Scientific Research Publishing

Journal of Computer and Communications, 2020, 8, 55-74
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Fingerprint Enhancement, Minutiae Extraction and Matching Techniques

Sek Socheat, Tianjiang Wang

School of Computer Science and Technology, Huazhong University of Science and Technology (HUST), Wuhan, China
Email: I201722157@hust.edu.cn, socheat_sek@yahoo.com, tjwang@hust.edu.cn

How to cite this paper: Socheat, S. and Wang, T.J. (2020) Fingerprint Enhancement, Minutiae Extraction and Matching Techniques. *Journal of Computer and Communications*, **8**, 55-74.
https://doi.org/10.4236/jcc.2020.85003

Received: April 9, 2020
Accepted: May 25, 2020
Published: May 28, 2020

Abstract

Nowadays, it is a new technology era. Fingerprint is necessary identification recognition of citizens. Fingerprint technology has become more popular and connected to human being life and come to replace traditional identification and verifying recognition today. The fingerprint will continue to substitute the ID of citizens as soon as possible in the future. Fingerprint refers to a complex of combination between gap of ridges and valleys on all of the fingertips. Clearer ridges quality is more convenient to analyze who you are and system can recognize your unique identity. Poorer ridges quality image is a significant problem that system has to improve and enhance the images quality before analyzing the results. Dry and wet ridges are the main issues that developers and researchers need to work on as it provides poor quality image. Medium ridge image is a good condition for analysis, but it also needs to be improved. Therefore, fingerprint images have to control the clearer quality and computing minutiae result and then comparing to templates, which stored in the database. The result will display if it is matched but it will not appear when that person has not yet registered. The paper proposed three algorithms to enhance image, extract minutiae and match with fingerprint templates. The first step, is used to enhance the image quality using brightness and Gabor filters on the fingerprint surface to make ridgelines darker. The second step is to extract minutia. It used to convert the images to binary (0 and 1) and process thinning image with Zhang Suen algorithms. Then, the pictures go through the fixing procedure to correct any missed links, error ridges or spurious minutiae that generated by fingerprint algorithms before they undergo final analysis, calculate location of minutiae and the total of the minutiae on the fingerprint surface. The last step is matching algorithms that can be proof of a person identity by comparing minutiae result with those in the database. If a person has already enrolled, the result will confirm.

Keywords

Fingerprint Enhancement, Minutiae Extraction, Minutiae Matching, Ridgeline Thinning, Removable Spurious Minutiae

1. Introduction

1.1. A Short History of Fingerprint

Fingerprint has been used since eighth century AD history, during China's Tang dynasty in clay to describe, served as a kind of signature in business contracts and law enforcement cases [1]. Fingerprint has been used for recognizing for individual since thousand years ago in clay. In the past, they used fingerprint to recognize a person in law enforcement. After that, they used fingerprint for criminal investigation and forensic. It is continuous until now. A fingerprint is an impression or made by a person's fingertip on a surface [2]. Fingerprint is a significant biometric among other biometrics traits. The FBI and US government departments in the 1970s developed were releasing biometric recognition database [3]. Fingerprint has used for personal identifying in digitalization applications and has been used in forensic applications for over hundred years. Fingerprint recognition recognizes the identity of an individual according to "who he/she is" or based on "who you are".

Fingerprint is an utmost kind among of another significant biometrics. Biometric recognition refers greater security and convenience that traditional methods of person recognition based on official documents, PINs, and passwords [4]. Biometric is a group number of technologies that used to authenticate persons using their physical traits such as fingerprints, iris, retina, speech, face, palm-print patterns or behavior traits including gait, hand written signature and keystrokes movement. There is a rapidly expanding range of applications for fingerprint system across the public and commercial sectors including: national government services, driving license, criminal justices records, criminal detection, voter registration, CCTV surveillance, border security or passport issuing systems, refugee assistance, financial services, computer systems, secure database access, venue access, smartphone access, healthcare identity management, workplace attendance management, and so on. Biometric allows a person to be authenticated or identified using behavioral or physiological characteristics and these characteristics must be automatically recognizable and verifiable.

1.2. Significant of Fingerprint in Digitalization Era

Until today, it is a digitalization technology era. Fingerprint is an essential unique pattern to identify individual characteristics. Ridge pattern on the fingertips has to be differentiating from each other, even in practical, twins do not match the same templates or structures. Fingerprints become a key unique of recognition system platform to identify personal identity and authentications to

user have a right to login to use the system or access to cross a security control. Fingerprint refers to a complex of pattern's combination that presenting about the friction ridges and valleys on the surface of a fingertip. Fingerprint is one of the most complexity systems, which requires a constant and continuous on contribution with other researchers and scholars in research and development (R & D) institutions. Fingerprint has received more and more attention for security in a wide range of applications and smartphone until nowadays and keep continue to the future. Fingerprint has an answered to proof a person's identification and peoples will no cheating the system machines. Fingerprint authentications are more useful than a combination of secret characters (passwords) authentication that have some obvious drawbacks, stolen, lost, or forgotten and so on. Fingerprint recognition need a bit require effort from the users, it cannot copy, stolen or shared with others.

Fingerprint recognition is an utmost and interesting topic for identification and verification (authentication). Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse [5]. Fingerprint recognition is a type of biometric technology that uses the unique pattern of physical or behavioral traits of users for authentication and identification. It is a very strictly and necessaries for recognition processing, and provides relatively as a good performants. Fingerprint specification need to improving the techniques and systems for enhancement fingerprint images, fingerprint feature extraction templates, and minutiae matching results, especially in a large-scale or big data of biometrics database.

Fingerprint technology becoming more prevalent via biometric scanners on devices and smartphone, as well as a growing number of authentication in high security system and good customers certified experiences to replace old and traditional methods of authentication (passwords or PINs) system. Developers and analysts of biometric recognition systems always bear in mind that such system are complex and need to be addressed and this system is an inherently probabilistic endeavor. Biometric system will automate recognition of individuals as an awareness of the uncertainty associated with that recognition. Biometric recognition needs law enforcement in supports from government such as policy makers, developers, and researchers. For policy makers, it seeks to provide a comprehensive assessment of biometric recognition that examines current capabilities, future possibilities, and the role of government in technology and system development. For developers and researchers, are to articulate challenges posed by understanding and developing biometric recognition systems and point out opportunities for future researches.

Nowadays, fingerprint technology is increasing and widely used in government and private sectors. Fingerprint is a new crucial security protection and personal unique identification. Identification and verification are distinct methods for fingerprint matching. Many researchers, scholars, students, and development institution, to try their best to develop new or/and enhancement ex-

isted algorithms and techniques to accurate the fingerprint recognition more accuracy and quick processes, especially for the large population management systems. A person has to verifying his/her live fingerprint (image) with fingerprint template (results) that stored in the database. One-to-one matching called verification (known as 1:1 comparison). One-to-many matching called identification (known as 1: N comparison).

1.3. Fingerprint Verification

Verification is a searching function that is not dependent on a suggested identify and therefore the enquiry template interrogates the entire database for a possible match [6]. Verification system is a comparison method to identified individual and has to claim his/her identity by compared to their fingerprint template, which stored in the database. One-to-many matching called identification (well known as 1: N comparison). The searching and matching system generates a similarity score for potential matches and either automatically selects a high confidence match or presents a candidate list of suggested matches to a human operate for comparison with the enquiry template. Moreover, a process of confirming the user identifying after verification and authentication, called authentication. Templates refers to the features extracted from biometric characters are stored in the database as templates.

1.4. Fingerprint Identification

Identification is a processing to compares the enquiry template with the database template and confirms either that the two templates originate from the same person or that they do not. Biometric technologies collect and usually store unique or distinctive biological and/or behavioral characteristics of a person (biometrics data) for the automated verification of an identity claim or for the identification or that person [7]. All biometric data is the first captured by camera or sensor devices as an image and then further processed into a biometric template [8]. Matching algorithms used for verification and de-duplication are based on comparing these biometric templates. A fingerprint identification system is an automatic pattern recognition system that consists of three fundamental stages: 1) data acquisition: the fingerprint to be recognized is sensed; 2) feature extraction: a machine representation (pattern) is extracted from the sensed image; and 3) decision-making: the representation derived from the sensed image are compared with a representation stored in the system [9]. This model uses an asserted identity to select one template from the database or electronic document for comparison with the enquiry template [6].

Fingerprint is a unique pattern of individual without duplicate data even twins. Ridge and valley on the fingertips surface used to identify each characteristic. Fingerprint with high quality contains 25 to 80 number minutiae [10] [11] [12] depending on fingerprint capture device and fingers condition. Different fingerprint sensors produce different quality of fingerprint data. For high and poor images have to following the fingerprint recognition procedure [12].

1.5. Study of Structure

As the following guidelines of this paper will describes in four parts. First part will capture of the literature review of the fingerprint. In the second part, will explanations about the fingerprint enhancement and extraction minutiae technique. In the third part, will showing about the methodology of fingerprint matching algorithm and the last part of this paper will doing a conclusion and future work. In the part two and part three of this paper will describes more methodology in detail including: 1) fingerprint acquisition, 2) fingerprint pre-processing or enhancement processing such as bright image, Gabor ridgelines, convert image to binarization, and thinning ridges, 3) minutiae extraction, 4) minutiae matching, and the last 5) results.

2. Literature Review

2.1. Biometric Data

The word biometric is a combination of two words in Greek 1) bios means that "life" and 2) metrikos means that "measure" [13] [14]. Biometric are physical or behavioral characteristic to that could be used to digitally identify a person to grant access to systems, devices or data [15]. Biometrics refers to automatic systems that use measureable, physical or physiological characteristics or behavioral traits to recognize identify, or verify/authenticate the claimed identity of an individual [16]. Biometric recognition is an emerging personal recognition technology developed to overcome the inherent limitations of the traditional personal recognition approaches [13].

Biometric data is the extracted information taken from the biometric sample and used either to build a template or reference or to compare against a previously created template or reference [17]. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things [18].

Biometric system are designed to recognize individuals by using their biological and physiological characteristics such as fingerprints, hand vein patterns, iris, face, DNA and others. In general, biometric modalities share features that make them, to lesser and greater degrees such as universal, unique, permanent, measurable, perform effective, acceptable, and vulnerable to circumvention risk [6]. Biometrics demands to increase for reliable and automatic solution to security systems. Biometric recognition is becoming ever more widely developed in many commercial, government, and forensic applications [13]. Biometric applications are often large-scale, which means biometric system should be operating in large population database, including: welfare-disbursement, national ID cards, border control, land title registration, student's registration, patient's information, voter ID cards, driver's licenses, criminal investigation, corpse identification, parenthood determination, and identification of missing children.

Given an input biometric sample, a big data biometric identification system determines whether the pattern is associated with, any of a large number (e.g.,

millions) of enrolled identities. A Biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [5].

2.2. Biometric Technology and Analysis

Biometric is a new solution that offers to identify any person based on his or her distinctive anatomical and behavior characteristics. Biometric could be providing many solutions that other technologies cannot offer such as uniqueness, convenience, non-repudiation, non-transferable, and proven (See **Table 1**). Nowadays, biometric technologies employing unique physical traits are applicable to multiple sectors ranging including health care, education, agriculture, airport, and to any enterprise from large to small such as aviation, hotels, banking and finance, government agencies and social welfare schemes, insurance, retail, manufacturing, law enforcement to hospitality, and tourisms [19].

Biometric has the potential to make authentication dramatically faster, easier and more secure than traditional passwords, but companies need to be careful about biometric data they collect [15]. Any human biological or behavioral characteristics can become a biometric identifier, provided seven analysis pillars of biometrics as the following properties below:

1) Universality: refers to any trait of human characteristics to determine their identity. Each individual should have the biometric characteristic [20].

2) Uniqueness (distinctiveness): refers to unique of person recognition to determine their identity without duplicate features even from twins such as fingerprint or iris patterns. Each person should have the feature but distinct from others [20].

3) Permanence: refers to any identity of human have untransformed of their characteristics, for instance fingerprint and iris are good stability recognized, whereas signature, facial, and voice features have changes their significantly by aging and trait along the time life. The biometric trait should be constant for certain period of time [20].

4) Collectability (measurability): refers to obtaining, acquisition, or measurement of the trait feature(s) that non-intrusive, reliable, and robust according

Table 1. Feature and advantage of biometric technology.

Features	Advantages
Uniqueness	Fingerprint is distinctive and different from one another even identical twins have different minutiae features too.
Convenience	Replace traditional recognition identities such as password or PINs that no longer to remember, lost, long and complex (mix characters)…
Non-repudiation	Non-fake user if they are no present at the point and time of recognition and later cannot deny having accessed the system.
Non-transferable	Unique and stable, data cannot be shared, stolen, copied, lost, or non-forgotten.
Proven	Unique data, distinctiveness and permanence of fingerprint.

to quality and cost devices. For instance, face recognition may need a simple webcam but fingerprint and iris may need very specialized devices and cost is not so expensive, ease of data capturing, measuring and processing [20].

5) Performance: refers to the results of analysis by systems to proven accuracy levels, speed, and robustness of technology used. It used in evaluate the accurate level of false acceptance rate (FAR) of automated systems, security, speed, accuracy and robust [20].

6) Acceptability: refers to vital points to obtain end-users support and willing of people in evaluate the necessaries of technology among population to adopt and share their biometric data and assessed or not accepted by the user population without any objection [20].

7) Circumvention: refers to evaluation how difficult it is to fool the system with high false acceptance rate (FAR) by easy methodologies to matching level. This is so important point to prevent consideration of any fake fingers hacking to the system. Ease of use of a substitute for instant the act of cheating [20].

2.3. Fingerprint Biometrics

Until nowadays, they used fingerprint for many functions in technology including for law enforcements, criminal investigation, human resources management, security control, system authentication. Both of government and private sectors are trusted on fingerprint biometric and fingerprint became a most popularity among biometrics in science and technology generation. Fingerprint has been used to recognized individual without duplicate identity feature even twins. The world are well-known recognized that fingerprints are the utmost widely used biometric characteristics for forensics community for over hundred years and automatic fingerprint identification systems were first installed almost fifty years back [21].

Fingerprint is a group of combinations of ridges and valleys in the fingertips on the surface prints. Fingerprint are unique patterns, made by friction ridges (raised) and furrows (recessed), which appear on the pads of the fingers and thumps and prints from palms, toes and feet are also unique; however, these are used less often for identification, so this guide focuses on prints from the fingers and thumps [22]. Friction ridges (also called ridgelines) on the fingerprint are black color and valleys are white color. Ridges and valleys often run in parallel; sometimes they bifurcation and sometimes they terminate [21]. According to earlier study and research has been classification of friction ridges on the fingerprint pattern into three distinct types such as loops, whorls, and arches. Ridgelines are the most commonly used minutiae types since all types of minutiae are depending on Ridge Island, Ridge Ending, Ridge Dot, Ridge Enclosure, and Ridge Bifurcation etc. (see **Figure 1**).

Fingerprint recognition is a complex pattern problem; designing algorithms capable of extracting salient features and matching them in a robust way is quite hard, especially in poor quality fingerprint images [21]. Fingerprint running crossed many generations from individual matching to automatically matching.

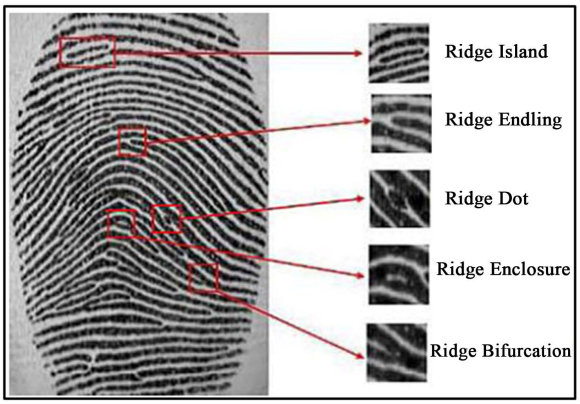

Figure 1. Ridgelines minutiae types or points.

First automated fingerprint identification system (AFIS) established in the 1980s, used for criminal identification have become central to the work of police and other law enforcement agencies around the world [23]. Fingerprints, according to Sir Francis Galton (Charles Darwin's cousin), the probability of finding two similar fingerprints is one in 64 billion even with the twins [23].

3. Fingerprint Enhancement and Extraction Minutiae

3.1. Fingerprint Architecture

In this paper will described about the architecture system to enhancement, extraction and matching fingerprint as shown in (**Figure 2**). In this architecture have been divide into two processing. In first part has shown the flowchart of fingerprint acquisition or enrollment process and in second part shown the flowchart of fingerprint matching feature with samples of fingerprint minutiae in database to identity each individually (who is he?, who is she?, or who you are?). Fingerprint recognition system constitutes of fingerprint acquiring device, fingerprint enhancement, minutiae or feature extraction and minutiae matcher.

Fingerprint architectures or systems consist of both hardware and software. Fingerprint is the most common biometric identifiers used in biometric systems authentication systems today. Fingerprint systems are automated system designed to employ fingerprint derived from sensor or from another sources. First, fingerprint data can receive from a fingerprint capture device or sensor and associated circuitry. Fingerprint acquisition, optical or semi-conduct sensors are widely used [24]. After, fingerprint data need to extracts the relevant data from the actual submitted sample. The minutiae extractor and matcher require three stage approach is widely used by researchers such as preprocessing, minutiae extraction and matching stage. In preprocessing step require to use three methods including image enhancement, image binarization and image segmentation. After minutiae extraction with two methods by thinning and minutiae making points, fingerprint need to matches the submitted sample with templates (minutiae). A post-processing is used to removable any false minutiae after extraction done. Finally, fingerprint need to determine whether the identity

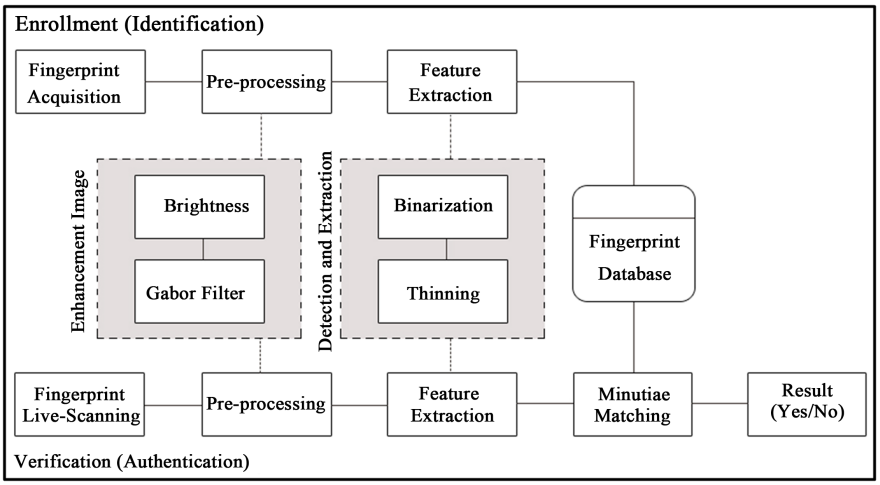

Figure 2. Fingerprint system architecture.

of the fingerprint data holder is authentic. The minutiae matching choose any two minutiae as a reference minutia pair and then match their associated ridge first. If the ridge matches well, the two fingerprint images are aligned and matching is conducted for all remaining minutia. All features template are stored in database system.

3.2. Fingerprint Recognition

Fingerprint is the oldest one known biometric identifier that used for authentication and identification purpose. A fingerprint is an impression left by the friction ridges of a human finger [25]. Fingerprints authentication system are designed to performance four operation including data collecting, enrollment, authentication, and matching. Data capture is a sensor device that used to capture data from the finger identifier used. Enrollment is a processing to the capture fingerprint, analyzed its unique features, and store minutiae features as a digital template. Authentication is a methodology that used to compare their features when an enrolled user wants to authenticate himself/herself. If missed matches his or her fingerprint data, require capturing fingerprint and compared against the template generated by the enrollment. Matching is an algorithm that used to compare live-scan fingerprint within system if there is a match between the stored template or not.

What are types of fingerprint patterns? There are a lot of explanations and described about fingerprint pattern but Joannes Evanelista Purkinje was described in part of his thesis published on December 22, 1823, dealt in considerable detail with the function of ridges, furrows, and pores; additionally, he illustrated and described nine fingerprint patterns: one arch, one tent, two loops, and five types of whorl [9]. The interesting observations, Purkinje made regarding the four basic patterns but for authors [14] [22] made focused on three basic patterns by excepted tent pattern in their research (See Figure 3) including:

1) Loops: The pattern of ridgeline that go-forward and curve backward on the

Figure 3. Three basic fingerprint ridge patterns.

surface of the fingertips structure. However, other authors explained in different theory such as, the author of [26] describe that its ridge entering from one side of finger then forming a curve and exiting from then same side through where it entered. The author of [14] explained that, in this pattern is a loop pattern from the other side ridges enter recurve and pass out the same side. Nevertheless, the author [22] write-down that prints that recurve back on themselves to form a loop shape. Divided into radial loops (point toward the radius bone, or thump) and ulnar loops (point toward the ulnar bone, or pinky), loops pattern approximately 60 percent of the total population.

2) Whorls: The pattern of ridgeline that illustration as a cycle format on the surface of the fingertips structure. There are four group of whorls: plain (concentric circles), central pocket loop (a loop with a whorl at the end), double loop (two loops that create an S-like pattern), and accidental loop (irregular shapes). The author of [26] proposed that ridge which form a circle like structure in the fingerprint but the author of [14] in this pattern the ridge are usually circular. Nevertheless, the author [22] explained that form circular or spiral patterns, like tiny whirlpools. Whorls pattern make up about 35 percent of the total population.

3) Arch: The pattern of wave shape that rises between the gap of started and ended point of ridgeline format on the surface of the fingertips structure. It is one type of ridge, which is seen like entering from one side and rises in middle forming "a" arc and exit from other side [26]. Tent arches rise to a shaper point than plain arches. The author of [14] in this pattern from one side the ridges entered make a rise in the center and opposite side generally exit. Nevertheless, the author [22] explained that create a wave-like pattern and include plain arches and tented arches. Arches pattern make up about five percent of the total population.

3.3. Fingerprint Acquisition

In acquisition or enrollment's processing may need to follow several important steps such as fingerprint capture device, enhancement fingerprint image, extraction minutiae point, and store features or samples of minutiae in database. Fingerprint enrollment is an important processing that need to use to capture fin-

gerprint data, analyzing its unique features, and store the result as a digital template.

Fingerprint enrollment is in most cases the first step of a biometric comparison process [7]. During enrollment (or acquisition), individual have to registered their biometric characteristic via biometric devices with the system (preprocessing and features extraction) and stored their biometrics template (minutiae results) into the database are acquired, called fingerprint enrollment. A biological or behavioral trait (*i.e.*, submitted from a subject or fingerprint) called delivered and subsequently (*i.e.*, live from a subject or fingerprint scanning) called captured. Fingerprint system will use only samples (templates results) for storage and later comparison. Features template can be use after enrollment or registered done. Information was designing in a biometric system as respectively the "reference sample(s)" and the "reference template(s)" [7].

Fingerprint acquisition steps can produce a good or bad quality depending on acquisition devices or fingerprint scanner and the condition of fingertips skin (dry, wet, normal, clean, injury, dirty, or imprint). Fingerprint acquisition needs the first image from a fingertip and extraction the pattern of ridges and valleys in image and matches the pattern in pre-scanned images. Most of scholars and researchers are propose many problems of fingerprint image quality happen with a lower quality of scanner devices. Different acquisition sensor is different quality of fingerprint image. Fingertip skin also makes a lot of problem when fingertips skin are dry, imprint, dirty, wet, or injury. Different condition of fingertip skin is different quality of fingerprint image. In practical purpose are proposing to use a high quality fingerprint scanners or devices with correct using of fingerprint before scanning. If using high quality fingerprint sensor, clean fingertip, and use correct direction of fingertip to printing on device could be produce a good quality of fingerprint image and can also be improved at the algorithm level (*i.e.*, through software).

Acquisition processing needs a good quality image to analysis. A poor quality biometrics may not be worth including as part of a watch list. Where the quality is insufficient, the biometrics will be likely to miss genuine matches and may generate a high number of false acceptances [6]. The measurement and management of biometric image quality is an important aspect of ensuring an accurate biometric system. Each modality has its own quality measures, for instance for face there are issues such as lighting, pose and head coverings. Any factor that degrade or obscures the biometric during the enrollment process will affect to search and matching capability of the system.

3.4. Fingerprint Pre-Processing

Fingerprint Enhancement indicates to making fingerprint image quality better. Fingerprint data is the main concept for fingerprint analysis system. Good quality image is required. Biometric recognition is recognition of individuals based on his/her biological and behavioral characteristics, encompassing biometric verification and biometric identification [27]. Biometric recognition in high di-

mensional data usually is expected to be more powerful. A multimodal biometric system uses multiple applications to capture different types of biometrics and allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements [5]. In addition, biometric recognition is usually a statistical rather than deterministic outcome; such as, it is liable to errors. There are two main parameters to be consider in connection with a biometric system are first the false rejection rate (FRR) and second the false acceptance rate (FAR) [27]. Quality of biometric data is poor quality may lead to higher FRR and FAR. While FAR increases security risks for the system, a false rejection often causes some follow-up procedures that can be privacy-invasive to the individual [16].

Enhancement methodology is the most important processing in the fingerprint system. In this processing may need a number of utmost steps to execution after received an image from acquisition sensor for both enrollment and matching processing methodology. The enhancement fingerprint image needs an algorithm checking and evaluating to improve good quality image. The quality of fingerprint image from live-scan or sensor device may be met some problems behind the scene according to the quality of scanning devices or fingertips condition (wet, dry, or normal). With different sensor devices will received different result of fingerprint image. Light of sensor and measurement of each device may not the same. In this paper, I propose to use a digitalPersona 4500 fingerprint reader to capture a fingertip from individuals. For human activities may need to be trained how to use the right printing direction with a cleaning fingers. Fingertip's condition is an important for acquisition processing step. Good sensor and clean fingertips could be produced high quality fingerprint image. High quality fingerprint image is an utmost for fingerprint system execution to extract features and matching minutiae are working properly.

Fingerprint image enhancement is an essential preprocessing step in fingerprint recognition applications and is a technique performed to make the image clearer than the original image [28]. Fingerprint recognition system using enhancement algorithm methods that needed to increase the contrasting between ridges and valleys and for connection the false broken points of ridges due to insufficient mount of black color (ridgelines). Enhancement algorithm is an important step in any applications execution based authentication system and used to correct noisy in fingerprint surface. Ridgelines are present by black or dark gray color and valleys gap narrow is present by white color. The noises, errors, and broken ridges are arise with a poor skin condition, varying finger pressure while acquisition or enrollment, sensor noise and dry, wet or oily fingers. Enhancement algorithm is a preprocessing algorithm work with original image to created clearer ridges and valleys before extract features of minutiae.

3.5. Fingerprint Extraction Minutiae Points

A good quality image is an essential for minutiae extraction. However, sometimes the image quality might poor due to various reasons and hence it becomes

necessary to enhance the fingerprint image before minutiae matching of fingerprints.

Minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the uniqueness of a fingerprint image. For good quality fingerprint image may contains around 25 to 80 minutiae depending on the fingerprint scanner resolution and the placement of finger on the sensor. Minutiae can define as the points where the ridgelines end of fork. Therefore, the minutiae points are the local ridge discontinuities and can be of many types (See Table 2) below.

In this paper will be introduce a methodology to extraction minutiae point in C# (C-sharp) programing with five following steps: 1) binarization, 2) thinning, 3) minutiae location, 4) removable spurious minutiae, and 5) classification minutiae.

3.5.1. Binarization Technique

The black and white image (called binary image) are transforming into two parts (object and background). The object is often shown as black and background is often shown as white [29]. In this paper the object is refers to ridgelines on fingerprint surface. This processing will be execution after image has been enhancement and accurate the quality of image is good to be accepted. Binarization technique will be analysis on each pixel of image after calculated the average pixels. To examine the average bright color has the limit of its minimum and maximum. The threshold calculated is 126. The pixel is black (or 1) based on pixels less than 126 and the pixel is white (or 0) based on pixels bigger than or equal 126. The methodology to divide these two parts is according to analysis based on if…then condition on threshold while the wide range of pixels is 255. If the color of each pixel are brightness than the average will determine the pixel as white and beside this will determine the pixel image to black (See Figure 4).

Table 2. Fingerprint minutiae categories.

Type of Minutiae	Description
Ridge ending	Abrupt ending of a ridge or the point where the ridge ends suddenly.
Ridge Bifurcation	Divides the single ridge into two ridges or the point where a single ridge branches out two or more ridges.
Ridge ponds, Lake or enclosure	A single ridge bifurcates and rejoins shortly and continues as a single ridge or the empty space between two diverging ridges.
Short ridge, islands or independent ridge	A ridge begins and ends after travelling a short distance. Ridge islands are slightly longer than dots and occupy a middle space between two diverging ridges.
Ridge Dots	An independent ridge having same length and width or very small ridges.
Spur	A short ridge with bifurcation extended as long ridge or a notch protruding from a ridge.
Crossover or bridge	A connecting ridge between two parallel running ridges. Bridges are the small ridges that join longer adjacent ridges. Crossovers are form when two ridges cross each other.

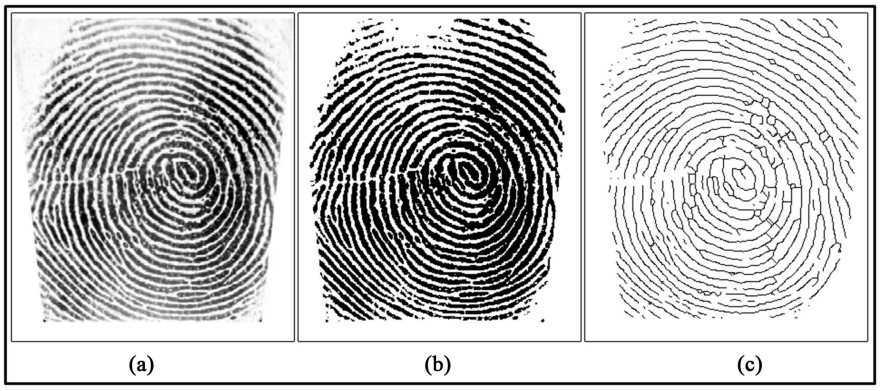

Figure 4. Binarization processing and thinning fingerprint. (A) Original fingerprint; (b) Binarization fingerprint; (c) Thinning fingerprint.

Threshold is the technique to consider focused on finding the global threshold. The main black and white pixel value of each image is determined. The pixels widely range in between pixel value is use to separate the object (black) and background (white). This algorithm used the quality of the result ultimately depends on the complexity of the image.

3.5.2. Thinning Technique

Thinning is a technique that used to reduce the ridgeline of fingerprint from thick lines to a single line or pixel. This thinning function performs a thinning object on binarization (0, 1) image. Thinning algorithms literature has more proposed until now. For good thinning algorithms are based on efficient results in term of thinning rate, speed, number of connected components, peak signal to noise ratio, mean square value, and so on. Among those algorithms, ZhangSuen (co-authors of Zhang and Suen) thinning is the one most frequently used (See **Figure 5**). ZhangSuen thinning has been execution in binarization processing. Thinning algorithms used to reduces the amount of data, time and object analysis to thinned patterns. Thinning object is an utmost fundamental of the digital image processing for pattern recognition applications, for instance pattern recognition, fingerprint classification, and medical application etc. Thinning algorithms can be classified in one of two broad categories [30] including iterative thinning algorithms and non-iterative thinning algorithms.

Iterative thinning algorithms was divided into two parts (parallel and sequential) works on the pixel by pixel based thinning and examine the pixels until the result is obtained. Sequential thinning takes place in predetermined order in which processing take place in fixed sequence. In sequential pre-determined order is followed and deletion of point will depend upon the $(n-1)^{\text{th}}$ iteration that all the operations performed so far [31]. Zhang and Suen was optimized iterative algorithms are discussed what are the steps on the methods. Parallel thinning only the result that remains after the previous iteration is taken in consideration. Iterative parallel thinning algorithm is working on 3 by 3 neighborhood (by Zhang and Suen).

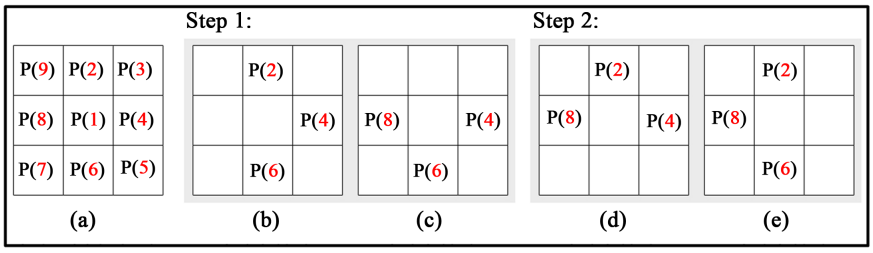

Figure 5. ZhangSuen (3 by 3) pixels neighborhood and two steps processing. (a) Zhang-Suen 3 by 3 pixels neightborhoods; (b) P(2), P(4), P(6) pixels is black; (c) P(4), P(6), P(8) pixels is black; (d) P(2), P(4), P(8) pixels is black; (e) P(2), P(6), P(8) pixels is black.

In Zhang and Suen algorithms works on two-iterations combined with direction approach. The result will be obtaining the skeleton from the binarization image and pixels are removable or replaced a pixel color to white will be satisfies in two steps below:

Step 1:

1) $2 \leq B(P(1)) \leq 6$
2) $A(P(1)) = 1$
3) $P(2) * P(4) * (P(6) = 0$
4) $P(4) * P(6) * P(8) = 0$

Step 2:

1) $2 \leq B(P(1)) \leq 6$
2) $A(P(1)) = 1$
3) $P(2) * P(4) * (P(8) = 0$
4) $P(2) * P(6) * P(8) = 0$

3.5.3. Define Minutiae Location Technique

To compute each location of minutiae that founded on the fingerprint thinned surface with 3*3 pixels window by comparing to the central pixel with eight neighborhoods pixels to determine location of each type of minutiae. Ridgeline ending have four types and bifurcation ridge have four types are most commonly used (See **Figure 6**).

3.5.4. Removable Spurious Minutiae Technique

There is no one algorithm is perfect after thinning fingerprint image pre-processing. Noisy or spurious minutiae may appear or generated by subsystem. Spurious minutiae or noisy is the problem for matching minutiae. For any spurious or noisy that rises up with ridgeline on object will removed or corrected from the fingerprint surface. Spurious minutiae that should be satisfied, in case of two minutiae distance are less than six pixels length will classified to the spurious minutiae type by the subsystem.

3.5.5. Classification Minutiae Technique

Two most commonly used in detection minutiae are ridge termination (ending) and ridge bifurcation. This technique will used after the performance on thinned images. The technique uses a sample window, 3 by 3 pixels wide to detect by key features such as termination and bifurcation. It is a matrix formula. If neighborhood of the central pixel containing only one pixel is black, the system will classified these kinds of ridge to ending point refers to the first type. Whereas, in case of neighborhood of the central pixel containing three pixels are black, the

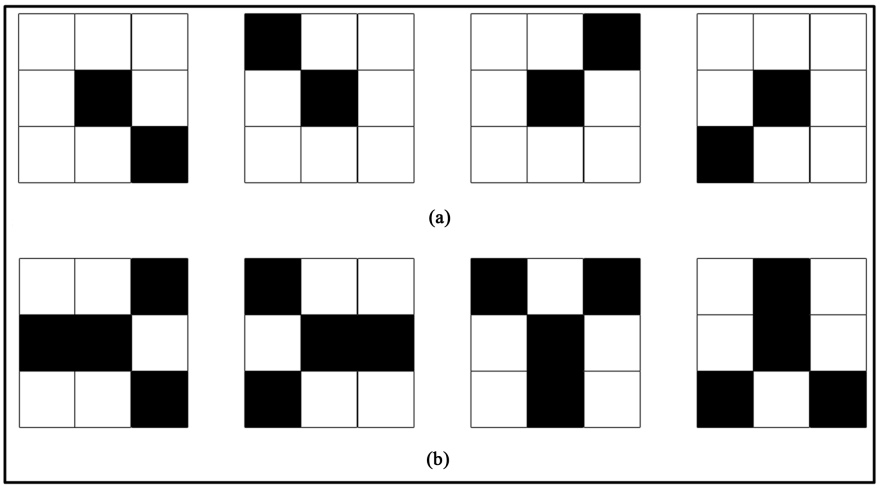

Figure 6. Minutiae of ridgeline ending and bifurcation. (a) Ridgeline ending minutiae; (b) Ridgeline bifurcation minutiae.

system will classified these kinds of ridge to bifurcation refers to the second type (See Figure 6). Two classification has been proposed in this paper, first is ridgeline ending and second is ridge bifurcation.

4. Fingerprint Matching

Matching fingerprint are used minutiae on the fingerprint to compare with each other. The two fundamental principles immutability (ridge patterns never change during the lift time) and uniqueness (distinct ridge patterns on different fingers of the dame individual) are used in identification of individual's fingerprint [20]. No match is perfect in both verification and identification [32]. If match is found or not based on a threshold value by using real minutiae points to compare each other. It consists of finding the best alignment between the compared fingerprints before processing with the comparison step to maximize the score that quantified the quality of the matching [33]. The fingerprint biometric has its own strength and limitations listed in the (See Table 2). The spurious minutiae are the problem for accuracy of matching. Good spurious minutiae removal is the common key point for good matching minutiae.

The author of [34] described that the most of existing fingerprint matching approaches can coarsely classified into two families based on different features: minutiae based algorithms and global feature-based algorithms. Minutiae-based algorithm is to maximize the number of matching minutiae pairs between two fingerprints and the local minutia topologic structures are widely used in minutia matching methods since local areas suffer less from non-linear distortion [34]. The most popular global feature-based are remains to fixed-length feature was extracted from the region around the reference point after filtering by a bank of Gabor filters that response to different ridge orientation [34]. However, the author of [12] explained that the most commonly techniques that used for fingerprint matching are divided into three approaches as the following:

1) Minutiae-based: Minutiae is a majority for fingerprint identification technique. It is the identification of minutiae points along with their relative position on finger. Minutiae refers to the points where the ridgelines terminate or fork are call minutiae whereas according to Galton, each ridge is characterized by numerous minute peculiarities and there are two fingerprints match if their minutiae are matched.

2) Correlation-based: This technique using match two fingerprints are aligned and the correlation is computed for corresponding pixels, however, as the displacement and rotation are unknown it is necessary to apply the correlation for all possible alignments. It is based on abundant gray scale information but it can be bad with quality data.

3) Pattern matching or Ridge feature based: This technique are based on series of ridges as opposed to discrete points which forms the basis of ridge feature based. It compares the basic fingerprint patterns between claimant and a store fingerprint templates. A matching using ridges feature in form of finger code consists of computing the difference of two fingers code vectors (query and reference).

Among three matching algorithms approach, the minutiae-based algorithms is the most recommended and very sensitive to the accuracy of the minutia detection and orientation computation. Minutia feature is only using for matching.

5. Conclusions and Future Works

This paper has focused much works in theory of biometric fingerprint, enhancement quality of image, extraction minutiae technique and matching fingerprint. In practical, the authors are designed application in C# to certify that all theory proposed can adopt. In fingerprint enhancement and matching system using U.R.U 4500 digital Persona fingerprint sensor to capture fingerprint surface from individuals, the quality of fingerprint images has been used for brightness and Gabor algorithms to enhance the light and increasing ridges wide (more black). In extraction minutiae technique has been used Zhangsuen algorithm to thinning ridgelines from binarization image. After that defined the location of each minutiae point and correction of any spurious minutiae that generated after thinned processed. All minutiae that extracted have been classified into two categories which are ridge ending and bifurcation. The last is matching minutiae of two fingerprints by comparing live-scan fingerprint to the template fingerprint stored in the database. Technique used to compare in this application based on minutiae-based algorithm.

Overall, this paper is not studied and evaluated to the large sample size database of fingerprints and does not focus on children and older, too.

For the further work should carry out in field of:

- Extraction and matching minutiae point based on speed and other more minutiae points, not only works with these two minutiae types such as ridge ending and bifurcation.
- Works with millions population including children and the older for gov-

ernment system.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Glaeser, A., Sonderegger, B. and Peter, M.U. (2012) 1913-2013 the Fingerprint: 100 Years in the Service of the Swiss Confederation. Federal Department of Justice and Police, Bern.

[2] Perichappan, K.A.P. and Sasubilli, S. (2017) Accurate Fingerprint Enhancement and Identification Using Minutiae Extraction. *Journal of Computer and Communications*, **5**, 28-38. https://doi.org/10.4236/jcc.2017.514003

[3] Jain, A.K., Nandakumar, K. and Ross, A.A. (2011) Introduction to Biometrics. Springer, Berlin. https://doi.org/10.1007/978-0-387-77326-1

[4] Jain, A.K. (2007) Biometric Recognition. Vol. 449, Nature Publishing Group, Berlin. https://doi.org/10.1038/449038a

[5] Delac, K. and Grgic, M. (2004) A Survey of Biometric Recognition Methods. 46*th ISEM*, Zadar, 18 June 2004, 184-193.

[6] CTED and UNOCT (2018) United Nations Compendium of Recommended Practices for Responsible Use and Sharing of Biometrics in Counter-Terrorism. Biometrics Institute, London.

[7] Kindt, E.J. (2013) Chapter 2: An Introduction into the Use of Biometric Technology in Privacy and Data Protection Issues of Biometric Applications. In: *A Comparative Legal Analysis*, *Law*, *Governance and Technology*, Springer Science + Business Media, Dordrecht, 15-85. https://doi.org/10.1007/978-94-007-7522-0_2

[8] Wolf, P., Alim, A., Kasaro, B., Saneem, M., Namugera, P. and Zorigt, T. (2017) Introducing Biometric Technology in Elections. International IDEA, Stockholm.

[9] Lee, H.C. and Gaensslen, R.E. (2001) Advances in Fingerprint Technology. 2nd Edition, CRC Press, Boca Raton.

[10] Barnouti, N.H. (2016) Fingerprint Recognition Improvement Using Histogram Equalization and Compression Methods. *International Journal of Engineering Research and General Science*, **4**, 685-692.

[11] Annapoorani, D. and Caroline Viola Stella Mery, M. (2014) A Survey Based on Fingerprint Recognition—Minutiae. *International Journal of Science and Research*, **3**, 607-611.

[12] Pawar, S., Ghodke, A., Gaikwad, B.P. and Wakhure, G.P. (2016) A Survey of Minutiae Extraction from Various Fingerprint Images. *International Journal of Advanced Research in Computer Science and Software Engineering*, **6**, 169.

[13] Zhang, D., Song, F.X., Xu, Y. and Liang, Z.Z. (2009) Advanced Pattern Recognition Technologies with Applications to Biometrics. IGI Global, Hershey.

[14] Vats, S. and Harkeerat Kaur, G. (2016) A Comparative Study of Different Biometric Features. *International Journal of Advanced Research in Computer Science*, **7**, 169-171.

[15] CSO US (2019) 10 Physical and Behavioral Identifiers That Can Be Used for Authentication.

https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html

[16] Cavoukian, A. and Stoianov, A. (2007) Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy. Information and Privacy Commissioner of Ontario, Toronto.

[17] Ryan, R., Evanoff, V., Norton, R.E. and Harvey, C. (2008) Biometric Technology Application Manual, Volume 1. Biometric for Nation Security (BiNS V).

[18] Pato, J.N. and Millett, L.I. (2010) Biometric Recognition: Challenges and Opportunities. National Academy of Sciences, Washington DC.

[19] Mantra (2019) Our Biometrics (Fingerprint Scanner). https://www.mantratec.com/Solutions/Biometric-Technologies

[20] Sabhanayagam, T., Prasanna Venkatesan, V. and Senthamaraikannan, K. (2018) A Comprehensive Survey on Various Biometric Systems. *International Journal of Applied Engineering Research*, **13**, 2276-2297.

[21] BioLab. (2019) Fingerprint [Online]. http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=111&pathSubj=111&Req=&

[22] NFSTC (2019) Principles of Fingerprint Analysis [Online]. http://www.forensicsciencesimplified.org/prints/principles.html

[23] Gemalto (2019) Automated Fingerprint Identification System (AFIS): A Short History [Online]. https://www.gemalto.com/govt/biometrics/afis-history

[24] Jain, K., Patrick, F. and Arun, A. (2008) Handbook of Biometrics. Springer Science Business Media, Berlin.

[25] Wikipedia (2019) Fingerprint [Online]. https://en.wikipedia.org/wiki/Fingerprint

[26] Patel, U. (2015) A Study on Fingerprint (Biometrics) Recognition. *International Journal of Engineering Science*, **1**, 1-6.

[27] Italiana, V. (2014) Guidelines on Biometric Recognition and Graphometric Singapore. Annex A to the Garante's Order.

[28] Abdelwahed Motwakel Eltayeb Ismaeil, M. Eng. (2017) Fingerprint Image Quality Analysis and Enhancement Using Fuzzy Logic Technique. PhD Dissertation, Faculty of Computer Science and Information Technology, Sudan University of Science and Technology, Khartoum.

[29] Otsu, N. (1979) A Threshold Selection Method from Gray-Level Histograms. *IEEE Transactions on Systems, Man, and Cybernetics*, **9**, 62-66. https://doi.org/10.1109/TSMC.1979.4310076

[30] Boudaoud, L.B., Sider, A. and Tari, A. (2015) A New Thinning Algorithm for Binary Images. 3*rd International Conference on Control, Engineering & Information Technology* (*CEIT*), Tlemcen, 25-27 May 2015, 1-6. https://doi.org/10.1109/CEIT.2015.7233099

[31] Bansal, P. and Kaur, B. (2015) A Review on Thinning in Digital Image Processing. *International Journal of Science and Research*, **5**, 228-231.

[32] Krishnam Raju, K.V., Nishmitha, P., Mounika, P., Ajeeth, N., Krishna Sandeep, V. and Kishore Raju, N. (2019) Implementation of Fingerprint Recognition System Using Minutiae Score Matching. *International Journal of Recent Technology and Engineering*, **8**, 62-67.

[33] Nedjah, N., Wyant, R.S., Mourelle, L.M. and Gupta, B.B. (2019) Efficient Fingerprint

Matching on Smartcards for High Security. *Information Sciences*, **479**, 622-639. https://doi.org/10.1016/j.ins.2017.12.038

[34] Zhang, F.D., Xin, S.Y. and Feng, J.F. (2019) Combining Global and Minutia Deep Features for Partial High Resolution Fingerprint Matching. *Pattern Recognition Letters*, **119**, 139-147. https://doi.org/10.1016/j.patrec.2017.09.014