Fast fourier transform is used to enhance the quality of the images and the features extracted efficiently to determine the minutia points in fingerprints with morphological operation, and the distribution of grey level co-occurrence matrix (GLCM) with canny filter. The proposed morphological operation determined the bifurcation, termination of the ridges and valleys, and their corresponding angles, and Euclidean distance was used for matching. On the other hand, features such as energy, homogeneity, entropy and correlation were extracted after canny filter was applied and again, Euclidean distance was used for matching. The experimental results showed the accuracy of the proposed methods through path analysis cases, and their performances were compared for their success rate, false accepted rate and false rejected rate. The overall success of the system under morphological algorithm was 99.70% with 0.15% false accepted rate and 0.30% false rejection rate. On the other hand, the overall accuracy obtained for GLCM, canny filter was 99.85% success rate with 0.15% false accepted rate and 0.15% false rejection rate. From the obtained results, it can be concluded that GLCM-canny filter overcame the morphological operation in obtaining high accuracy.

ABSTRAK

Pengesahan cap jari adalah kaedah yang paling berkesan dan paling dipercayai, dan ia memainkan peranan yang penting dalam aplikasi komersial dan forensik. Merekabentuk satu sistem pengesahan yang kurang rumit dan lebih tepat adalah diperlukan. Tesis ini mencadangkan satu sistem pengesahan cap jari yang menggunakan penapis cerdik dan pengendali morfologi melalui analisa kes ujian. Langkah-langkah yang terlibat dalam sistem ini ialah perolehan imej, pra-pemprosesan, ciri-ciri pengekstrakan dan pemadanan. Fast Fourier digunakan untuk meningkatkan kualiti imej dan ciri-ciri yang diekstrak dengan lebih cekap untuk menentukan perincian dalam cap jari dengan operasi morfologi, dan pengedaran kaedah bersama kejadian (GLCM) tahap kelabu dengan penapis cerdik. Operasi morfologi yang dicadangkan menentukan pencabangan dua, penamatan rabung dan lembah, dan sudut sama mereka, dan jarak Euclidean digunakan untuk memadankannya. Ciri-ciri lain seperti tenaga, kehomogenan, entropi dan korelasi diekstrak selepas penapis cerdik digunakan dan jarak Euclidean digunakan untuk pemadanan. Keputusan eksperimen menunjukkan ketepatan kaedah yang dicadangkan melalui kes analisa laluan, dan dilihat prestasi mereka dari segi kadar kejayaan mereka, kadar diterima palsu dan kadar ditolak palsu. Kejayaan keseluruhan sistem di bawah algoritma morfologi diberikan sebagai 99.70% dengan 0.15% kadar diterima palsu dan 0.30% kadar penolakan palsu. Tetapi, ketepatan keseluruhan yang diperolehi melalui GLCM - penapis cerdik ialah sebanyak 99.85% daripada kadar kejayaan dengan 0.15% kadar diterima palsu dan 0.15% kadar penolakan palsu. Dari keputusan yang diperolehi, kesimpulan yang boleh dibuat adalah bahawa, GLCM-penapis cerdik adalah lebih berkesan daripada morfologi dalam mendapatkan ketepatan yang tinggi dan mengurangkan kerumitan.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

$\sigma_i \sigma_j$	–	The Variance of Image
μ_i	–	The Mean of Image
DB1	–	Database 1
DB2	–	Database 2
DB3	–	Database 3
B.C.	–	Before Christ
FVC	–	Fingerprint Verification Competition
FBI	–	Federal Bureau of Investigation
NIST	–	National Institute of Standards and Technology
GLCM	–	Grey-Level Co-occurrence Matrix
PINS	–	personal identification numbers
FFT	–	Fast Fourier transform
MC	–	Match Count
NF	–	Number of Fingers
MMC	–	Miss Match Count
TSR	–	Total Success Rate
FRR	–	False Rejected Rate
FAR	–	False Accepted Rate
AFIS	–	Automated Fingerprint Identification System

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Due to their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (biometrics) due to the advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration. Fingerprint recognition is one of the oldest and most reliable biometric used for personal identification. Fingerprint recognition has been used for over 100 years now and has come a long way from tedious manual fingerprint matching. The ancient procedure of matching fingerprints manually was extremely cumbersome and time-consuming, and required skilled personnel.

1.2 Motivation

For nearly a hundred years, fingerprints have represented definitive proof of individual identity in our society. We trust them to tell us who committed a crime, whether a criminal record exists and how to resolve questions of disputed identity. Fingerprint information has been around since 1901, when it was introduced at Scotland Yard. It has played a key role with law enforcement and crimes. Everyone has a fingerprint on the tip of their fingers and every person's fingerprint is different or unique. They differ because of the curves and ridges that make up the skeleton of the fingerprint. The finger is usually rolled in black ink in order to obtain the fingerprint image. Once the ink is on the fingertip, the finger is then rolled on a really heavy paper in order to leave an impression. The fingerprint is scanned into a machine with the name for safe keeping and held in the Federal Bureau of Investigation (FBI) database or in any organization (Kadhem *et al.*, 2010).

1.3 Problem Statement

Fingerprint recognition system is one of the most common systems in forensic and commercial applications and it had been used for security for a very long time. The accuracy of the system is still facing challenges to achieve perfect rate, even though several systems have been built. Hence, designing a system with get good accuracy is the main task in fingerprint recognition system.

1.4 Objectives of the Study

The objectives of this study are summarized below:

(i) To implement canny filter and morphological operation for fingerprint recognition system.

(ii) To do a comparative study between the proposed two methods for fingerprint recognition system.

(iii) To evaluate the methods based on the total success rate, false accepted rate and false rejected rate.

1.5 Scope of the Study

The scope of the study is defined as follows:

This study developed a fingerprint recognition system based on canny and morphological operation methods. The features extracted by the algorithms were based on minutia, ridges, valleys, energy, entropy, homogeneity, correlation, and contrast. Euclidean distance was used for matching these features.

1.6 Outline of the Study

The flow of this project includes applying the canny filter and morphological based approaches on designing fingerprint recognition system. This thesis provides description and report on the effort that had been carried out throughout the duration of the project in order to achieve the scope of the study. This report is divided into five chapters that cover the whole project. Chapter one provides a brief introduction to biometrics and its application to security issues. It explains the fingerprint recognition prototype system in detail. Furthermore, this chapter explains the problem statement and states the motivation and objectives of this study. Chapter two introduces the history of fingerprint recognition system and some theories involved in the process. In this chapter, previous methods and algorithms were discussed and summarized, and the related topics and works relevant to the study based on various journals and publications were reviewed and used as references for this study. Chapter three introduces the proposed method and discusses the mathematical calculations related to canny filter and fast minutia based approaches, cross-correlation homogeneity, entropy and energy of images. Next, chapter four discusses the obtained results from the proposed methods and discusses some parameters such as, false accepted rate, false rejected rate and total success rate. This chapter also introduces comparatives of the obtained accuracies by the two proposed methods/algorithms. Chapter five summarizes and concludes the study and proposes future work for the system in order to increase the accuracy and simplify the algorithm used in this study.

CHAPTER 2

LITERATURE REVIEW

This chapter introduces the fundamentals of biometrics traits to security system. The history of biometrics is introduced and general overview of the physical and behavioural characteristics is elaborated. Furthermore, it introduces the history of fingerprint and the applications that can be implemented using fingerprint traits. It also introduces and discusses the previous published work that has been done by other researches in order to implement and improve the fingerprint system technology.

2.1 Introduction to Biometrics

Biometrics refers to the technique that depends on automatic authentication and verification. In other words, human beings have unique personalities that can be used for identification purposes. There are many types of biometrics that can be used, such as fingerprints, pattern of retinal and characteristics of voice. The knowledge of biometrics is still in its infancy, but the biometrics system is unavoidable and it plays a critical role.

Biometrics can be divided into two categories; physiological and behavioural. First, physiological biometrics uses fingerprint, iris, face recognition and hand, while behavioural biometrics observes patterns such as voice. In other words, fingerprint is the best among them as it offers the cheapest cost and possesses high degree of reliability (Li & Anil, 2009).

Behavioural based biometrics is related to the behaviour of a person. It can be easily changed by altering a signature or using a new phrase. The examples are signature recognition, voice recognition, and keystroke dynamic.

In some applications, more than one biometrics trait is used to attain higher security and to handle failure to enrol situations for some users. These systems are called multimodal biometrics systems. Examples of multimodal biometrics are, thumbprint, fingerprint, iris, face recognition, palm print and ear feature as shown in Figure 2.1.

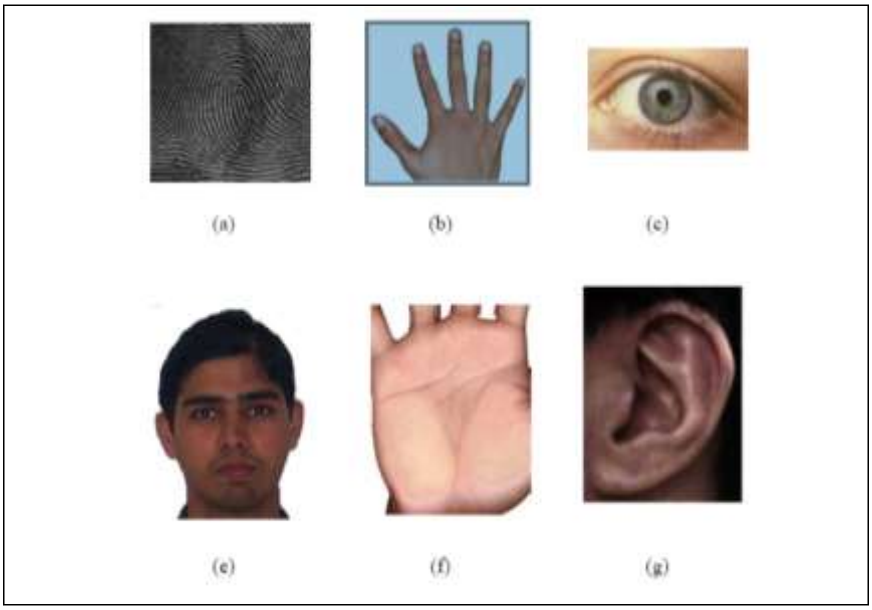


Figure 2.1: Multimodal Biometrics System (Li & Anil, 2009).

A biometrics system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific anatomical or behavioural characteristic possessed by the user. Numerous important issues must be considered in designing a practical biometric system (Li & Anil, 2009). The user must be enrolled in the system so that his biometric template or reference can be captured and stored in a central database or a smart card issued to the user. The template is used for matching when an individual needs to be identified and it depends on the context as the biometrics system can operate either in verification or identification mode.

2.2 History of Fingerprint Recognition

Fingerprint imaging technology has been in existence since a very long time. The use of fingerprints as a unique human identifier dates back to second century B.C., where the identity of the sender of an important document could be verified by his fingerprint impression in the wax seal (Kuchen & Newell, 2004).

The first modern use of fingerprints occurred in 1856 when Sir William Herschel, the chief magistrate of the Hooghly district in Jangipara, India, had a local businessman, Rajyadhar Konai, impress his handprint on the back of a contract. Then, the right index and middle fingers were printed next to the signature on all contracts made with the citizens. The purpose was to frighten the signer of repudiating the contract because the locals believed that personal contact with the document made it more binding. As his collection of fingerprints grew, Sir Herschel began to realize that fingerprints could either prove or disprove identity (Zhang & Shu, 1999).

The 19th century introduced systematic approaches to matching fingerprints to a certain group of people. One systematic approach, the Henry Classification System, based on patterns such as whorls and loops, is still used today to organize fingerprint card files (Jain *et al.*, 1999). In the late 1960s, the NEC worked with the Federal Bureau of Investigation (FBI) and the home office in London, which had been working on a system for new Scotland Yard to develop fingerprint identification system based on minutia. It was initially installed in Tokyo in 1981 and in San Francisco in 1983. In 1986 Australia was the first country to adopt a national computerized form of fingerprint imaging, which implemented fingerprint imaging technology into its law enforcement system (Okada *et al*., 1998). In 1996, after a year of study, the National Institute of Standards and Technology (NIST) has been convinced that minutia is an acceptable way to store fingerprint biometrics data on smart cards. With the acceptance of minutia, it became inevitable for the NIST to set standards for all fingerprint systems.

2.3 Fingerprint Recognition

Fingerprint recognition is one of the most common biometrics fingerprint technology based on uniqueness and ease of acquisition. Researchers and scientists discover two important keys about fingerprints; first, human fingerprints cannot change its structure normally after one year of birth, and second, everybody has unique fingerprint that is different from the other. Habitual fingerprint recognition was one of the first systems of machine recognition, and it did not solve problems, but on the contrary, fingerprint recognition is still a difficult and a very challenging pattern identification task. This is because, designing algorithms that are capable of getting efficient features and matching them in a stout way is very difficult, especially in poor quality fingerprint images and when low-cost acquirement devices with a small area are depended upon (Kalle, 1996).

Fingerprints have been used in forensics for more than 100 years and since the field of fingerprint analysis is so well-developed, fingerprint scanners are among the cheapest, most prolific, and most accurate biometrics applications found today. They are also easy to use and offer relatively high accuracy at a low price, with scanners available for less than $100. Fingerprint scanners are now incorporated into many firms that use them as a payment mechanism or to verify employee attendance. Recently, employee authentication solutions provider, Digital Persona Inc., integrated fingerprint biometrics into the company's software offerings. Such systems can reduce payroll costs related to time and attendance fraud and also prevent unauthorized manager over rides. In hospitals, fingerprint recognition has been used for access control to medicines and drugs.

Fingerprint verification has become the preferred biometrics technology at the point-of-sale over such other options as iris scans, voice scans, and hand geometry because they present the best combination of a number of factors, including cost, accuracy, and size.

2.4 Fingerprint Classification

As for fingerprint classification, there are many different researches related to sub classification. The basic categories found within these subgroups are aches, loops, and wholes. In order to avoid system comparisons and large data issues, which operates effort of the system when the definition of a person is required, the large data are divided into smaller pieces and compared through the items so that the test would class and compare the fingerprints. An imprint of the fingerprint may contain circles and edges extended in directions, fixed ends, and the ramifications of these forms. Figure 2.2 portrays five of fingerprint classifications developed by Henry to identify fingerprints (Sekar, 2011). These classifications are listed below:

(i) Left Loop.
(ii) Right Loop.
(iii) Whorls.
(iv) Arch.
(v) Tented Arch.

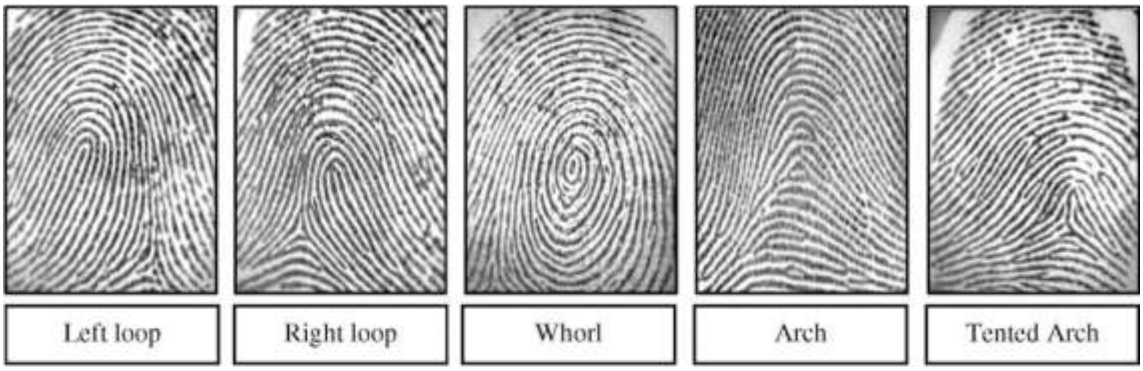


Figure 2.2: Subgroups of Fingerprint Classification (Sekar, 2011).

2.5 Classification of Process

In any fingerprint system, its operations usually depend on the following classifications:

(a) Core point is considered the nucleus or centre fingerprint.
(b) Delta points are points of the embranchments at the top and bottom of the fingerprint (the edge).
(c) To link the fingerprint forms with their applications by a specific algorithm based on the points of core and delta concept are as follows:
(i) If there are no major points to be classified but footprint Arch, the classification is Arches.

(ii) If there is a key point and only one in the bow, the classification is left or right loop.

(iii) If there are only two points and the arcs are in opposite directions, the classification is whorl.

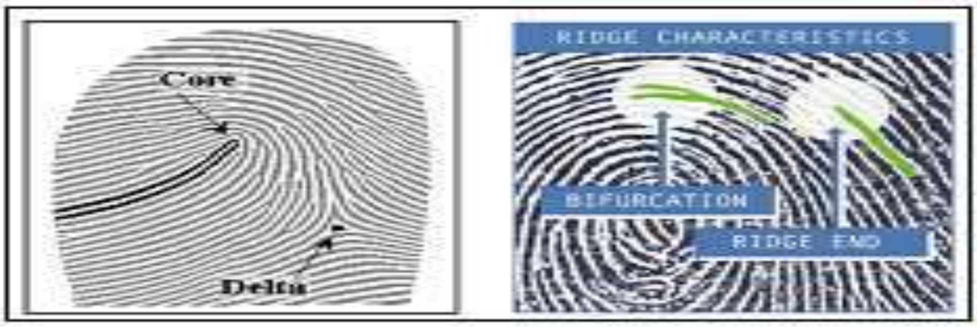
The classifications can be summarized using the general idea of algorithms as in Table 2.1.

Table 2.1: The Algorithms of sub-groups of Fingerprints

Class	NO. of Core	NO. of Delta
Arch	0	0
Tented arch	1	1(middle)
Left loop	1	1(left)
Right loop	1	1(right)
Whorl	1	2

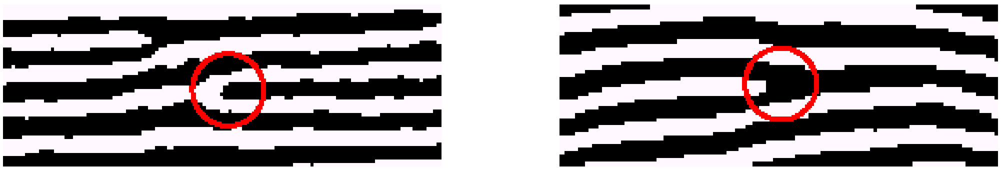
2.6 Representation of Fingerprint

There are two types of fingerprint representations, namely, local and global representations as shown in Figure 2.3. Local fingerprints are based on the entire image and the edges of the fingerprint, as shown in Figure 2.4. Hence, by taking the salient features that are the most common, it takes the details of the individual and the information stored effectively and accurately observed, as well as strong, no matter how small the fingerprint may be. As for global representation, it depends on the location of critical points, the core and the delta (Bana & Kaur, 2011).



(a) Global Feature (b) Local Features

Figure 2.3: Global Feature and Local Features (Verm & Goel, 2011)

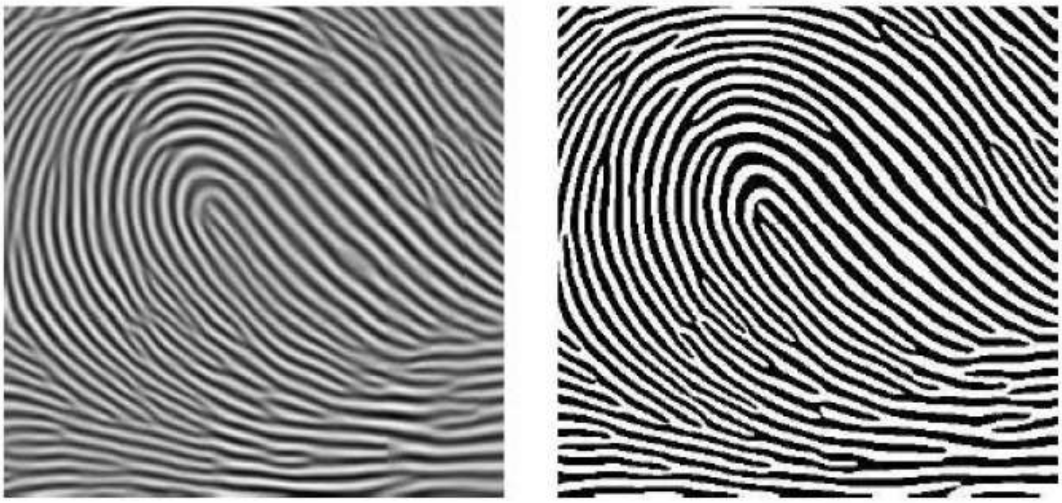


(a) Ridge Ending (b) Ridge Bifurcation

Figure 2.4: Ridge Ending and Ridge Bifurcation (Bana & Kaur, 2011)

2.7 Fundamentals of Image Processing to Fingerprint Recognition Finalization

Fingerprint finalization is a converts on process from grey level image into binary image. After the process is over, the ridges will be changed to black and the furrows, white. The process of filtered image produces pixel value of zero and therefore, finalization of the image can be performed using global threshold of zero. Usually, the finalization process involves examining the grey-level value of each pixel in the enhanced image and if the value is greater than the global threshold value, then the pixel value is set to a binary value. The outcome is a binary image containing two levels of information which are; the foreground ridges and the background valley, as shown in Figure 2.5 (Ashok & Ummal, 2013).



(a) Enhanced Image (b) Binary Image

Figure 2.5: Processing of Binarization (Ashok & Ummal, 2013)

2.8 Thinning

The last image enhancement step on minutia extraction is thinning. Thinning transforms the image from binary to the pixels, which performs the thinning operation using two sub iterations. This algorithm is accessible in MATLAB via the thin operation under the bimorph function. Iteration begins by examining the neighbourhood of each pixel in the binary image and based on a particular set of pixel-deletion criteria, it is used to check if the pixel can be deleted. The process continues until there is no more pixels that can be deleted in the image (Ashok & Ummal, 2013). The application of the thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeletonised version of the binary image, as shown in Figure 2.6.

(a) Enhanced image (b) Binary image (c) Thinned image

Figure 2.6: Enhancement Steps (Ashok & Ummal, 2013)

2.9 Fingerprint Pattern Recognition Approaches

The design of a pattern recognition system essentially involves the following three aspects as data acquisition and pre-processing and data representation, and decisions making. The problem domain dictates the choice of sensor, pre-processing technique, representation scheme, and the decision making model. It is generally agreed that a well-defined and sufficiently constrained recognition problem (small interclass variations and large inter class variations) will lead to a compact pattern representation and a simple decision making strategy. Learning from a set of examples (training set) is an important and desired attribute of most pattern recognition systems. The four best known approaches for pattern recognition are template matching and statistical classification, and syntactic or structural matching, and neural networks. These models are not necessarily independent and sometimes the same pattern recognition method exists with different interpretations (Anil *et al*., 2000).

(a) Template-Matching and Correlation Method

One of the simplest and earliest approaches to pattern recognition is based on template matching. Matching is a generic operation in pattern recognition which is used to determine the similarity between two entities (points, curves, or shapes) of the same type. In template matching, or a prototype of the pattern to be recognized is available. The pattern to be recognized is matched against the stored template while taking into account all allowable pose (translation and rotation) and scale changes. The similarity measure, often a correlation, may be optimized based on the available training set. Often, the template itself is learned from the training set. Template matching is computationally demanding, but the availability of faster processors has now made this approach more feasible. The rigid template matching mentioned above, while effective in some application domains, has a number of disadvantages. For instance, it would fail if the patterns are distorted due to the imaging process, viewpoint change, or large intraclass variations among the patterns (Anil *et al*., 2000).

(b) Statistical Approach

In the statistical approach, each pattern is represented in terms of d features or measurements and is viewed as a point in a d-dimensional space. The goal is to choose those features that allow pattern vectors belonging to different categories to occupy compact and disjoint regions in a d-dimensional feature space. The effectiveness of the representation space (feature set) is determined by how well patterns from different classes can be separated. Given a set of training patterns from each class, the objective is to establish decision boundaries in the feature space which separate patterns belonging to different classes. In the statistical decision theoretic approach, the decision boundaries are determined by the probability distributions of the patterns belonging to each class, which must either be specified or learned one can also take a discriminant analysis-based approach to classification. First a parametric form of the decision boundary (e.g., linear or quadratic) is specified, then the best decision boundary of the specified form is found based on the classification of training patterns (Anil *et al*., 2000).

(c) Syntactic and Structural Approach

In syntactic and structural approach, it is not only the digital values of the characteristics of each category are looked into, but also their inter-relations. Inter-relationship or interconnection of features between these characteristics in each category gives the necessary structural information to identify patterns. Recent studies in this area found that the most powerful way to identify the patterns is via combination of statistic pattern recognition approach with syntactic called Syntactic-Semantic approach. This way represents the style of a tree diagram or a graph string (literal string) on the initial elements of primitives, relations upon relations, and decision-making processes at the stage of recognition or classification is called Syntax analysis, or in other words, the Localization of parsing procedure. The highest percentage compared to the result of a comparison of the input image is with each tree (or graph/string, depending on the representation adopted in the application) stored determines the class to which the input image belongs (Anil *et al*., 2000).

(d) Neural Networks Approach

Neural networks can be viewed as massively parallel computing systems consisting of an extremely large number of simple processors with many interconnections. Neural network models attempt to use some organizational principles (such as learning, generalization, fault tolerance and distributed representation, and computation) in a network of weighted directed graphs in which the nodes are artificial neurons and directed edges (with weights) are connections between neuron outputs and neuron inputs. The main characteristics of neural networks are that they have the ability to learn complex nonlinear input-output relationships, use sequential training procedures, and adapt themselves to the data (Anil *et al.*, 2000).

2.9.1 Histogram Equalization

Histogram equalization is a technique of improving the global contrast of an image by adjusting the intensity distribution on a histogram. This allows areas of lower local contrast to gain a higher contrast without affecting the global contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values, Figure 2.7 shown the original histogram of a fingerprint image has the bimodal type, and the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced (Bana & Kaur, 2011).

In the meantime, contrast is expanded for most of the image pixels; the transformation improves the detectability of many image features. The probability density function of a pixel intensity level (r_k) is given by:

$$p_r(r_k) = \frac{n_k}{n} \tag{2.1}$$

where

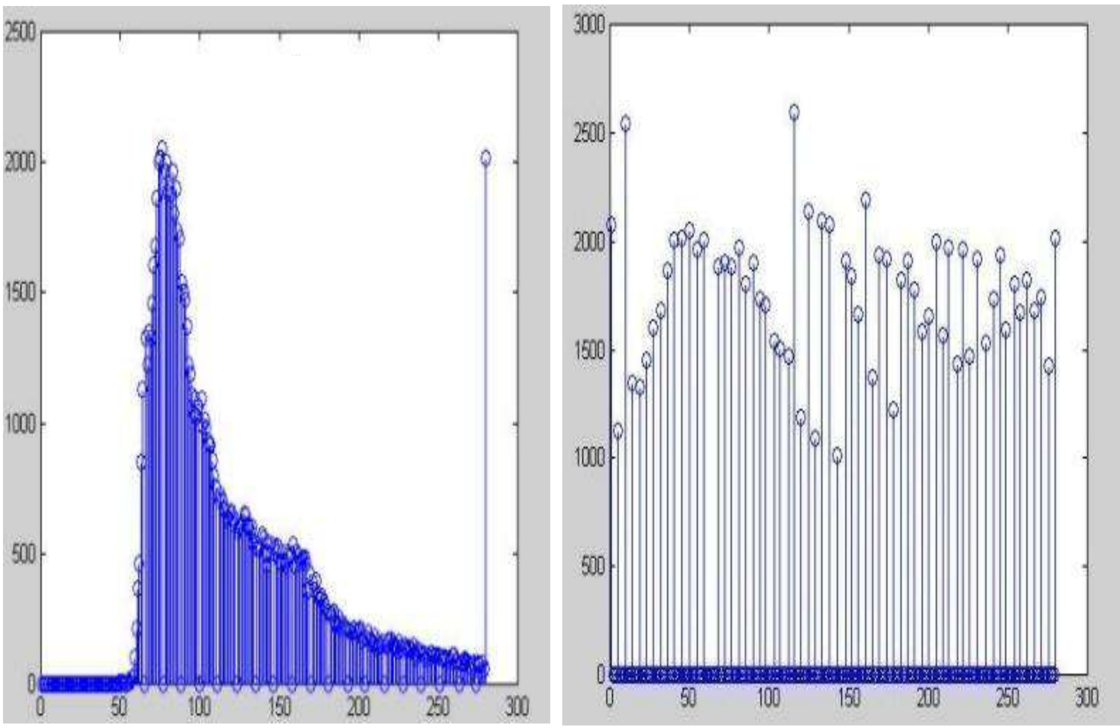
$0 \leq r_k \leq 1$, $k = 0,1,...,255$, n_k is the number of pixels at intensity level, r_k and n is the total number of pixels. The histogram is derived by plotting $p_k\ (r_k)$ against r_k. A new intensity s_k of level k is defined as:

$$S_k = \sum_{j=0}^{k} \frac{nj}{n} = \sum_{j=0}^{k} p_r(r_j) \tag{2.2}$$

Applying the histogram equalization locally using local windows of NxN pixels will result in expanding the contrast locally and changing the intensity of each pixel according to its local neighbourhood.

where

p	: Mean.
n_k	: The number of pixels at intensity level.
n	: Total number of pixels.
k	: Number of pixels.
j	: Number of picture.



(a) Original Histogram (b) Histogram Equalization

Figure 2.7: Histogram Equalization (Bana & Kaur, 2011)

2.9.2 Fast Fourier Transform (FFT)

In this method, the image is divided into small processing blocks such as (32 x 32 pixels) and Fourier transform is performed according to Equation as given:

$$F(u,v) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) e^{\left\{-j2\pi\left(\frac{\mu x}{M}+\frac{vy}{N}\right)\right\}} \qquad (2.3)$$

As for the calculation, u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31. In order to enhance a specific block by its dominant frequencies, multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs (F (u, v)) = |F (u, v)|. So, an enhanced block is acquired according to the Equation:

$$g(u,v) = f^{-1}(F(u,v) * |F(u,v)|^{k}) \qquad (2.4)$$

For x = 0, 1, 2 …31 and y = 0, 1, 2 ...31.

The value k in Equation 2.4 is an experimentally determined constant, whereby k=0.45. High value of k improves the appearance of the ridges by filling up the small holes in the ridges, but if the value is too high, it can result in false joining of ridges which might lead to termination and bifurcation. The enhanced image after the FFT is improved as some falsely broken points on ridges get connected and some spurious connections between ridges get removed (Masqueen & Renu, 2013).

2.9.3 Introduction to Minutia-Based Algorithm

Algorithms of Minutia-based extract information such as ridge ending, bifurcation, and short ridge from a fingerprint image are shown in Figure 2.8.

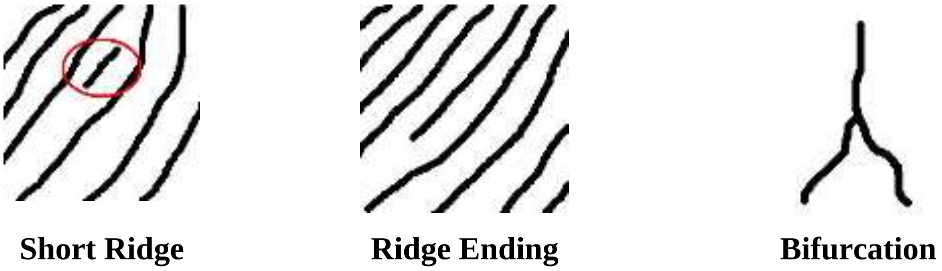


Figure 2.8: Different Ridge Shapes (Jain *et al*., 1999)

These features are then stored as mathematical templates or stored in matrices form. The identification or verification process compares the template of the live images with a database of enrolled templates (identification), or with a single enrolled template (authentication).

Figure 2.9: Ridge Endings in Different Locations in Two Minutia (Jain *et al*., 1999)

People with few or no minutia points cannot have successful enrolment or use of the system. This is demonstrated by the fingerprint immigration programmes such as the physical access control, information system security, customs and immigration, and National Identification (ID) systems, the largest Automated Fingerprint Identification System (AFIS) repository in America is operated by the department of homeland security's US visit program, containing over 120 million persons' fingerprints where finger moistening peripherals are standard. Furthermore, a low number of minutia points, as shown in Figure 2.9, can be a limiting factor for security of the algorithm. This can lead to false minutia points (darkened areas appear due to low-quality enrolment, fingerprint ridge detail or imaging). In the environment of the application, enrolment without assistance may take several attempts due to lack of pressure or poor position. While not quantified, user’s frustration will certainly have a negative impact on technology acceptance. Moreover, the widely used minutia-based representation does not utilize a significant component of the rich discriminatory information available in the fingerprints (Jain *et al*., 1999).

2.10 Minutia Match

Two sets of minutia of two fingerprint images are matched and the algorithm would determine if the two minutia sets are from the same finger. An alignment-based match algorithm is partially derived from Jain *et al*. (2004) to be used in this study. This algorithm includes two consecutive stages; alignment and match.

(i) Alignment stage: Given two fingerprint images for matching, choose any one minutia from each image, then the similarity of the two ridges associated with the two referenced minutia points are calculated. If the similarity appears larger than the threshold, each set of minutia is to be transformed to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.

(ii) Match stage: After getting the two sets of transformed minutia points, use the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

2.10.1 Alignment Stage

In first step, the ridge associated with each minutia is represented as a series of x-coordinates x_1, x_2…x_n of the points on the ridge. All the points are sampled per ridge length L starting from the minutia point, where the L represents the average inter-ridge length. The setting of n is 10 unless the total ridge length is less than 10*L. So the similarity resulted from correlating the two ridges are derived from:

$$S = \sum_{i=0}^{M} x_i X_i / \left[\sum_{i=0}^{M} x_i^2 \, X_i^2\right] \text{^}0.5 \qquad (2.5)$$

where

$(x_{i\sim}x_n)$ and $(X_{i\sim}X_N)$ respectively are the set of minutia for each fingerprint image and M is minimal one of the n and N value. If the similarity score is greater than 0.8, then go to step 2, otherwise continue to match the next pair of ridges (Nandian & ravi, 2011).

In second step, for each fingerprint, translate and rotate all other minutia with respect to the reference minutia according to the following formula:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ 0i\_new \end{pmatrix} = TM * \begin{bmatrix} (xi - x) \\ (yi - y) \\ (0i - 0) \end{bmatrix}$$

where

(x,y,θ) is the parameters of the reference minutia, and TM is as below:

$$TM = \begin{pmatrix} \cos 0 & -\sin 0 & 0 \\ \sin 0 & \cos 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

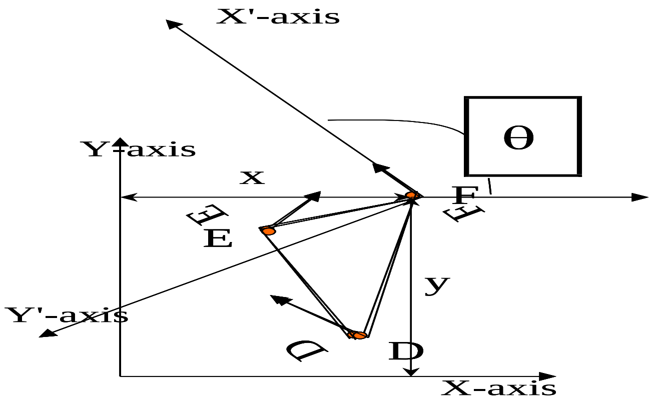


Figure 2.10: The Diagram Illustrate the Effect of Translation and Oration (Nandian & Ravi, 2011).

The new coordinate system is originated as shown in Figure 2.10 at minutia F and the new x-axis is coincident with the direction of minutia F. There is no scaling effect taken into account by assuming two fingerprints from the same finger nearly similar size.

The method to align two fingerprints is almost the same with the one used by (Nandian & Ravi, 2011). But it is different at step 2. Lin's method uses the rotation angle and it is calculated from all the sparsely sampled ridge points. This study used the rotation angle that was calculated earlier by densely tracing a short ridge starting from the minutia with length D. The minutia direction is derived from the minutia extraction stage. This method obviously reduces the redundant calculation and it still holds the accuracy. Besides, Lin's transformation is to directly align one fingerprint image to another according to the discrepancy of the reference minutia pair.

However, it still requires transform to the polar coordinate system for each image at the next minutia match stage. This study obtained its transformation according to its own reference minutia and then, matched in a unified x-y coordinate. Therefore, less computation workload is achieved through this method.

2.10.2 Match Stage

The algorithm of matching for the aligned minutia patterns needs to be elastic as it requires that all parameters (x,y,θ) are the same for two identical minutia is impossible due to slight deformation and inexact quantization of minutia.

Match minutia is achieved by placing a bounding box around each template of minutia. If the minutia match is obtained within the rectangle box and the direction discrepancy between them is very small, then the two minutia are classified as a matched pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia. The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. The score is 100 multiplied by ratio and ranges from 0 to 100. If the score is greater than a pre-specified threshold, then the two fingerprints are from the same finger. However, the elastic match algorithm is involved with large computation complexity and is vulnerable to spurious minutia.

2.10.3 Spectrum Analysis

Utilizing research from Nagoya Institute of Technology Graduate School in Japan, an algorithm was developed by Digital Development System (DDS) that is based on spectrum analysis, where this technique captures cross sections of a sliced fingerprint pattern and converts them to waves as shown in Figure 2.11. Spectrum analysis uses the wave's spectral series as feature information to find the maximum correlations in the wave and verifies the identity of the fingerprint.

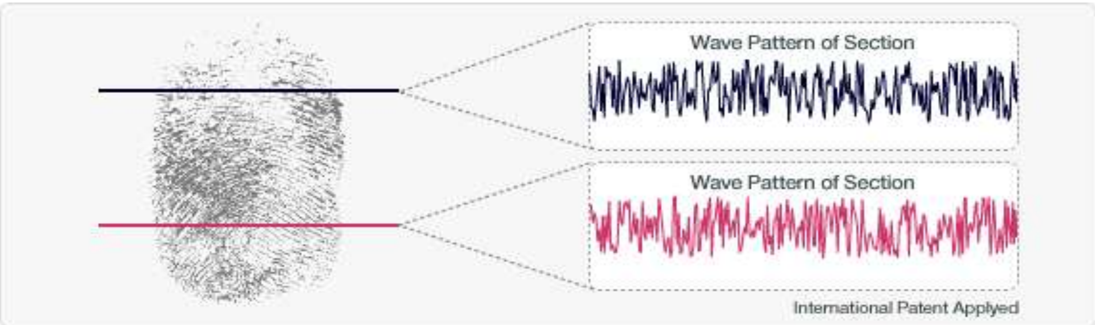


Figure 2.11: Wave Pattern of Two Different Sections (Sang *et al*., 2000)

The algorithm of spectrum analysis works extremely well because this algorithm extracts characteristics from the concavo-convex information of a fingerprint without being influenced by the position of the characteristic points used in the conventional Minutia and Pattern-matching method.

In the course of verification under the spectrum analysis algorithm, storing the fingerprint image itself in the system is not needed, which eliminates the possibility of exposure or leakage of fingerprint images. It is impossible to regenerate original fingerprint image from the extracted characteristics of images. As a result, this addresses issues raised by the (Sang *et al*., 2000) on fingerprint reconstruction of minutia-based systems. The algorithm performs extremely well in controlled environments where positioning of the finger in verification and enrolment are similar. However, with disparate fingerprint positioning for enrolment and verifications results, it can be less than desired or low accuracy. This requirement limits the application developer to be more controlled in its ergonomic environments and may reduce some commercial viability.

2.11 Canny Filter

The edges for an image are always the important characteristics that offer an indication for higher frequency components. Detection of edges for fingerprint image helps in finding the core, ridges and minutia points.

Canny edge detection algorithm is well known as an optimal edge detector in digital image processing. Canny has found that the optimal smoothing function for finding edges of a noisy step edge is approximately a Gaussian (Shriram *et al*., 2010).

Edges can be defined as the boundaries between different textures. The discontinuities in image intensity from one pixel to another in the entire image are called edge. The edges for an image are always the important characteristics that offer an indication for higher frequency components.

2.12 Features Extraction under Canny Filter

Several features are extracted from the trained and tested images. The most commonly used features are; energy, homogeneity, correlation, contrast and entropy of the images. The Grey-Level Co-occurrence Matrix (GLCM) is used to extract the features from the whole data and it will be stored and used for comparison at the matching step/process in canny approach.

2.12.1 Entropy

The entropy or average information of an image is determined approximately from the histogram of the fingerprint image. A Shannon entropy value is calculated from each sub bands obtained from the second level wavelet packet tree. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Shannon entropy criteria find the information content of signal ‘S’ using the Equation below. The histogram shows the different grey level probabilities in the image. The entropy is useful for image focusing. The wavelet energy signatures reflect the distribution of energy along the frequency axis over scale and orientation and have proven to be very powerful for texture characterization (Selvarajah & Kodituwakku, 2011).

$$Entropy = -\sum_{i=1}^{N} P\,(x_i) \log_b P(x_i) \qquad (2.6)$$

where

$P\ (x_i)$ is the probability that the difference between 2 adjacent pixels is equal to i, and Log $_b$ is the base 2 logarithm.

2.12.2 Energy

The sum of squared elements in the GLCM is given by the Equation below. The range for GLCM is [0 1], energy is 1 for a constant image (Selvarajah & Kodituwakku, 2011).

$$Energy = \sum_{i=1}^{N} \sum_{j=1}^{M} P(i,j)^2 \qquad (2.7)$$

where

i : Image Pixel.

j : Image Pixel.

p : Probability Density of Grey Level.

2.12.3 Correlation

It is a measure of how correlated a pixel is to its neighbour over the whole image, in other words, it determines the similarities between two images. The range for GLCM is given by [-1 1]. Correlation is 1 or -1 for a perfectly positively or negatively correlated image. Correlation is NaN (Not-a-Number) for a constant image. It is given by the following Equation (Selvarajah & Kodituwakku, 2011).

$$Correlation = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{(i-\mu_i)(j-\mu_j)P(i,j)}{\sigma_i \sigma_j} \quad (2.8)$$

where

$\sigma_i \sigma_j$: The Variance of Image.

μ_i : The Mean of Image.

i : Image Pixel.

j : Image Pixel.

p : Probability Density of Grey Level.

2.12.4 Homogeneity

It is a value that measures the closeness of the distribution of elements in the GLCM to the diagonal as given by the Equation below (Selvarajah & Kodituwakku, 2011). The range for GLCM is [0 1], homogeneity is 1 for a diagonal GLCM.

$$Homogenity = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{P(i,j)}{(1+(i-j))} \quad (2.9)$$

where

i : Image Pixel.

j : Image Pixel.

p : Probability Density of Grey Level.

2.12.5 Contrast

It is a measure of the intensity contrast between a pixel and its neighbour over the whole image, as in the Equation below (Selvarajah & Kodituwakku, 2011). The range for GLCM is given by [0, (size (GLCM,1)- 1)^2], contrast is zero for a constant image.

$$Contrast = \sum_{i=1}^{N} \sum_{j=1}^{M} (|i-j|)^2 \; P(i,j) \qquad (2.10)$$

where

i : Image Pixel.

j : Image Pixel.

p : Probability Density of Grey Level.

2.13 Morphological Operator

Morphological operations can be used to distinguish the boundaries of binary object. This operation is important. It is easy to see that the boundary points have at least one background pixel in its neighbourhood. Thus, applying the operator of erosion with a structural element that contains all possible neighbouring elements will remove all the boundary points. After that, the boundary is obtained. The operation of the difference between the sets of the original image and obtained as a result of erosion, thinning is a morphological operation that is used to remove selected foreground pixels from the binary images. In this process, it is used to tidy the wide-spread ridges by reducing all lines to single pixel thickness (Rajeswarl *et al.,* 2012).

2.14 Region of Interest Extraction by Morphological Operation

Two Morphological operations called 'OPEN' and 'CLOSE' are used in this project. The 'OPEN' operation can expand images and remove peaks introduced by background noise whereas; the 'CLOSE' operation can shrink images and eliminate small cavities (Latha & Rajaram, 2013).

2.14.1 Fingerprint Ridge Thinning

Ridge Thinning is the process that is used to eliminate the redundant pixels of ridges until the ridges are just one pixel wide in the image template. An iterative parallel

REFERENCES

Anil, K. J., Robert P.W. & Jianchang, M. (2000). Statistical Pattern Recognition: A Review. *IEEE Transactions On Pattern Analysis and Machine Intelligence, 22(1),* pp. 4 – 37.

Ashok, K. D. & Ummal, T. (2013). Comparative Study on Fingerprint Matching Algorithms for EVM. *Journal of Computer Sciences and Applications, 1(4),* pp. 55 – 60.

Bana, S. & Kaur, D. (2011). Fingerprint Recognition using Image Segmentation. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST), 5*, pp. 12 – 23.

Ganesh, P. V., Habibullah, K., Bhavana, K., Muralidhar, Ch. & Tulasi, Ch. (2012). Image enhancement using Wavelet transforms and SVD. *International Journal of Engineering Science and Technology (IJEST)*, *4(3)*, pp. 1080 – 1087.

George, J. P., Abhilash, S. K. & Raja, K. B. (2012). Transform Domain Fingerprint Identification Based on DTCWT. *International Journal of Advanced Computer Science and Applications (IJACSA), 3(1),* pp. 190 – 195.

Jain, A.K., Ross, A. & Pankanti, S. (1999). A Prototype Hand Geometry-based Verification System. *Proc. of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C.,* pp.166-171.

Jain, K., Ross, A. & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, *14(1),* pp. 1 – 29.

Jian, D. Z., Yuan, G. & Ming, Z. Z. (2009). Fingerprint Matching Algorithm Based on Similar Vector Triangle. *Second International Congress on Image and Signal Processing,* pp. 1 – 6.

Jianjiang, F. & Jie, Z. (2011). A Performance Evaluation of Fingerprint Minutia Descriptors. *International Conference on Hand-Based Biometrics (ICHB), 1*, pp. 1 – 6.

Josphineleela. R. & Ramakrishnan. M. (2012). An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique. *(IJCSIS) International Journal of Computer Science and Information Security, 10(3),* pp. 1 – 6.

Kadhem, M. & Hazeem, B. T. (2010). A New Algorithm for Fingerprint Recognition. *Journal of education of college, 1(1),* pp. 1 – 8.

Kalle, K. & Anil, K. (1995). Michigan State University, East Lansing, *M1 48824, U.S.A. Pattern Recognition, 29(3)*, pp. 389 – 404.

Kuchen, M. & Newell, C. (2004). A Model for Fingerprint Formation Europhysletters. *International Journal of Computer Science and Information Security 68(1),* pp. 15 – 24.

Latha, S. S., & Rajaram, M. (2013). Optimization Technique for Fingerprint Recognition and Matching. *Life Science Journal*, *10,* pp. 289 – 296.

Li, S. Z., Anil, J. K. (2009). Encyclopedia of Biometrics. *XXXII, 1419 Hardcover ISBN 978-0-387-73002-8*, 7, pp. 680 – 695.

Madhuri & Mishra, R. (2012). Fingerprint Recognition using Robust Local Features. *International Journal of Advanced Research in Computer Science and Software Engineering, 2(6),* pp. 1 – 5.

Maltoni, D. & Maio, D. (2009). Handbook of Fingerprint Recognition (Second Edition) Springer-Verlag *http://extras.springer.com/2009/978-1-84882-253-5/FVC2000/Dbs.*

Masqueen, B. & Renu, D. (2013). Fingerprint Recognition Using Optimal Global Transformation. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 3(6),* pp. 773 – 777.

Meenakshi, A., Gaganpreet, K. & Ravi, S. (2012). Minutiae Feature Based Algorithm for Finger Print Recognition and Verification. *VSRD International Journal of Electrical, Electronics & Comm. Engg, 2,* pp. 279 – 287.

Nandian, C. & Ravi, K. (2011). Improve fingerprint image representation for recognition. *MIT International Journal of Computer Science & Information Technology, 1 (2),* pp. 59 – 64.

Naresh, A. (2002). Testing from Use Cases, using Path Analysis Technique. *International Conference on Software Testing Analysis & Review,* pp.1 – 22.

Nasibe, A. & Ali, S, (2012). Automation of Fingerprint Recognition Using OCT Fingerprint Images. *Journal of Signal and Information Processing, 3,* pp. 118 – 121.

Okada, K., Steffens, J. & Maurer, T. (1998). Face Recognition. The Bochum/USC Face Recognition System and How it Fared in the FERET Phase III Test. Springer-Verlag. NATO ASI Series, *163*, pp. 186 – 205.

Rajeswarl, Allen, M. R., Arjun, A. & Asif, M. S. (2012). A novel enhancement method for low-quality fingerprint images in both spatial and frequency domains. *International Journal of Computational Engineering Research, 2(6),* pp. 1 – 5.

Ravi. K. L., Sai, S. K., Rajendra, J. P., Subba, B. V. R. & Ravi, P. P. (2012). Fingerprint Minutia Match Using Bifurcation Technique. *International Journal of Computer Science & Communication Networks,* 2(4), pp. 478 – 486.

Sang K., I., Hyung M., P., Soo W. K., Changkyung, C. & Hwansoo, C. (2000). Improved Vein Pattern Extracting Algorithm and its Implementation. *IEEE International Conference on Digest of Technical*, pp. 2 – 3.

Sekar, V. (2011). Denoising of Fingerprint Images using Q-shift Complex Wavelet Transform. *International Journal of Computer Applications, 15(3),* pp. 12 – 17.

Selvarajah, S. & Kodituwakku, S. R. (2011). Analysis and Comparison of Texture Features for Content Based Image Retrieval. *International Journal of Latest Trends in Computing, 2,* pp. 108 – 113.

Shriram, K., Sivaraman, R. & Karthick, S. (2010). Automotive Image Processing Technique Using Cranny's Edge Detector. *International Journal of Engineering Science and Technology, 2*, pp. 32 – 35.

Suvarna, J. & Abhay, K. (2012). Correlation Filter based Fingerprint Verification System. *International Conference on VLSI, Communication & Instrumentation (ICVCI) Proceedings published by International Journal of Computer Applications (IJCA),* pp. 1 – 5.

Tico, M., Kuosmanen, P. & Saarinen, J. (2001). Wavelet domain features for fingerprint recognition. *IEE Electronics Letters, 37(1)*, pp. 21 – 22.

Verma, R. & Goel, A. (2011). Wavelet Application in Fingerprint Recognition. *International Journal of Soft Computing and Engineering (IJSCE), 1*(*4*), pp. 129 – 133.

Wan, A., Lim, T. & Salasiah, H. (2004). Fingerprint recognition in wavelet domain. *Jurnal Teknologi, 41(D), Universiti Teknologi Malaysia*. pp. 25 – 42.

Xuzhou, L., & Fei, Y., (2009). A New Fingerprint Matching Algorithm Based on Minutia. *IEEE International Conference on Communications Technology and Applications*, pp. 869 – 873.

Zhang, D. & Shu, W. (1999). Two Novel Characteristic in Palm-print Verification: Datum Point Invariance and Line Feature Matching. *The Journal of the Pattern Recognition Society*, *32(4)*, pp. 691 – 702.