USMANU DANFODIYO UNIVERSITY, SOKOTO

(POST GRADUATE SCHOOL)

TITLE PAGE
A CLONED ACCESS PREVENTION IN BIOMETRIC SYSTEM

A Dissertation

Submitted to the

Postgraduate School,

USMANU DANFODIYO UNIVERSITY, SOKOTO, NIGERIA

In partial Fulfilment of the Requirements

For the Award of the Degree of

MASTER OF SCIENCE (COMPUTER SCIENCE)

BY

Oni, Akindayo Sunday

Admission. No.: 14210310005

Department of Mathematics

DECEMBER, 2020.

DEDICATION

This dissertation is dedicated to Almighty God, Who helped and saw me through difficult moments while embarking on this journey.

CERTIFICATION

This dissertation by ONI, Akindayo (14210310005) has met the requirement for the award of the Degree of Master of Science (Computer Science) of the Usmanu Danfodiyo University, Sokoto, and is approved for its contribution to knowledge.

External Examiner Date

Prof. Ahmed Garko

Dr. Ahmad Tambuwal Date

Major Supervisor

Dr. A. B. Muhammad Date

Co-Supervisor I

Dr. B. Y. Isah Date

Co-Supervisor II

Dr. A. I. Garba Date

Ag. Head of Department

ACKNOWLEDGEMENTS

My unreserved gratitude goes to the Almighty God, the creator of heaven and earth for His unwavering mercies towards me over these years. May His name forever be praised. I am particularly indebted to my late parents Mr. and Mrs. J. K. Oni who taught me to be hardworking and depend on God for survival. It is so sad that you are not alive to see me growing bigger and better. My lovely parents, rest on till we part no more. Thank you!

I want to specially appreciate my supervisory team; Dr. A. Y. Tambuwal, Dr. A. B. Muhammad and Dr. B. Y. Isah for their interests, patience, numerous corrections, guidance and contribution towards the success of this thesis.

My profound gratitude to leaderships of The Redeemed Christian Church of God, Region 18, Sokoto Province for giving me the permission to pursue this additional degree and platform to be among end time soldiers. I want to appreciate Pastor Tunde Oduwole (SATGO House fellowship to G. O.) for the assistance when it matters, God bless you Sir. Prof. Mojiminiyi has been an instrument of motivation and encouragement towards this program, thank you Sir. Prof. and Dr. (Mrs) Faleke, thank you, for the support received in the course of this research, your contribution towards my school fees when I ran to you for help. I also wish to sincerely thank the head of Department (Dr. I. Garba), the head of Computer Science Unit (Dr. A. Roko) as well as the entire staff and postgraduate students of the Department of Mathematics whose criticisms and contributions helped improve the quality of this research work. Thank you all for your contributions.

My special appreciation also goes to my siblings; Mrs. Omonike Akinpelu, Mr. Oluwasegun Oni, Mr. Adeleke Oni, Mr. Oluwadamilare Oni and Mr. Oluwabukunmi Oni for believing in me and supports received during the period of this pursuit. Also, I need to specially appreciate God's wonderful heritage in my life; Ifeoluwa and Enoch Oni, I

really stressed both of you, at a time we attended lectures together, even up to the period of doing the correction of this thesis, you stayed with me from morning till night in school. Yet, you never grumbled or complained. We laughed at stress together. Thank you for been there for daddy, it means a lot to me. Oluwaseun, thank for your contributions during and after period of my studies, without those experiences, I will never know I am this strong.

Finally, I would like to say a big thank you to the family of Mr. and Mrs. David Awodi for been there, during my troubled moments. My colleagues and course mates: Ishaya Emmanuel, Daniel Dauda, Yese Solomon and a host of others too numerous to mention. You people are wonderful and made my stay in UDUS a memorable one. Thank you all.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Biometric is human generated signal or attribute for authenticating a person's identity. Its operations is based on behavioral/physical features. Previous studies have clearly shown, that the conventional fingerprint recognition systems are vulnerable to cloned or fake attacks, and there are many existing systems that need to update their anti-cloning capability inexpensively. This research work centers on image quality-based clone detection method to address this problem. Samples of real and cloned fingerprints were taken through fingerprint sensor resolution above 500dpi and analyzed. Experimental results demonstrated that, the proposed method is better because, the system is trained to differentiate between real and cloned fingerprint and cheaper to implement. Therefore, this method could be recommended for use to authenticate person's identity using fingerprint identification, verification and authentication in biometric system.

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

This chapter introduce the development of biometrics, different approaches to security, fingerprint application in brief, statement of the problem, aim and objectives, scope of the study and contribution to the knowledge of the research:

The word “biometrics” comes from the Greek language and is derived from two words; bio (life) and metric (to measure) Gayathri & Sridhar, (2014). Biometrics is the technology used to measure and analyze personal characteristics, both physiological and behavioral Bansal, Sehgal, & Bedi, (2011). These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity Kudu, (2016). The developments in biometrics recognition of a person has led to improvements in reliability and accuracy, in the sense that an individual biometrics characteristics can be taken and such can be used to identify individual anytime and anywhere weather locally or internationally (Afsar, Arif & Hussain, (2004)). It has been established that no two people share the same biometric features and if there is, research has revealed that, it is in the ratio 1:64,000,000 Zhang, (2010) and NSTC, (2006). The testing of biometric authentication devices has been the subject of several papers Mojtaba S., Cristinel M., & Wamadeva B., (2010), Kumar K., Kumar & Kumar D., (2011), Khan M., Khan T., Bailey D., & Kong Y., (2016), Shinde & Bendre, (2015), Sahu & Shrivas, (2016), Sudiro, & Yuwono (2012).

One of the first to be published was Van der T., Putte & Keuning J., (2000). He described two ways to create dummy; one method without cooperation and one with cooperation. Creating fingers with cooperation was performed pressing the finger into

plaster to create a mold, and then use silicon waterproof cement or liquid silicon to create a finger using the mold. When no cooperation, they recommend trying to get a latent fingerprint, since the quality should be good and it would be the correct finger. The print was enhanced using fine powder and removed from the reader using scotch tape. Then the print was transferred to a photo sensitive copper plated circuit board (PCB) to create a mold. The mold might be deepened further using a dremel multi-tool before the artificial finger is created using silicone. The work confirmed that it is very much possible to create a similar fingerprint, despite the fact that the possibility of getting same fingerprint is ratio 1:64 million in human. The molded fingerprint was able to bypass the biometric security measure in place.

Ain N., Shaukat N., Nagra A. & Raja G., (2018), proposed an efficient algorithm for fingerprint recognition using minutiae extraction. The technique was good because, different schemes were used which gave the work an edge over previous works. The proposed work Ain N., (2018) used different schemes i.e. correspondence computation and similarity computation. For correspondence based computation, all minutiae points get assigned with two descriptors: texture descriptor and minutiae descriptor while in similarity based computation, a feature vector Gnanasivam, P. & Muttan., (2010) is extracted from matching result, and the result is converted to feature vector using vector classifier. Moreover, during matching phase of two sets of minutiae Ain N., (2006), minutiae template and minutia to be verified are aligned for final matching. Thereafter, alignment-based matching algorithm is used to establish a level of correspondence among obtained minutiae.

1.2 Fingerprint application in brief

Today, the employment of fingerprints has increased considerably with applications in different scenarios such as social identification, physical access control to

the facility or network, and obtaining permission to cross the border. It has become accepted as a very secure method for identification and authentication of individuals. A solution to increase the security of these methods is that of using cloned prevention or spoofing prevention example of cloned fingerprints as presented in fig.1.1 (a) and (b).

Figure 1. 1: (a) Fake hand (b) Cloned/Fake Fingerprint

1.3 Statement of the problem

Despite various schemes proposed in the previous works especially; Ain, etal., (2018). Hackers use different means to override biometric systems through cloned materials, majority of the works earlier proposed concentrated majorly on locations and patterns of the minutiae or minutiae based matching and correlation based matching Tiwari & Sharma, (2012), Peralta, Galar, Triguero, Paternain, Garcia, Barrenechea, Benítez, Bustince, & Herrera, (2015), these mechanisms are good but hackers used play dough, gelatin, silicon, candle wax, high resolution pictures and prosthetics to override the biometric schemes proposed. Attacking biometric systems via the input port and attacking the biometric data warehouse are other problems which the earlier works did not profer solutions. Since fingerprint of an individual can be cloned, necessity was laid to find a more secured way of preventing cloned fingerprints by subjecting the fingerprint image to analysis. The previous analysis was on fingerprint minutiae, which is not effective enough to limit the hackers from having access into biometric systems. The intention of this work is to concentrate on the prevention of cloned fingerprints access in

biometrics systems by analyzing the fingerprint sample through additional features (i.e. minutiae, incipient and crease) to decide whether to grant access or denied access.

1.4 Aim and objectives of the Research

The aim of this work is to propose an improved security system that utilizes minutiae, incipient and crease to detect fake fingerprints. The aim will be actualized through the following objectives:

i. To obtain real and cloned images through fingerprint sensor.
ii. To develop an algorithm for processing of the real and cloned fingerprints.
iii. To train the system to note and differentiate between the features of real fingerprint i.e. minutiae, incipient and crease from cloned fingerprints.
iv. To compare and evaluate proposed system with the previous works.

1.5 Scope of the study

The work focuses on fingerprint system with a unimodal system in mind and not bimodal system in biometric.

1.6 Research Contributions

The study comprises of the following contributions;

i. The work provides a more secured way of protecting devices and systems from the hackers.
ii. The work reveals other features of fingerprints and how they can be used to provide better and reliable security systems.
iii. The work shows a cheaper way to secure systems.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The previous chapter has discussed the motivation for this work by presenting the problem statement. The aim and objectives are also discussed in order to address the problem related to the fingerprint cloning and present a number of existing approaches which aimed to address this problem with varying degree of success. This chapter will also discuss the concept of security, cloning fingerprint, the minutiae, the incipient, the crease, previous works on Fingerprint biometric, the limitations of the works then, the reviewed literatures, the summary and literature review table:

2.2 The Concept of Security

Security is freedom from, or resilience against, potential harm caused by others. Beneficiaries of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change (Wikipedia, 8/11/2019). Security methods can be divided into three categories: something you know (password), something you have (key, smart card) and something you are (biometrics) Bana, (2011), (Algarra, Radotić, Kalauzi, Mutavdžić, Savić, Jiménez-Jiménez, Rodríguez-Castellón, da Silva, J.C.E. & Guerrero-González, (2014)). A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services Conti, (2010), (Jain Feng & Nandakumar, (2010), Chaudhari, Patnaik, & Patil, (2014). The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else Cao & Jain, (2018), Bana, & Kaur, (2011). Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes (Cao Yang, Tao, Li, Zang, & Tian,

(2010)), Peralta (2015), (Moshen, Farhan, & Hashem, (2004)), Ishpreet & Raman, (2012), these systems are vulnerable to the wiles of an impostor Gonzalez, (2009). Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. The major advantages of this traditional personal identification are that; they are very simple and they can be easily integrated into different systems with a low cost (Choi, Kang, Choi, Jin, & Kim, (2009)).

2.3 Cloning fingerprint

Van der *et al.*, (2000). He described two ways to clone fingerprint; one method without cooperation and one with cooperation. Creating fingers with cooperation was performed pressing the finger into plaster to create a mold, and then use silicon waterproof cement or liquid silicon to create a finger using the mold. When no cooperation, they recommend trying to get a latent fingerprint from the fingerprint reader itself, since the quality should be good and it would be the correct finger. The print was enhanced using fine powder and removed from the reader using scotch tape. Then the print was transferred to a photo sensitive copper plated circuit board (PCB) to create a mold. The mold might be deepened further using a dremel multi-tool before the artificial finger is created using silicone. The work confirmed that it is very much possible to create a similar fingerprint, despite the fact that the possibility of getting same fingerprint is ratio 1:64 million in human. The molded fingerprint was able to bypass the biometric security measure in place.

2.4 The minutiae

Gnanasivam and Muttan, (2010). Proposed an efficient Algorithm for fingerprint preprocessing minutiae extraction. The proposed minutiae based extraction technique for fingerprint matching with enhanced images to increase verification capability of

fingerprints. It used two schemes, which were; matching algorithm correspondence computation and similarity computation. The scheme works better when the image is vertically positioned but if the image during capturing is not vertically aligned on the scanner there will be problem with the result. Also, the Work does not considered other features of the fingerprint like incipient and creases of the fingerprints, it is a known fact that location of minutiae alone cannot prevent the cloners from fooling biometric systems.

2.5 The incipient

Journal of Forensic Identification (1992), incipient ridges may create certain inconsistencies as to their inclusion and value as part of the fingerprint identification process, but they can be a vital factor in determining individuality when approached from their morphological structure and evaluated as to their significance in the clarity spectrum. During the identification process, the value of incipient ridges depends on the clarity of friction ridge structures. Clarity also dictates whether incipient ridges may qualify as nonspecific or accidental characteristics. Incipient ridges are thin, fragmented ridges which appear in the furrows between normal, mature friction ridges. They are narrower in width, do not usually have the same height as normal ridges, and are reported to lack pore structure. Incipient ridges are often called false ridges when fingerprints are classified for ten print searching and filing purposes. Nonetheless, incipient ridges form in the same manner as normal ridges and have the same subcutaneous structures. Ridge units begin developing at different times and at various locations on friction skin. As incipient ridges are formed by ridge unit development, some incipient ridges will mature more than others. The location of ridge structure on the clarity spectrum dictates the level of detail that can be compared. Whether incipient ridges qualify as nonspecific or accidental characteristics depends on the clarity of ridge structures and on the examiner's ability to judge where ridge structures fit in the clarity spectrum.

2.6 The crease

The Hough transform is used to identify secondary crease extraction in a r, θ space. The methods proposed for secondary crease extraction works well and provides information about what areas of an image contains usable linear pattern. Methods for comparison is however not as robust and generates false rejection rate ⊔ 30% and false acceptance rate ⊔ 20% on the proposed dataset that consist of bad quality fingerprint. The methods still makes it possible to make use of fingerprint images earlier considered unusable in fingerprint recognition system.

2.7 Previous works on Fingerprint Biometric

The German computer magazine, Thalheim *et al.,* (2002). Described the easiness of fooling several types of fingerprint sensors, an iris camera and a face recognition solution. Among the discoveries they made were that, it was possible to steal fingerprints from other surfaces by dusting them with fingerprint powder and capture it with an adhesive film before pressing the film gently to a capacitive or optical reader. They also managed to fool optical fingerprint readers using a silicon finger created by pressing a real finger into a wax mold. The paper confirmed the possibility of spoofing or fooling a biometric system.

Matsumoto *et al.,* (2002) and Wahby & Ahmad M., (2013) looked at ways of creating artificial fingers using silicone and gelatin. They first cloned the finger using a mold made of free molding plastic, and then filled it with both gelatin and silicone rubber to create the artificial finger. They managed to fool the optical scanner using the gelatin finger, but not the one made from silicone. In their next experiment, they cloned a residual fingerprint, which was captured on a glass plate and enhanced using a cyanoacrylate adhesive. This was transferred to a photo sensitive copper plated circuit board (PCB) and a gelatin finger was created. All the verification systems tested accepted the artificial

finger more than 67% of the time. The work justifies the vulnerability of the biometric system.

Then, Kaseva & St´en (2003), performed several tests on the Precise Biometrics 100 SC capacitive fingerprint scanner. They were unable to fool the scanner breathing on it as Thalheim *et al.*, (2002). They were also unable to reactivate latent fingerprints on the sensor by pressing gummy bears upon it. They were however able to fool the sensor using a gelatin finger made from a mold created by pressing the finger into hot glue. They also managed to steal a latent fingerprint from a mug using photocopier powder and transfer it to a PCB, which was used as a mold for a gelatin finger, which fooled the biometric sensor.

Sandstr¨om, (2004), published a report on liveness detection in fingerprint systems. She performed an experiment in which she created an artificial finger from a latent fingerprint and enhanced it using a soot powder mixture and a squirrel hair brush. The print was further enhanced in Adobe Photoshop and printed on a PCB, which was used as a mold for the gelatin finger. The fake finger was tested on several of the fingerprint systems at the CeBIT trade fair in Hanover, Germany in 2004, where she had a mean success rate of 67% when using this finger.

Gnanasivam and Muttan, (2010). Proposed an efficient Algorithm for fingerprint preprocessing minutiae extraction. The proposed minutiae based extraction technique for fingerprint matching with enhanced images to increase verification capability of fingerprints. It used two schemes, which were; matching algorithm correspondence computation and similarity computation. The scheme works better when the image is vertically positioned but if the image during capturing is not vertically aligned on the scanner there will be problem with the result. Also, the Work does not considered other

features of the fingerprint like incipient and creases of the fingerprints, it is a known fact that location of minutiae alone cannot prevent the cloners from fooling biometric systems

Ain *et al.*, (2018), proposed an efficient algorithm for fingerprint recognition using minutiae extraction. The technique was good because, different schemes were used which gave the work an edge over previous works. The proposed work used different schemes i.e. correspondence computation and similarity computation. For correspondence based computation, all minutiae points get assigned with two descriptors: texture descriptor and minutiae descriptor while in similarity based computation, a feature vector (Wahby *et al.*, 2013) is extracted from matching result, and the result is converted to feature vector using vector classifier. Moreover, during matching phase of two sets of minutiae (Jie *et al.*, 2006), minutiae template and minutia to be verified are aligned for final matching Thereafter, alignment-based matching algorithm is used to establish a level of correspondence among obtained minutiae. However, the biometric system can be fooled by cloned samples because the work only considered locations and patterns of the minutiae, while other useful features like incipient which is not present in cloned images were not considered which could prevent cloned fingerprints from accessing the biometric system. Moreover, their schemes could not handle the effect of crease if present in the fingerprint sample captured.

2.8 The limitations of the works

The traditional approach to security are not based on any inherent attributes of an individual to make a personal identification thus having number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; Personal Identification Number may be forgotten or guessed by impostors. Security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor.

Furthermore, simple passwords are easy to guess by an impostor and difficult passwords may be hard to recall by a legitimate user.

Therefore, they are unable to satisfy the security requirements of our electronically interconnected information society. The emergence of biometrics addressed some of the problems that plague traditional verification. (Thalheim, Krissler, & Peter-Michael Ziegler (2002)), NTSC (2006). The biometric fingerprint feature characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. The characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing two major improvements: personal biological features which cannot be easily stolen and an individual does not need to memorize passwords or codes Lim & Chin, (2014) and Mao, (2004), Moshen, Farhan, & Hashem, (2004). Since biometrics can better solve the problems of access control, fraud and theft, more and more organizations had considered biometrics a solution to their security problems. This research put into consideration by looking at additional features of fingerprint which are; minutiae, incipients and crease.

2.9 Summary

The biometric system can be fooled by cloned samples because the minutiae of the real fingerprint can be captured. Previous works considered locations and patterns of the minutiae, while other useful features like incipient and crease which cannot be captured in cloned fingerprint images were not considered which could prevent cloned fingerprints from fooling the biometric system. These three features has never been considered in the previous works and these are the area of concentration in this research work.

2.10 Literature review table

YEAR	TYPE	TITLE	METHODOLOGY	MERIT	WEAKNESS
2018	Paper	An Efficient Algorithm for Fingerprint Recognition Using Minutiae Extraction	Correspondence computation and similarity computation.	One than one scheme was used	It can be fooled
2018	Journal	Automated latent fingerprint recognition	Minutiae was extracted	67% restriction was achieved	It can be spoofed
2017	Conference	Latent fingerprint enhancement using Gabor & minutia dictionaries	Gabor filter was used and minutiae dictionaries	An improvement in the old approach	The system is weak
2016	Conference	Biometric Identification System	Used Fingerprint and Knuckle as Multimodality Features	Multimodal system	It was bulky and large memory needed
2016	Journal	A spatial domain scar removal strategy for fingerprint image enhancement	Crease was used in identify an individual	New feature was considered	Not strong to prevent cloned fingerprint
2015	Conference	Enhanced ridge structure for improving fingerprint image quality based on a wavelet domain	The waves produced from the fingerprint ridges was used in identifying individuals	The approach was new and fascinating	The feature considered can be gotten from latent fingerprint
2015	Journal	Learning fingerprint reconstruction from minutiae to image.	The work was on minutiae and its locations on the fingerprint	It does not require large memory	It is prone to spoofing
2014	Conference	Enhancing fingerprint recognition	using minutiae-based and image-based matching techniques	Better approach in using minutiae	Gelatine cloned finger can be used to fool the system
2014	Journal	Fingerprint orientation field reconstruction	weighted discrete cosine transform was used	Approach was new and good	It fails in real scenario.
2014	Conference	Fingerprint detection and using intercalated CdSe nanoparticles on non-porous surfaces		The idea was innovative and new	It was not efficient

2012	Conference	Q-Learning approach for minutiae extraction from fingerprint image	Knowledge of block was used in dife	Introduction of Q block to show clearly the graphical representation of fingerprint	It was not effective
2011	Conference	Fingerprint recognition system for low quality images	Pattern recognition system was used	It simple tomanage	It is too weak
2000	Face Recognitio n Vendor Test (FRVT) in 2000.	Conference	large-scale technology evaluation of multiple commercially available biometric systems	Evaluation of multimodal system	Large memory
2000	Use of vascular patterns for recognition	Paper	Commercially available vascular pattern recognition system	Robust	Complicated
2001	Face recognition is used at the Super Bowl	Paper	To identify wanted individuals entering the stadium	Commercial purpose	Misidentify individuals

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This section describe the methodology use to carry out the research on a cloned access prevention in biometric system. The chapter consist of the introduction, the framework that states step by step approach on how to solve the problem and some necessary diagrams:

3.2 The framework:

Five stages will be involved in finger-scan verification and identification; fingerprint image acquisition, image processing, location of distinctive characteristics, template creation and template matching. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a template/file. The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. Image quality is measured in dots per inch (DPI) – more dots per inch means a higher resolution image.

The problem of cloning prevention can be seen as a two-class classification problem where an input fingerprint image has to be real or cloned. The key point of the process is to find a set of discriminant features which permits one to build an appropriate classifier which gives the real state of the image description in the given extracted set of features. Figure 3.1 (a) (b) gives us details of fingerprint showing the different parts that can be used in securing the biometric systems while figure 3.1c shows the different classes of fingerprints.

Figure 3. 1 **(a)** Sagittal section showing internal detail

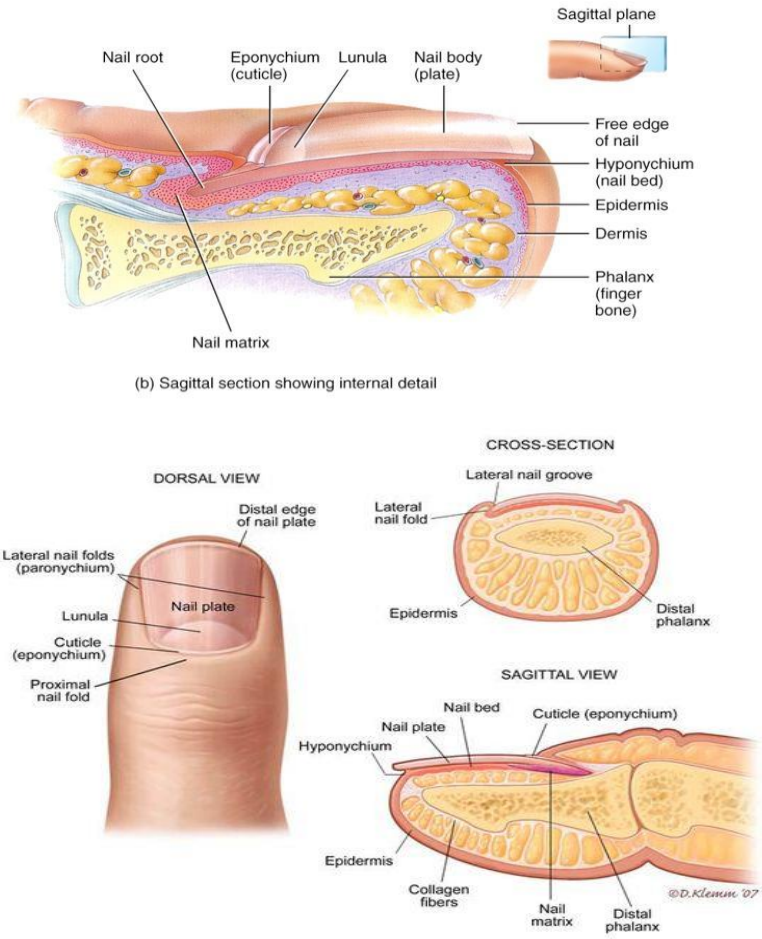


Figure 3. 2: ***Sagittal view of a finger*** **(www.google.com)**

Figure 3. 3*: Examples of fingerprint classes (Putte, 2000)*

This work leveraged on the concept of image processing. There are five stages involved in finger-scan verification and identification,

1. Fingerprint image acquisition
2. Image processing
3. Locating distinctive features between the real and clone fingerprints

4. Template creation

5. Template matching

The whole work centers on fingerprint, fingerprint image acquisition is important because access to biometric systems is based on fingerprint of an individual, both real and samples of real fingerprints that are cloned will be needed. Furthermore, the image has to be processed in order to make it easier to locate the features needed to secure the system. Locating distinctive features between the real and clone fingerprints is necessary because it will be used to train the system. In addition, template creation is used as a standard of what the system should note to know access will be granted or not. Finally, the template created must match with the real fingerprint present in order to have access.

3.2.1 The previous work:

Ain et al., (2018) proposed system for fingerprint recognition consist of two major steps: Feature extraction and feature matching. Initially, fingerprint images from user were taken as an input and some pre-processing techniques were applied to the input image. Next, minutiae were extracted and post-processing techniques (false minutiae removal) were applied. Finally, remaining minutiae points were aligned and matching was performed. Image was divided in small processing blocks of 32x32 window size. A fast Fourier transform formula was introduced to further help in image enhancement, the formula is stated below;

$$\mathrm{F}\left(u,v\right)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f\left(x,y\right)$$

Where U and V were horizontal and vertical elements of 32×32 matrix and ranged from 0 to 31. In $f(x,y)$ represents the pixel value in spatial domain. $\mathrm{F}\left(u,v\right)$ is the pixel

values in frequency domain obtained after taking FFT. The inter ridge distance was calculated by:

$$\text{Inter ridge distance} = \frac{\text{sum of all pixels with value 1}}{\text{Row length}}$$

The equation above was used for the minutiae marking and to eliminate the false minutiae points. Hence, after removal of false minutiae points, left over minutia points were marked. Finally, termination and bifurcations were unified through the following algorithm:

(i) Track a ridge segment of the fingerprint, whose starting point must be terminated by bifurcation.

(ii) Then sum up all the x-coordinates of points present in that particular ridge segment

(iii) After that, divide the above summation and sequentially obtained minutiae locations

The ridge associated with each minutia was represented as a series of x-coordinates (x1, x2…xn) of the points on the ridge. Similarity of correlating the two ridges was derived from;

$$s = \frac{\sum_{i=0}^{m} xi * Xi}{\sqrt{\sum_{i=0}^{m} xi^2 * Xi^2}}$$

Here xi represent the reference minutiae points stored in the template and Xi is the points of the image to be verified. Here, S is greater than 0.8 was used to compute match score

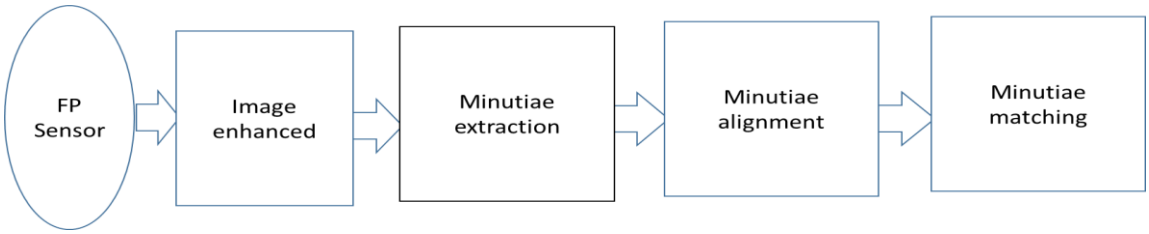


Figure 3. 4: ***Previous work (Ain et al., 2018)***

3.3 Proposed procedures:

Sensing (device for capturing real and cloned fingerprints) Different scan devices from various manufacturers was adopted, figure (a) (b) (c) (d) shows different scanning or sensing devices. A digital image is directly obtained by placing the finger on the surface of a fingerprint reader for preprocesses and processes to continue. The cloned samples were obtained through concessional and unconcessional ways. Images of real and cloned fingerprints were saved in a format that makes them to be readable by the algorithm designed. Further implementation continues in MATLAB and morphological toolbox was used because we are dealing with human skin. In the past, they used numerous technologies e.g. using traditional "ink and paper" method, this is still practicable by many law enforcement agencies which involves applying ink to the finger surface, rolling the finger from one side of the nail to the other on a card, and finally scanning the card to generate a digital image. Optical sensors based on the finger total internal reflection (FTIR) technique are commonly used to capture live-scan fingerprints in forensic and government applications, while solid-state touch and sweep sensors silicon-based devices that measure the differences in physical properties such as capacitance or conductance of the friction ridges and valleys dominate in commercial applications. The most significant characteristics of fingerprint readers are their resolution and capture area. The standard fingerprint image resolution in law enforcement applications is 500 pixels per inch (ppi), but some readers now have dual-resolution capability (500 and 1,000ppi).

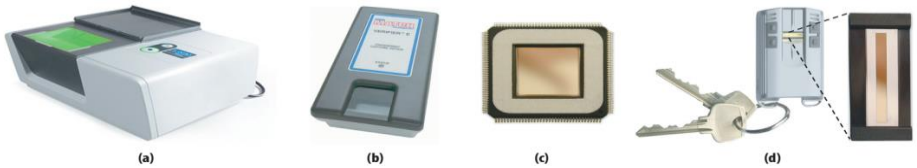


Figure 3. 5: ***(a) Fingerprint readers: Cross Match (www.crossmatch.com) optical 10-print, (b) single-print scanners; AuthenTec (www.authentec.com) solid-state (c) touch and (d) sweep sensors embedded in Privaris plus ID (www.privaris.com) devices.***

3.3.1 Optical scanners:

The pictures above fig. 3.3 shows the oldest method of capturing and comparing fingerprints, it relies on capturing an optical image like a photograph & then using algorithm to detect unique patterns on the surface such as ridges or unique marks. Also, Security of this type of scanner depends on the resolution of photographing the fingerprint. However, it can be easily fooled by photograph or forged image, 2D image, prosthetic or pictures with good quality.

3.3.2 Capacitance scanners

Capacitance scanners are mostly found on fingerprint scanners today, it uses electronic components called capacitors. It does not create an image instead; the scanner uses a small capacitor, circuits to collect data about the fingerprint unlike optical scanners. Also, capacitors can store electrical charges, connecting them up to conductive plates on the surface. This allows them to use track details of the fingerprint. Nonetheless, the risk there, is hardware/software hacking.

3.2.3 Ultrasonic scanners

Ultrasonic hardware consists of both an ultrasonic transmitter and a receiver. The pulse is transmitted against the finger and some of this pulse is absorbed while some bounce back to the sensor, depending on the ridges, pores and other details unique to fingerprint. The returning signal is detected by a sensor that can detect mechanical stress and is used to calculate the intensity of the returning ultrasonic pulse at different points

on the scanner. This particular scanner has better performance over the once earlier discussed. It is considered to be more suitable for this research work coupled with its higher resolution.

3.4 Proposed Algorithm for the Multi-level Processing:

3.4.1 Proposed Algorithm for the first phase:

i. Use fingerprint sensor to acquire images of both real and fake

ii. Convert the images into readable format

iii. Integrate the algorithm designed in Matlab,

iv. use morphological toolbox in Matlab
for multi-level analysis of the images iteratively

v. Create templates for the real samples after the analysis

vi. Train the system to note the features and characteristics of real to clone

vii. If all the features are the same i.e minutiae, incipient and crease then
grant access otherwise deny

viii. Compare the effectiveness in a tabular form.

Algorithm for later phases:

1. Input X and Y as two co-ordinates.
2. Input a feature point (I th), where 1<=I<=total feature points.
3. Now, input another feature point J th, Where 1<=J<=total feature points and I!=J.
4. if Y_I=Y_J then
DISTANCE: =X_J-X_I 32wqf
if DISTANCE <0 then
DISTANCE:=DISTANCE×(-1);
else if (Y_I>Y_J) then
if (Y_I-Y_J:=1) or (Y_I-Y_J:=-1) then

DISTANCE:=0

else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2) then

DISTANCE:=Y_I-Y_J

Else if DISTANCE:=(Y_I-Y_J)-2

DISTANCE:=(DISTANCE*WIDTH) +(WIDTH-X_J)+X_I

else if (Y_I-Y_J):=1 or(Y_I-Y_J):=-1

then DISTANCE:=0

else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2)

then DISTANCE:=Y_J-Y_I

else DISTANCE:=(Y_J-Y_I)-2

DISTANCE := (DISTANCE*WIDTH) +(WIDTH-X_I)+X_J

5. Repeat step 1,2 & 3 for the verified image also.

6. Find the equality of feature points

7. Calculate total number of correlated distances DISTANCE-of-all

8. End.

3.5

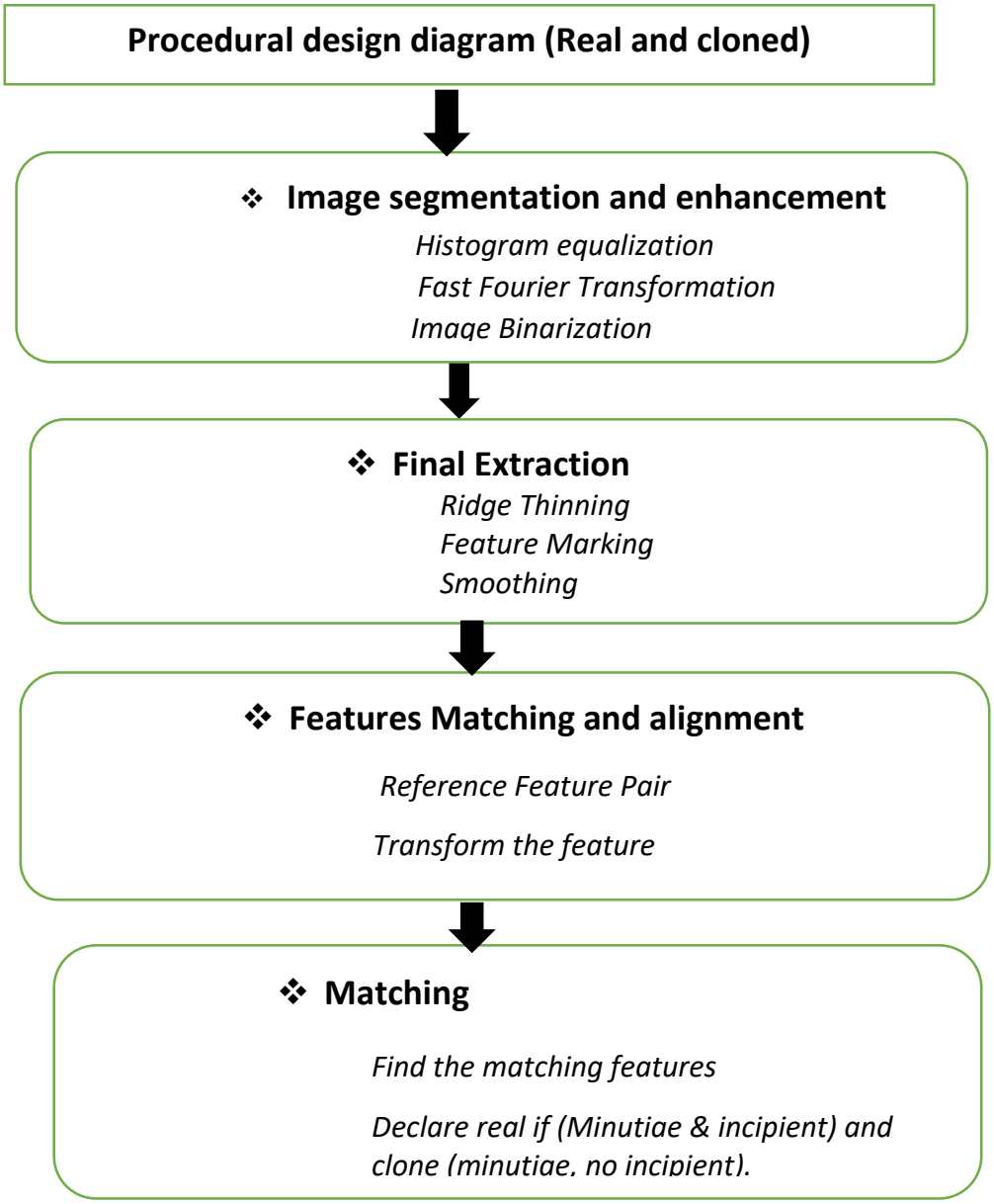


Figure 3. 6: Fingerprint image enhancement/processing

The first step from fig. 3.5 is the features extraction stage is Fingerprint Image enhancement. This is mainly done to improve the image quality and to make it clearer for further operations. Often fingerprint images from other sources lack sufficient contrast and clarity. Hence, image enhancement is necessary in all fingerprint techniques to improve the accuracy of matching, locating of distinctive features of the image. It increases the contrast between ridges and furrows and connects some of the broken points of ridges if there is crease on the fingerprint sample.

3.5.1 Histogram equalization

Histogram equalization was used to expand the pixel value distribution of an image so as to increase the perceptional information.

3.5.2 Fast fourier transform

The Fourier transform was obtained to find the frequency of the pixel, so that the output would be an image in the frequency domain. The image is divided into blocks in order to enhance a specific block *by its* dominant frequencies. So, the process is to multiply the FFT of the block by its magnitude a set of times. The enhanced image after

FFT has the improvements as some falsely broken points on ridges get connected and some spurious connections between ridges get removed.

3.5.3 Image binarization

This step was done to convert a 256-level image to a 2-level image. It is done to differentiate image pixels from background Because of variations in contrast, locally adaptive thresholding is used.

3.5.4 Image segmentation

Only a certain Region of Interest (ROI) is useful to be recognized for each fingerprint image to extract the ROI, a two-step method was used; block direction estimation and ROI extraction.

ROI extraction (Morphological Method)

• *Close* (shrink images and eliminate small cavities)

• *Open* (expands images and remove peaks introduced by background noise)

3.5.5 Final features extraction

The image has been enhanced, then image is segmented and the required area is obtained as template. The requirement of features extraction closes down to four

operations: Ridge thinning, feature marking, false features removal and features representation.

3.5.6 Image thinning

To eliminate the redundant pixels of ridges till the ridges are just one pixel wide. Morphological approaches, filter by other morphological operations to remove some breaks and isolated points. In this step, any single point (single-point ridges or single point breaks) in a ridge are eliminated and considered as processing noise, it is done using imerode and imfill.

3.5.7 Proposed work

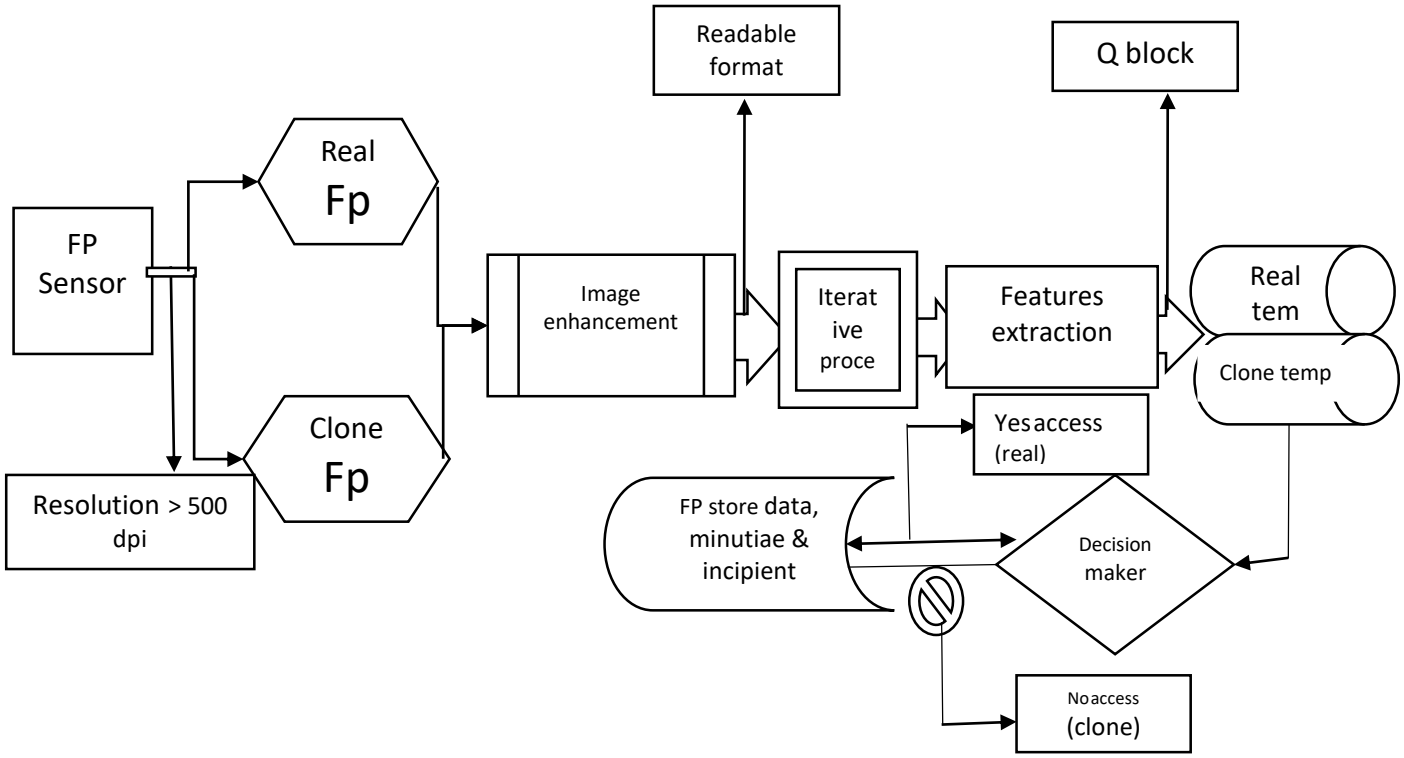


Figure 3. 7: The proposed work (image enhancement, iterative process, feature extraction, trained system and template creation)

CHAPTER FOUR

PERFORMANCE EVALUATION AND RESULTS

4.1 Previous Performance Evaluation Index

The previous chapter enumerated the methodology and the procedures involved in prevention of clone access prevention in biometric system. Here, contain the performance evaluation and results both from the previous and proposed works. There are tables and graphs which show the differences and achievement in the proposed work. Two indexes are well accepted for determining the performance of a fingerprint recognition system:

a. False Rejection Rate (FRR):- For an image database, each minutia sample is matched against the remaining samples of a particular finger to compute the FRR. A system's FRR is basically calculated by the following formula.

$$\%\text{FRR} = \frac{FR}{N} \times 100 \qquad (4.1)$$

FR = number of false rejections.

N = number of samples.

*b. False Acceptance Rate (FAR):-*Also in a database the first sample of each finger is matched with the first sample of the remaining fingers in order to compute the FAR. A system FAR is calculated by the formula.

$$\%\text{FAR} = \frac{FA}{N} \times 100 \qquad (4.2)$$

FA=number of cases of false acceptances

N=number of samples.

4.2 Experiments and Discussions

The extracted features are tested over a dataset collected from the Biometrics Engineering Research Center BERC, 2019 Gnanasivam, P. & Muttan (2010), Mojtaba (2010), Ain et al., (2018). The data repository is not accessible online because of hackers, this makes it reliable. By considering the fingerprint features, the datasets are collected at different levels and three sensors with ≥ 500 DPI resolution and above were adopted in this dataset collection. For the purpose of real simulation, instead of a ten-fold cross verification method, one third random samples of both the real and the cloned were selected in a training procedure, and the rest of the datasets are used to perform a test. This random process is made 10 times and the error rate and standard deviation are recorded.

4.3 Results

Figure 4. 1: Samples of Real Fingerprints

From figure 4.1 Samples were gotten with the help of different sensors. The fingerprint samples of real fingers are saved as soon the images were captured and converted to readable format.

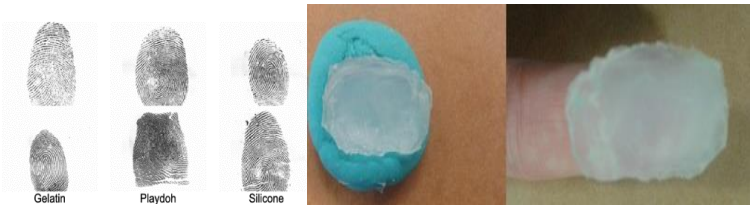


Figure 4. 2: Samples of fake Fingerprints

Different ways were devised in order to have exact copy the real images in fig. 4.2 that are already saved in Fig. 4.1. Components used in generating clone samples of fingerprints are; gelatin, silicon, candle wax, seal tape, high resolution pictures, printed circuit printed board. However in this work gelatin and candle wax were used. An attempt was made on seal tape but because of time, it was dropped while attention was given to gelatin and candle wax in order to generate the cloned samples of the real fingerprints. After careful iterative analysis Fig. 4.3 reveal some of the features that cannot be gotten during cloning, some of the features can only be gotten through careful subjection of fingerprint image to iterative operations.

4.4 Histogram equalization results

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information as it shows in figure 4.3.3 below.

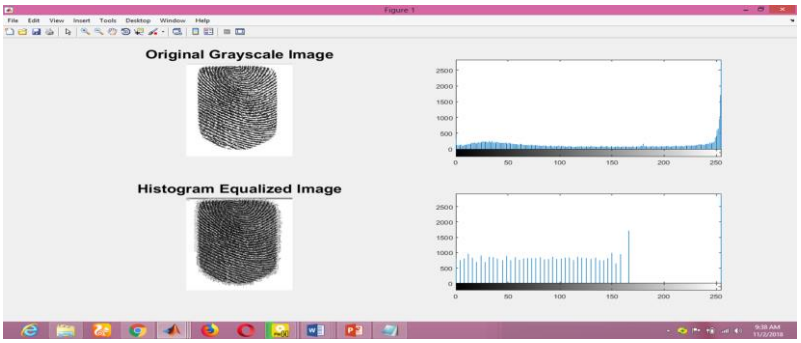


Figure 4. 3: **Histogram equalization of the scanned fingerprint**

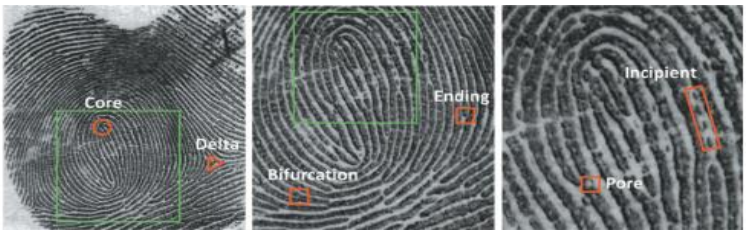


Figure 4. 4: **Analyzed fingerprint sample iteratively**

The features are better revealed in Fig. 4.4, in actual sense the work went beyond minutiae because the aim of the work is to prevent cloned fingerprints

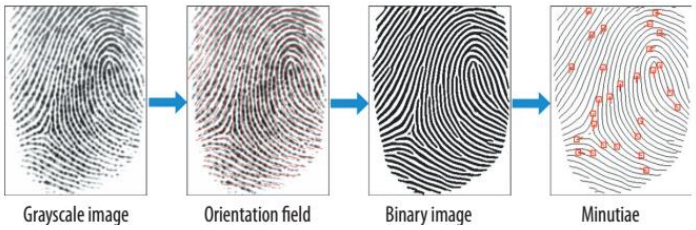


Figure 4. 5: **Feature extraction**

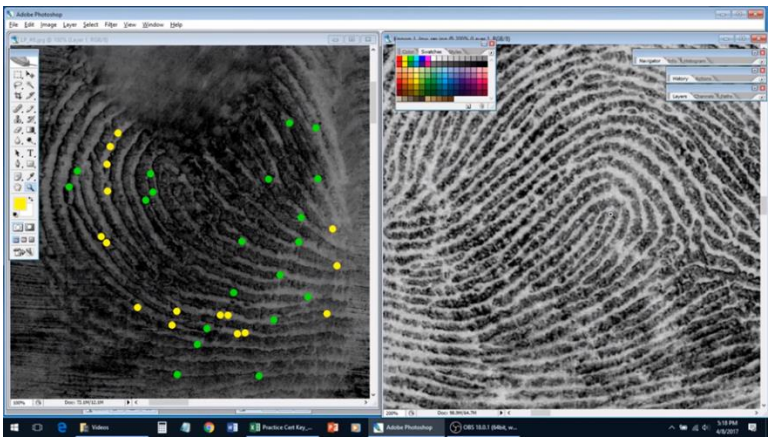


Figure 4. 6: **Nistlab Analysis used for the template**

In fig. 4.6 was used as the template that the system considers before granting access. However, access is granted to an individual whose minutiae, incipient or crease matches.

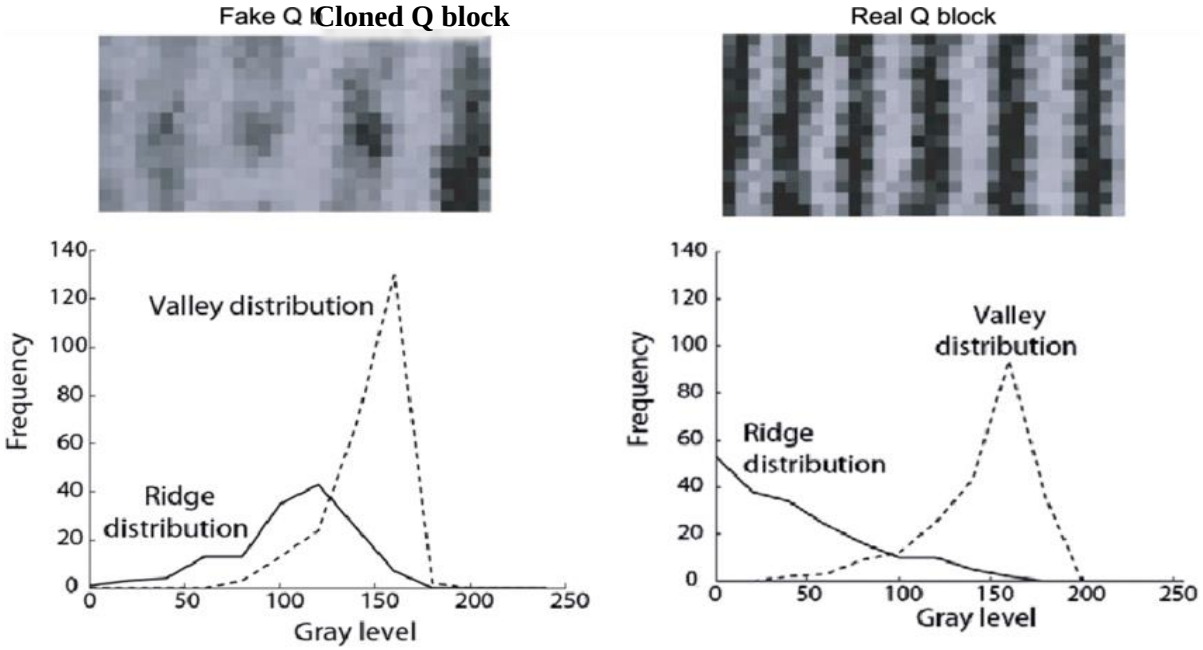


Figure 4. 7*:* **Sample test with Q- block**

Q block clearly differentiate between the ridges and valleys of real fingerprint and clone fingerprint. Another noteworthy in figure 4.7 is the way the images of clone and real fingerprint is represented, the image of the clone is not as clear as the real fingerprint.

4.5 The tables below showing the results of the tests for real and cloned fingerprints on different scanners

Table 4. 1 scfp1*:* results for the real fingerprints on scanner without the template.

SUBJECTS	SUCCESSFUL LOGINS	FALSE REJECTIONS	FALSE ACCEPTANCE
R1	50	0	0
R2	50	0	0
R3	50	0	0
SUMMATION =	150	0	0
PERCENTAGE (%)	100.00%	0%	0%

The table 4.1 above shows the result of the real fingerprint when tested with the scanner without the template created through the proposed work having put into consideration the issue of resolution that plagued the previous works. There was no issue of false rejection or false acceptance.

Table 4. 2 Scfp2: results for the cloned fingerprint on scanner test 1. Without the template

SUBJECTS	FALSE ACCEPTANCE	REJECTED LOGINS	FALSE ACCEPTANCE (OTHERS)
C1	50	0	0
C2	33	17	0
C3	39	11	0
SUMMATION =	145	28	0
PERCENTAGE(%)	96.7	18.70%	0%

Table 4.2 above shows the result of the cloned fingerprint for the first time it was tested with the previous work and it revealed the results for each condition column by column.

Table 4. 3: Scfp3: results for the cloned fingerprint on scanner test 2 without the template

SUBJECTS	FALSE ACCEPTANCE	REJECTED LOGINS	FALSE ACCEPTANCE (OTHERS)
C1	49	1	0
C2	46	4	0
C3	50	0	0
SUMMATION =	145	5	0
PERCENTAGE (%)	96.70%	3.30%	0%

Table 4.3 above showing the result of the cloned fingerprint for the second time it was tested with the previous work and it revealed the results for each condition column by column.

Table 4. 4: Scfp4: results for the real fingerprints on scanner without the template.

SUBJECTS	SUCCESSFUL LOGINS	FALSE REJECTIONS	FALSE ACCEPTANCE
R1	50	0	0
R2	50	0	0
R3	50	0	0
SUMMATION =	150	0	0
PERCENTAGE (%)	100.00%	0%	0%

Table 4.4 above showing the results of the real fingerprint of the proposed work having given attention to the issue of resolution which had negative effect on the previous works.

Table 4. 5: Scfp11: The successful rate of false rejection and false acceptance

SUBJECTS	SUCCESSFUL RATE	FALSE RR	FALSE ACCEPTANCE
R1	98.7%	1.30%	0%
R2	78%	22%	0%
R3	94%	6%	0%
Mean value =	90.2%	9.8%	0%

The table 4.5 revealed success rate of false rejection and false acceptance rate per subject for all Fingerprints scanners tested for real fingerprints. The mean value for all subjects are also shown

Table 4. 6: Scfp12*:* The results for the cloned fingerprint on scanner test 2 without the template

SUBJECTS	FALSE ACCEPTANCE	REJECTED LOGINS	FALSE ACCEPTANCE (OTHERS)
C1	46	4	0
C2	6	44	0
C3	41	9	0
SUMMATION =	93	57	0

Table 4.6 is the results for the cloned fingerprint on scanner test 2 without the template.

Table 4. 7: **The mean values for all the subjects for all test 1 cases.**

SUBJECTS	FAR	REJECTION RATE	FALSE ACCEPT (OTHERS)
C1	99.30%	0.70%	0%
C2	45.30%	54.70%	0%
C3	56.70%	42.70%	0%
MEAN VALUE =	67.10%	32.70%	0%

The table 4.7 shows the mean values for all the subjects for all test 1 cases.

Table 4. 8*:* The mean values for all the subjects for all test 2 cases

SUBJECTS	FAR	REJECTION RATE	FALSE ACCEPT (OTHERS)
C1	96%	4%	0%
C2	68%	32%	0%
C3	93%	7.3%	0%
MEAN VALUE =	85.6%	14.4%	0%

The table 4.8 above is the mean values for all the subjects for all test 2 cases:

Table 4. 9: Scfp15*:* Successful rate of false rejection rate and false acceptance rate per subject

SUBJECTS	SUCCESSFUL RATE	FALSE RR	FALSE ACCEPTANCE
R1	99.1%	0%	0%

R2	98.7%	0%	0%
R3	99.6%	0%	0%
Mean value =	99.1%	0%	0%

The successful rate of false rejection rate and false acceptance rate per subject for all Fingerprints scanners tested for real fingerprints. The mean value for all subjects are also shown

Table 4. 10: scfp16 results for the cloned fingerprint on scanner test 2 with the template.

SUBJECTS	FALSE ACCEPTANCE	REJECTED LOGINS	FALSE ACCEPTANCE (OTHERS)
C1	0	50	0
C2	0	50	0
C3	0	50	0
SUMMATION =	0	150	0

Table 4.10 is the results for the cloned fingerprint on scanner test 2 with the template.

Table 4. 11: Mean values for all the subjects for all test 1 cases

SUBJECTS	FAR	REJECTION RATE	FALSE ACCEPT (OTHERS)
C1	0%	99.2%	0%
C2	0%	99%	0%
C3	0%	99.7%	0%
MEAN VALUE =	0%	99.3%	0%

The mean values for all the subjects for all test 1 cases

Table 4. 12 The mean values for all the subjects

SUBJECTS	FAR	REJECTION RATE	FALSE ACCEPT (OTHERS)
C1	0%	99.4%	0%
C2	0%	99.1%	0%
C3	0%	99.51%	0%
MEAN VALUE =	0%	99.34%	0%

Table 4.12 is the mean values for all the subjects for all test 2 cases.

The overall results from the tables, shows that the proposed system is better than earlier works because, the earlier method was tested and compared with the proposed work and we can see that this system is efficient and effective compared to previous works.

Table 4. 13: Final Decision

Correct decision (proposed)	Incorrect decision (previous)
Genuine individual accepted	Genuine individual is rejected (FRR)
Cloned fingerprint denied	Cloned accepted (FAR)

The way the system was trained is simplified in the table. 4.13 below, which helps greatly in preventing cloned fingerprints from accessing the system when they do not have the privilege of doing so.

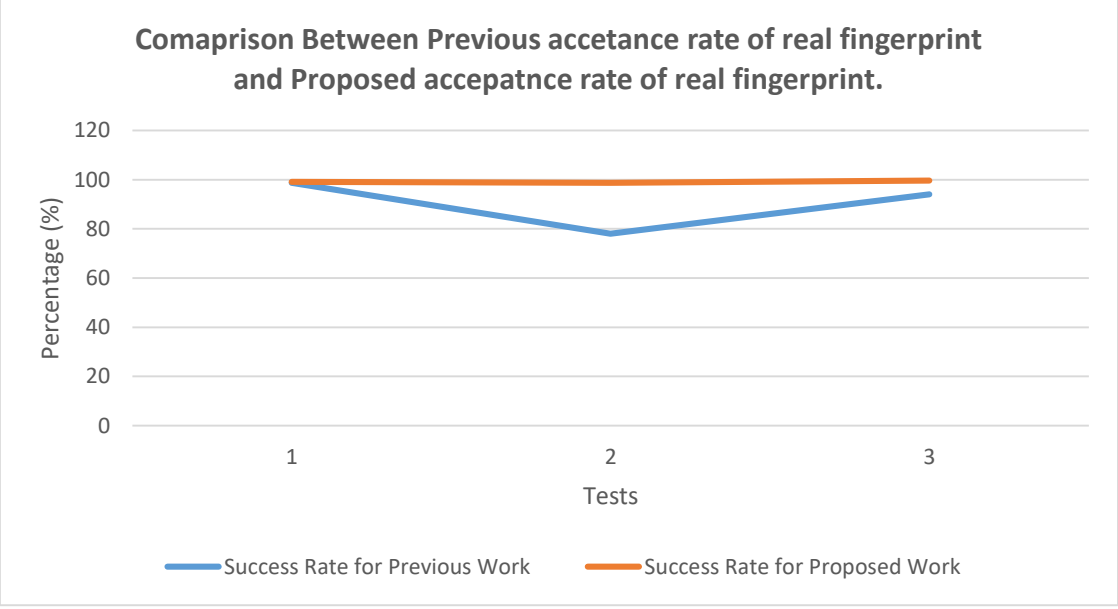
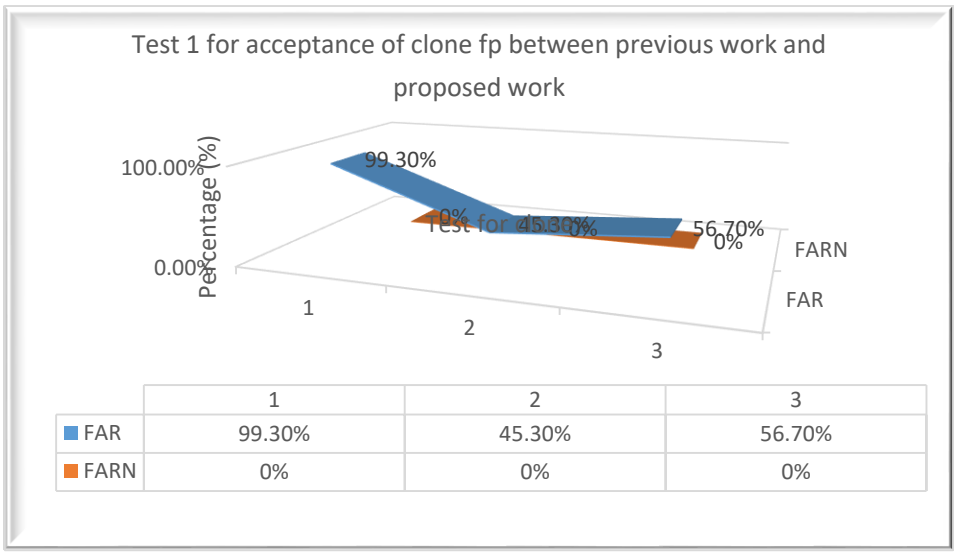


Figure 4. 8: Comparison between previous work and proposed work for Real Fingerprint..

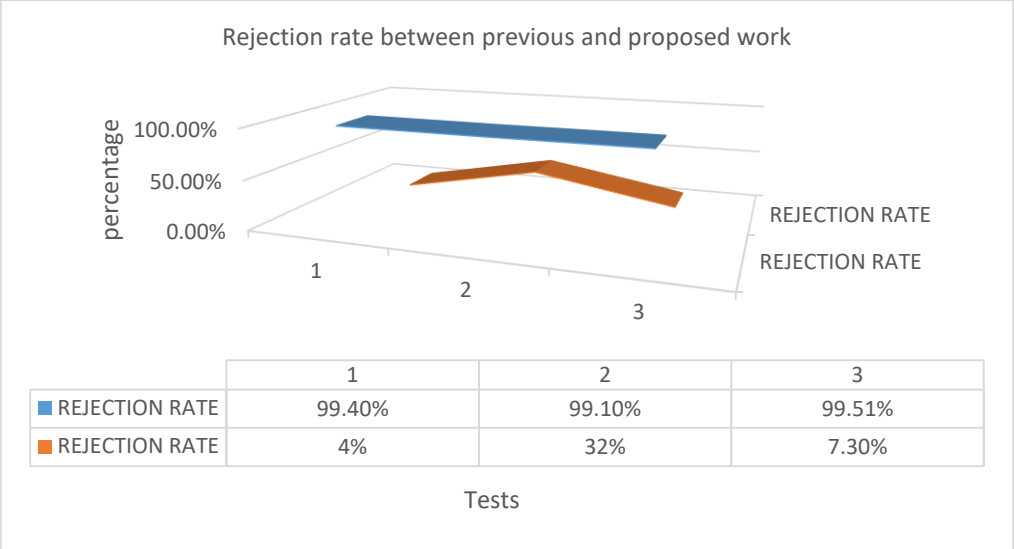
The figure 4.8, the horital line (straight) represent acceptance of rate of real fingerprints of the proposed work compared to the previous work (curve).



	1	2	3
FAR	99.30%	45.30%	56.70%
FARN	0%	0%	0%

Figure 4. 9: Test 1 for clone fp between previous and proposed work

The figure 4.9 above represents the rate of false rejection of clone fingerprint of the Proposed (straight) work compared to the previous work (curve).



	1	2	3
REJECTION RATE	99.40%	99.10%	99.51%
REJECTION RATE	4%	32%	7.30%

Figure 4. 10: Test 2 for clone fingerprint between previous and proposed work

The figure 4.10 above represents the proposed work rejection rate of clone fingerprint (straight) compared to the previous work (curve). The rejection rate of the proposed work is very high and stable as it is indicated in the graph.

CHAPTER FIVE

SUMMARY, CONCLUSION AND FUTURE WORKS

The previous chapter discussed the performance evaluation and results of the study. This chapter consist of the summary, conclusion and recommendation of the research work, publication, conference and award:

5.1 Summary

The images of both real and fake were captured and thorough algorithm designed and implemented in Matlab with the use of toolbox called morphology. The images were subjected to an iterative process to really know the real and cloned fingerprint. At initial presentation of a cloned sample, it might look real but multi-level process or analysis revealed the general properties of the image once the features are not as detailed as the real fingerprint samples it is said to be cloned and access will be denied.

5.2 Conclusion

The research work considered other features of fingerprint extracted in other to achieve cloned access prevention. The research started from the use of a biometric device to turn it into an efficient biometric fingerprint recognition to detect cloned fingerprints. The algorithm and basic concept of acquiring quality image, behind each step are given priority. And the entire algorithm was implemented in MATLAB, which finally gives a graphical user interface where we can watch the processes evolving. The reliability of any automatic fingerprint system strongly relies on the precision obtained in the fingerprint feature enhancement and extraction process. A number of factors can damage the correct location of these features. Among them, poor image quality, this is the one with most negative influence and must be avoided as much as

possible. The preprocessing stage does not usually fix the fingerprint image in total. The unwanted features will significantly affect the accuracy of matching if they are simply regarded as genuine feature. Mechanisms of removing false features are essential to keep the fingerprint verification. This was achieved with the help of NISTLAB application which was used before creation of the standard template.

5.3 Recommendation

Artificially created fingerprint or cloning had been taken care of in this work but there are still other challenges for example attacking biometric system via the input port and attacking the biometric data warehouse are good areas of research, these has to do with hardware devices used in biometric systems**.**

Publication: Science Association of Nigeria (SAN).

Conference: 53nd Annual Conference of Science Association of Nigeria, held in Sokoto, 2019.

Award: One of the best presenters during the Conference.

REFERENCE

Ain N., Shaukat N., Nagra A. & Raja G. (2018). An Efficient Algorithm for Fingerprint Recognition Using Minutiae Extraction**.** *Pakistan Journal of Science*: Vol. 22, pp 71-80.

Afsar F., Arif M. & Hussain M., (2004). Fingerprint identification and verification system using minutiae matching. Department of Computer & Information Sciences, Pakistan Institute of Engineering & Applied Sciences Islamabad, Pakistan. *National Conference on Emergence Technology NCET*: pp 141–146.

Algarra M., Radotić K., Kalauzi A., Mutavdžić D., Savić A., Jiménez-Jiménez, J., Rodríguez-Castellón, E., da Silva, J.C.E. & Guerrero-González, J.J., (2014). Fingerprint detection and using intercalated CdSe nanoparticles on non-porous surfaces. *Analitica Chimica Acta*, Vol. 812, pp 228-235.

Bana S., & Kaur D., (2011). Fingerprint Recognition using image segmentation. (IJAEST) *International Journal of Advanced Engineering Sciences and Technologies*. Vol. 5, pp 012 – 023

Bansal R., Sehgal P., & Bedi P., (2011). Minutiae extraction from fingerprint images. *(IJCSI) International Journal of Computer Science Issues,* Vol. 8, pp 258-267.

Cao K. & Jain A., (2015). Learning fingerprint reconstruction from minutiae to image. *IEEE: Transformation on information forensic and security: Vol.* 10, pp 104 - 117.

Cao K. & Jain A., (2018). Automated latent fingerprint recognition. IEEE *International Journals of Biometrics: Transformation on Pattern analysis machine Intelligent:* vol. 33, no. 1, pp. 88-100.

Conti V., (2010). Introducing Pseudo-Singularity points for efficient fingerprints classification and recognition. *In CISIS - The 4th International Conference of Computer Software Intensive System*: pp 368–375.

Chaudhari A., Patnaik G., & Patil S., (2014). Implementation of minutiae based fingerprint identification system using crossing number concept. *Journal of Informatica Economica*: Vol. 18, pp 17-25.

Choi H., Kang R., Choi K., Jin A., & Kim, J. (2009). Fake-fingerprint detection using multiple static features. *IEEE Transactions on Information Forensics* and Security *covers the sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features.* Vol. 48, pp 1-1-14.

Feng, J. (2008). Combining minutiae descriptors for fingerprint matching. *Science Direct*: Volume 41, Issue 1, pp 342-352.

Gayathri S. & Sridhar V., (2014). Implementation of image enhancement technique for Fingerprint Recognition process. *(IJEAT) International Journal of Engineering and Advanced Technology*. Vol.8, pp 868–873.

Gnanasivam, P. & Muttan (2010). An efficient algorithm for fingerprint preprocessing and feature extraction. *Science Direct: In proceeding of Computer Science*. Vol. 2, pp 133-142

Gonzalez R., (2009). Digita Image *Processing. Digital Image Processing, third edition of International Conference on Image processing Education:* Vol. 14, pp 8-20.

Hou Z., (2012). A variation formulation for fingerprint orientation modeling. *International Journal of Pattern Recognition*: Vol. 45, pp 1915–1926.

Ishpreet, S.V. and M. Raman (2012). Fingerprint image enhancement and minutiae matching in fingerprint verification. *Journal of Computer Technology first International Conference*: Vol. 17, pp 71-98.

Jain A., Feng J. & Nandakumar K. (2010). Fingerprint Matching. *Proceeding of International Computer Vision and Pattern Recognition Workshop Biometrics: Vol. 45,* pp. 1-8.

Jie, Y., (2006). Fingerprint minutiae matching algorithm for real time system. International Journal on Pattern Recognition: Vol. 39(1) pp 143–146.

Kaseva A., & Antti St´en., 2003. Fooling fingerprint scanners. *Biometric vulnerabilities of the Precise Biometrics 100 SC scanner*. http://citeseer.ist.psu.edu/695069.html.

Khan M., Khan T., Bailey D., & Kong Y., (2016). A spatial domain scar removal strategy for fingerprint image enhancement. Journal of Pattern Recognition: Vol. 60, pp 258–74.

Kudu N., (2016). Biometric Identification System using Fingerprint and Knuckle as Multimodality Features *International Conference on Electronics Electrical and Optimization Technology*: pp 3279–3284.

Kumar K., Kumar & Kumar D., (2011). Fingerprint recognition using minutiae extraction. International Conference on ICT-Initiatives: Vol. 43, pp 511-603.

Lim J. & Chin Y., (2014). Enhancing fingerprint recognition using minutiae-based and image-based matching techniques. *Proceedings - 1st International Conference of Artificial Intelligence Modelling Simulations AIMS*: pp 261–266.

Liu M., Liu S, and Zhao Q., (2014). Fingerprint orientation field reconstruction by weighted discrete cosine transform. *Information Science Journal*: Vol. 268, pp 65–77.

Maio D., (2004). Fvc2004. Third fingerprint verification competition. *International Journal of Biometric authentication:* Vol. 24, pp 1–7.

Matsumoto H., Matsumoto K., Yamada, & Hoshino H., (2002) Impact of artificial "gummy" fingers on fingerprint systems. *In Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV:* Vol. 4677, pp 275–289.

Mohsen S., Farhan S., & Hashem M., (2004). Automated fingerprint recognition using minutiae matching technique for the large fingerprint database. *3rd International Conference Electronics Computer Engineering ICECE: pp* 28–30.

Mojtaba S., Cristinel M., & Wamadeva B., (2010). Vitality - Detection in Fingerprint Identification. *School of Engineering & Design Brunel University Uxbridge, Moddlesex, UB8 3 PH UK:* Vol. 7, pp 211-233.

National Science and Technology Council (NSTC), 2006. Biometric History. *Committee on Homeland national Security, subcommittee on Biometrics.*

Peralta D., (2014). Fast fingerprint identification for large databases. *International Institute of Pattern Recognition:* Vol. 47, pp 588–602.

Peralta D., Galar I., Triguero D., Paternain S. Garcia E., Barrenechea J., Benítez, H., Bustince, & Herrera F., (2015*).* A survey on fingerprint minutiae-based local matching for verification and identification. *Taxonomy and experimental evaluation Information Science:* Vol. 315, pp 67–87.

Putte T. & Keuning J., 2000 "Biometrical fingerprint recognition: don't get your fingers burned", *In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications: Vol. 20, pp 5-8.*

Sahu D., & Shrivas R., (2016). Fingerprint reorganization using minutiae based matching for identification and verification. *International journal of science and research: Vol.* 5, pp 1710–1715.

Sandstr¨om M., 2004. Liveness detection in fingerprint recognition systems. Master's thesis, *Linkoping Tekniska Hogskola: http://www.ep.liu. se/exjobb/isy/2004/3557/exjobb.pdf.*

Serratosa F., & Cortes X., (2015). Interactive graph-matching using active query strategies. International *Journal* of *Pattern Recognition Systems:* Vol. 48 (4), pp 1364–73.

Silva A., Barbosa M., Parente R., Batista L., Primo J., Marinho A., & Alves P., (2015). Analysis of a genetic algorithm-based approach in the optimization. *International Conference on Computer* Science *Automatic Fingerprint Identification Systems matching algorithm*. pp 23–28.

Shinde, A. & Bendre V., (2015). An embedded fingerprint authentication system. *In Proceedings - 1st International Conference of Computer Communications Automation ICCUBEA:* pp 205–208.

Sivaranjani, S., (2015). *Footprint feature extraction on raspberry Pi*. *ICIIECS*: pp.1–6.

Sudiro, S. & R. Yuwono (2012). Adaptable fingerprint minutiae extraction algorithm based-on crossing number method for hardware implementation using FPGA device. *International Journal of Computer Science and Engineering, Information Technology (IJCSEIT)*. Vol. 2, pp 66

Thalheim L., Krissler J., & Peter-Michael Ziegler 2002. Biometric access protection devices and their programs put to the test. Committee on Biometrics http://www.heise.de/ct/enOglish/02/11/114/.

Tiwari S., & Sharma N., (2012). Q-Learning approach for minutiae extraction from fingerprint image. Procedia Technology, Vol. 6, pp 82–89.

Van der T., Putte & J. Keuning., (2000). Biometrical fingerprint recognition: don't get your fingers burned. In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications Kluwer Academic Publishers. pp 289-303.

Wahby, S., & Ahmad M., (2013). A multilevel structural technique for fingerprint representation and matching. Signal Processing: Vol. 93, pp 56–69.

Wang, J., Le, N.T., Wang N., & Lee, J., (2015). Enhanced ridge structure for improving fingerprint image quality based on a wavelet domain. International Conference on Signal Processing: Vol. 22, 390-394.

Win, Z.M. & M.M. Sein (2011). Fingerprint recognition system for low quality images. *SICE Annual Conference:* pp.1133–1137.

Xu, M., Feng, J., Lu, J. & Zhou (2017). Latent fingerprint enhancement using Gabor & minutia dictionaries. *Proceedings of International Conference of Computer Vision and Pattern Recognition (CVPR)*: pp. 2305-2312

Zhang, K., (2010). Study on the embedded fingerprint image recognition system. *International Conference on Proceedings of Information Science Engineering*: pp 169–172.