Fortifying Pattern Recognition for Substantiating Augmented Performance with an Ideal Authentication Scheme

A

Thesis

Submitted to

Lovely Professional University

For the Award of degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER APPLICATIONS AND INFORMATION TECHNOLOGY

By

Kuljeet Kaur

Guide

Dr. G.Geetha

Faculty of Technology And Sciences

Lovely Professional University,

Phagwara

May, 2015

DECLARATION

I declare that the thesis entitled Fortifying Pattern Recognition for Substantiating Augmented Performance with an Ideal Authentication Scheme has been prepared by me under the guidance of Dr.G.Geetha, Professor and Associate Dean of Division of Research and Development, Lovely Professional University, India**.** No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Kuljeet Kaur

School of Computer Applications
Lovely Professional University
Jalandhar – Delhi G.T.Road (NH-1)
Phagwara, Punjab – 144411
India

DATE: May 14, 2015

CERTIFICATE

I certify that Kuljeet Kaur has prepared her thesis entitled Fortifying Pattern Recognition for Substantiating Augmented Performance with an Ideal Authentication Scheme, for the award of PhD degree of the Lovely Professional University, India**,** under my guidance. She has carried out the work at the Department of School of Computer Applications, Lovely Professional University, India.

Dr.G.Geetha

Division of Research and Development
Lovely Professional University
Jalandhar – Delhi G.T.Road (NH-1)
Phagwara, Punjab – 144411,
India

DATE: May 14, 2015

ABSTRACT

This research adds to an understanding and fortification of pattern recognition by using an ideal authentication scheme to illuminate various dynamics of image processing that constitutes identity authentication. The major contribution of the research work is to advance science with respect to pattern recognition and contribute towards security and privacy through authentication and computing methodologies with tasks through biometrics. This study uses hash based scheme to depict authentication occurring within specific public networks and derives a new fingerprint hash algorithm RNA-FINNT[1] which refers to Reduced Number of Angles Fingerprint Hash Algorithm for substantiating its performance. Specifically this study advances in identity authentication literature[1,2,3] that portray fingerprint as relatively burly parameter that constituted and enacted around image processing ideals or resources. This study reveals the reduction in error percentage[4] through RNA-FINNT while at the same time suggesting the diminution of error approximation[5] and computing the overall recognition accuracy. The contributions of the study revolve around conceptualizing the identity authentication with RNA-FINNT as a practice that stabilize the fingerprint parameter as most acceptable and confer the security and privacy of the legitimate user.

By considering fingerprint as most acceptable identity authentication parameter through a survey[6] this study addresses fortification of pattern recognition. Such acceptability

[1] Kuljeet Kaur and Dr.G.Geetha, 'Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter', International Journal of Computer Science and Issues, ISSN: 1694-0814, Vol. 9, Issue 2, No 2: 188-193, March 2012

[2] Kuljeet Kaur and Dr.G.Geetha, 'Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters', International Journal of Computer Applications, ISSN 0975-8887, Vol. 42 No.6: 36-42, March 2012, doi: 10.5120/5700-7751

[3] Kuljeet Kaur and Dr.G.Geetha, 'Virtualization of Multi Server Environment results in Enhanced Communication and Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.3: 4101-4108, May-June 2012

[4] Kuljeet Kaur and Dr.G.Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," Proc. of the International Conference on Advances in Computer Science and Electronics Engineering — CSEE 2013 at New Delhi, India, ISBN: 978-981-07-5461-7 doi: 10.3850/ 978-981-07-5461-7_12, (p.55-59), 24th Feb, 2013. New Delhi, India

[5] Kuljeet Kaur and Dr.G.Geetha, 'Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to enhance Network Security', Journal of Information Security - JIS, ISSN 2153-1242 Volume 4, Number 4: 197-202, October 2013, http://dx.doi.org/10.4236/jis.2013.44022

[6] Kuljeet Kaur and Dr.G.Geetha, 'Survey for Generating an Ideal Password Authentication Scheme which results in Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.2: 3608-3614, March-April 2012

emerges from the views of users that constantly use identity authentication parameters for security. In this study the structured nature of fingerprint is adopted for reckoning[7] the minutiae points of the fingerprint image and is similarly acknowledged and will subsequently be discussed for improved pattern recognition. However by adopting fingerprint idea of practices as parameter in multi server environment it is also noted that certain identity authentication parameters do not stabilize and become recognizable as specific parameter for enhanced security[3]. Enhanced security is achieved when fingerprint constantly perform within RNA-FINNT with specific conventions upon error percentage and approximation. However even while the other identity authentication parameters might be stable, practices are transformed by the same structures for enhanced security that they could not achieve properly which means that only fingerprint could have stabilized results. RNA-FINNT revealed that its implementation in an ideal authentication scheme would result in advancing science with respect to pattern recognition and enhances security and privacy through authentication and computing methodologies with tasks through biometrics and fortifies transport layer security protocol[8] and it needs multi server environment for substantiating the security and privacy[9] of the legitimate user. Extraction of minutiae points using MATLAB reveals that fingerprint exhibit varied characteristics and takes on different security measures as participants or users draw with other identity authentication parameters to constitute the fingerprint as authentic medium for fortified pattern recognition.

Fingerprint with RNA-FINNT may therefore be enacted as application for Online Banking, Student Attendance System, Library Management System, Fortification of

---

[7] Kuljeet Kaur and Dr.G.Geetha, "Reckoning Minutiae Points with RNA-FINNT Augments Trust and Privacy of Legitimate User and Ensures Network Security in the Public Network," Fifth International Conference on Networks and Communications (NETCOM - 2013), Chennai (Tamil Nadu, India) dated 27th – 29th Dec, 2013, doi: 10.1007/978-3-319-03692-2_17

[3] Kuljeet Kaur and Dr.G.Geetha, 'Virtualization of Multi Server Environment results in Enhanced Communication and Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.3: 4101-4108, May-June 2012

[8] Kuljeet Kaur and Dr.G.Geetha, "Implementing RNA-FINNT in Ideal Password Authentication Scheme results in Fortification of Transport Layer Security Protocol," International Conference on Advances in Information Technology at Bangkok, Thailand, ISBN: 978-981-07-2683-6 doi:10.3850/978-981-07-2683-6 AIT-104 (p.14-18),23rd June,2012.Bangkok, Thailand

[9] Kuljeet Kaur and Dr.G.Geetha, "Generating Multi Server Environment for implementation of Ideal Password Authentication Scheme," International Conference on Advances in Electronics, Electrical and Computer Science Engineering - EEC 2012 at Dehradun, India, ISBN: 978-981-07-2950-9 doi:10.3850/ 978-981-07-2950-9 EEC-376, (p.55-59),7th - 9th July, 2012.Dehradun (Himachal Pradesh, India)

Transport Layer Security Protocol, Login into Customer Management System, Door Locking System, Auto Ignition in the Vehicles and ID card Enrollment Software etc and could use Graphical User Interface[7] of the MATLAB for its implementation. To evaluate the performance clear identification of research gaps in the study is done. The detailed literature review resulted in specifying the research gaps like mutual authentication required when fingerprint is used as identity authentication parameter with new algorithm using hash based scheme with reduction in error percentage and diminution in error approximation, new fingerprint hash algorithm should have error percentage less than 10, average processing time less than 10 seconds and average matching time as less than 0.1 seconds. Even the algorithm should have acceptable distortion tolerance to substantiate its performance. The performance evaluation of enactment as application of RNA-FINNT is done through defined performance indicators like False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage and few results are derived with reduction in error percentage[4] and diminution in error approximation[5]. Study advances science with respect to pattern recognition which further augments security in biometric[10] machines through embedded RNA-FINNT.

The experiment for the computation of performance indicators for RNA-FINNT is done on three different databases which are real time fingerprint database, existing fingerprint database (FVC2000, FVC2002 and FVC2004) and noisy fingerprint database (FVC2000 and FVC2002 for noisy images). Real time fingerprint database has total 50 subjects and 2 impressions of each subject (index finger) are taken for evaluation. Existing fingerprint

---

[7] Kuljeet Kaur and Dr.G.Geetha, "Reckoning Minutiae Points with RNA-FINNT Augments Trust and Privacy of Legitimate User and Ensures Network Security in the Public Network," Fifth International Conference on Networks and Communications (NETCOM - 2013), Chennai (Tamil Nadu, India) dated 27th – 29th Dec, 2013, doi: 10.1007/978-3-319-03692-2_17

[4] Kuljeet Kaur and Dr.G.Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," Proc. of the International Conference on Advances in Computer Science and Electronics Engineering — CSEE 2013 at New Delhi, India, ISBN: 978-981-07-5461-7 doi: 10.3850/ 978-981-07-5461-7_12, (p.55-59), 24th Feb, 2013. New Delhi, India

[5] Kuljeet Kaur and Dr.G.Geetha, 'Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to enhance Network Security', Journal of Information Security - JIS, ISSN 2153-1242 Volume 4, Number 4: 197-202, October 2013, http://dx.doi.org/10.4236/jis.2013.44022

[10] Kuljeet Kaur and Dr.G.Geetha, 'Pattern Recognition by Embedded Reduced Number of angles Fingerprint Algorithm in Biometric Machines augments Security', Inderscience International Journal of Computer Applications in Technology, Special Issue on Advances in Networking and Signal Processing for Social Security, ISSN 1741-5047 Volume 51, Number 2: 131-144, April 2015, doi: 10.1504/IJCAT.2015.068924

database has 40 subjects in each database and further in four sub databases each subject is contributing 8 images so in total 960 images are available in databases. While for testing purpose 10 subjects are taken 8 images per finger considered so in total 80 fingerprint images are taken for evaluation. Noisy fingerprint database has fake fingerprint images of 40 subjects 8 impressions of each fingerprint so in total 640 different fingerprint images for databases. While for testing 10 subjects are taken 8 impressions of each fingerprint are considered so in total 80 fingerprint images are taken for evaluation. Distortion tolerance of RNA-FINNT is also computed for all the three different databases real time fingerprint database, existing fingerprint database (FVC2000, FVC2002 and FVC2004) and noisy fingerprint database (FVC2000 and FVC2002 for noisy images).

Results of RNA-FINNT for performance indicators on the basis of one of the impression of the specific subject in real time fingerprint database are False Matching Rate = 0.020, Equal Error Rate =0.0534, Threshold Value = 30 and 5, False Acceptance Rate = 0.020, False Reject Rate = 0.198, False Non Match Rate = 0.198, Error Percentage = 0.632 and Difference of the Error = 2.0. Overall average for performance indicators in real time fingerprint database is False Matching Rate = 0.47, False Acceptance Rate = 0.47, False Reject Rate = 0.43 and False Non Match Rate = 0.43. Distortion tolerance is done with real time fingerprint database and it resulted in 70.83% as an average. To substantiate the performance of RNA-FINNT distortion tolerance is also checked by removing, replacing and disturbing few minutiae points from the fingerprint images and the output is 50%, 33.3% and 45.8% respectively which states that RNA-FINNT has acceptable distortion tolerance. Results of RNA-FINNT for performance indicators on the basis of one of the impression of the specific subject in existing fingerprint database are False Matching Rate = 0.110, Equal Error Rate =0.099, False Acceptance Rate = 0.110, False Reject Rate = 0.225, False Non Match Rate = 0.225, Error Percentage = 0.319. Overall average of performance indicators for existing fingerprint database is False Matching Rate = 1.22, False Acceptance Rate = 1.22, False Reject Rate = 0.68 and False Non Match Rate = 0.68. Results of RNA-FINNT for performance indicators on the basis of one of the impression of the specific subject in noisy fingerprint database are False Matching Rate = 11.70, Equal Error Rate =0.089, False Acceptance Rate = 11.70, False Reject Rate = 4.593, False Non Match Rate = 4.593, Error Percentage = 0.387 which states that RNA-

FINNT is unable to extract minutiae points of those fingerprints which have noise ratio more than 50%. Such computation of the performance indicators therefore challenge the overall recognition accuracy of RNA-FINNT since the participants or users depict fingerprint as burly parameter distinct from other identity authentication parameters.

Substantiation and validation of the overall recognition accuracy is validated through preset conditions like error percentage must be less than 10, average processing time should be less than 10 seconds and average matching time should be less than 0.1 seconds. Computation of the overall recognition accuracy of RNA-FINNT needs the combination of threshold values to be evaluated. The threshold value resulting in minimum difference between False Acceptance Rate and False Rejection Rate is considered for computation of the overall recognition accuracy. Overall Recognition Accuracy of RNA-FINNT for particular impression of the specific subject in real time fingerprint database is approximately 78%, in existing fingerprint database is approximately 83% (ranges between 77 to 89) and algorithm is unable to compute the value in noisy fingerprint database because the noise ratio in the fingerprints is more than 50%. The time and space complexity of RNA-FINNT is O(n).

RNA-FINNT performs better than other algorithms because during computation it does not consider the global feature[1] or core point for calculating number of angles which results in removal of dependency[1], the grid of squares in the algorithm executes in parallel[1] so the speed of computation is much faster[1] than the existing algorithms.

Reduction in error percentage[4] and error approximation[5] with RNA-FINNT is 4% and 33% respectively which in return increases the overall performance efficiency of the system. The error percentage, average processing time and average matching time of RNA-FINNT is 0.632 which is less than 10, 6.14 which is less than 10 seconds and

[1] Kuljeet Kaur and Dr.G.Geetha, 'Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter', International Journal of Computer Science and Issues, ISSN: 1694-0814, Vol. 9, Issue 2, No 2: 188-193, March 2012

[4] Kuljeet Kaur and Dr.G.Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," Proc. of the International Conference on Advances in Computer Science and Electronics Engineering — CSEE 2013 at New Delhi, India, ISBN: 978-981-07-5461-7 doi: 10.3850/ 978-981-07-5461-7_12, (p.55-59), 24th Feb, 2013. New Delhi, India

[5] Kuljeet Kaur and Dr.G.Geetha, 'Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to enhance Network Security', Journal of Information Security - JIS, ISSN 2153-1242 Volume 4, Number 4: 197-202, October 2013, http://dx.doi.org/10.4236/jis.2013.44022

0.00165 which is less than 1 second respectively. Distortion tolerance of RNA-FINNT for real time fingerprint database ranges from 33.3% to 50% when minutiae are removed, replaced and disturbed respectively. RNA-FINNT is able to validate the preset conditions for specifying the overall recognition accuracy. Implementation of RNA-FINNT into the biometric machines[10] will help in fortifying the security through biometrics.Overall it has resulted in accomplishing the research gaps of the study.

This study hence demonstrates that RNA-FINNT adopts fingerprint as the identity authentication parameter. This study also advances other image processing studies that have similarly challenged such security concerns. This research contributes in advancing science with respect to pattern recognition and for security and privacy through authentication and computing methodologies with tasks through biometrics. This research provides scope for future expansion in the behavioral, structural and physical domain of hardware implementation by suggesting scope as preparing the Boolean equation, transistor level circuit preparation, preparing mask of the circuit of RNA-FINNT for projection and fabrication of the silicon chip using different chip fabrication steps for making RNA-FINNT Chip. Such scope of the study makes it pertinent not only in advancing knowledge but also in terms of enlightening participants or users and security decisions targeting such fortification of pattern recognition in the ACM Computing Classification System 2012 of security and privacy through authentication and computing methodologies with tasks through biometrics.

[10] Kuljeet Kaur and Dr.G.Geetha, 'Pattern Recognition by Embedded Reduced Number of angles Fingerprint Algorithm in Biometric Machines augments Security', Inderscience International Journal of Computer Applications in Technology, Special Issue on Advances in Networking and Signal Processing for Social Security, ISSN 1741-5047 Volume 51, Number 2: 131-144, April 2015, doi: 10.1504/IJCAT.2015.068924

PREFACE

Thesis is based on the experimental evaluation of performance indicators and recognition accuracy of fingerprint algorithms. The thesis has proposed a new fingerprint hash algorithm RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm) which has removed dependency on global features, takes less time in calculation, rapid execution as all grid of squares are computed in parallel and reduces error approximation.

Chapter 1 gives brief introduction of the topic, hypothesis, objectives, scope of study and flow of methods and techniques. Chapter states as per ACM Computing Classification System 2012 the major contribution of the research is advancing science with respect to pattern recognition and contributing for security and privacy through authentication and computing methodologies with tasks through biometrics. The chapter focuses upon the main supposition or proposed explanation made in the study on the basis of limited evidence as a starting point for further investigation.

Chapter 2 is the review of literature which focuses upon the attacks and security requirements, existing password authentication schemes, most acceptable identity authentication parameter, types of fingerprints, technologies and techniques for fingerprint authentication, fingerprint algorithms, identifying need of new fingerprint hash algorithm (RNA-FINNT : Reduced Number of Angles Fingerprint Hash Algorithm), virtualization of multi server environment, substantiation of augmented trust and privacy, applications of ideal authentication scheme and MATLAB and its features. In this chapter few of the text is taken from previously published papers of ours. Portions of the introductory text in this chapter are also modified from previously written papers in year 2012 in International Journal of Computer Applications (doi: 10.5120/5700-7751, ISSN: 0975 – 8887, Volume 42– No.6, March 2012), International Journal of Computer Science and Information Technologies (ISSN 0975 – 9646, Volume 3, Issue No.2, March-April 2012) and International Journal of Computer Science and Issues (ISSN: 1694-0814, Volume 9, Issue 2, No 2, March 2012).

Chapter 3 focuses upon identification of research gaps based on the literature review, analysis of the survey, comparison of existing password authentication scheme,

comparison of technologies and techniques for fingerprint, comparison of fingerprint algorithms and methodology of deriving new ideal authentication scheme. In Chapter 3 Table 1 and 2 are taken from previously published papers of our in year 2012 and 2013 in International Journal of Computer Applications (doi: 10.5120/5700-7751, ISSN: 0975 – 8887, Volume 42– No.6, March 2012) and Journal of Information Security (http://dx.doi.org/10.4236/jis.2013.44022, ISSN 2153-1242 Volume 4, October 2013). Table 3 is created after comparing the advantages and problems of fingerprint algorithms or techniques. Table 4 and 5 are created on the basis of values of performance indicators derived in the specified references of the table. Complete chapter focused upon the research gaps.

Chapter 4 has details of new fingerprint hash algorithm RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm) published in the International Journal of Computer Science and Issues (ISSN: 1694-0814, Volume 9, Issue 2, No 2, March 2012). Chapter states the RNA-FINNT fingerprint match for identifying the malicious or legitimate user. This chapter also states the reduction in error percentage (doi: 10.3850/978-981-07-5461-7_12, ISBN: 978-981-07-5461-7, 2013) and diminution of error approximation in Journal of Information Security (http://dx.doi.org/10.4236/ jis.2013.44022, ISSN 2153-1242, Volume 4, October 2013). Benefits of RNA-FINNT like speedy computation, execution in parallel, reduction in error and diminution in error approximation are also stated in this chapter. Another focus of the chapter is complexity of RNA-FINNT.

Chapter 5 focuses upon experiments and results of RNA-FINNT. Chapter gives details that how to set environment for experiment, graphical user interface of MATLAB, main menu creation in MATLAB, database of images, implementation of RNA-FINNT and reckoning of minutiae points for augmented trust and privacy. Version of experiment is published in Networks and Communications 2013, Springer Lecture Notes in Electrical Engineering (doi: 10.1007/978-3-319-03692-2_17, ISSN: 1876-1100, Volume 284, January 2014).

Chapter 6 focuses upon performance evaluation and validation of results of RNA-FINNT. Testing of RNA-FINNT and computation of performance indicators is done in this

chapter. Distortion tolerance of RNA-FINNT is computed in this chapter. Validation of RNA-FINNT is substantiated with preset conditions on the basis of error percentage, average processing time and average matching time. Overall recognition accuracy of RNA-FINNT is also computed in this chapter. Substantiation of implementing RNA-FINNT into biometric machines results in augmented security is accomplished in this chapter. The version of Chapter 6 is published in Advances in Electronics, Electrical and Computer Science Engineering 2012(doi: 10.3850/ 978-981-07-2950-9 376, ISBN: 978-981-07-2950-9), Advances in Information Technology 2012 (doi: 10.3850/978-981-07-2683-6 AIT-104, ISBN: 978-981-07-2683-6), Advances in Computer Science and Electronics Engineering 2013 (doi: 10.3850/978-981-07-5461-7_12, ISBN: 978-981-07-5461-7, 2013) and Inderscience International Journal of Computer Applications in Technology Special Issue on Advances in Networking and Signal Processing for Social Security (doi: 10.1504/IJCAT.2015.068924, Volume 51, No. 2, April 2015).

Chapter 7 concludes the thesis by suggesting possible improvements like assimilation of fingerprint with password to add one more tier of security, extracting minutiae points of noisy fingerprints, increase or improve the overall recognition accuracy of the algorithm and future expansion in hardware domain like behavioral, structural and physical implementation.

I would never have been able to accomplish my objective of thesis without the blessing of God, guidance of my supervisor Dr. G.Geetha, help from friends and support from my family.

I would like to express my gratitude to my supervisor Dr. G.Geetha for her excellent guidance, atmosphere, care and patience towards me and my work. She was always involved throughout the thesis concept formation, execution, experimentation and composition. My special thanks to the faculty and students Soumik Dey, Pankaj Kumar Rai and Vakul Sharma of Lovely Professional University, Phagwara, Punjab (India) who contributed for the smooth conduct of the survey in the various parts of Punjab and fingerprint database formation. Personal thanks to students Maninder Singh, Anshu Anand, Ram Modi, Saurabh and Varinda Sharma of Lovely Professional University, Phagwara, Punjab (India) who helped us for aggregation of data of the survey. My special

gratitude towards Ms. Seema, Mr. Nikesh Bajaj, Mr. Manish and Mr. Ghosh for their intellectual contribution and scientific guidance for writing the code of RNA-FINNT and mathematical contributions. I thank the laboratory staff for their cooperation for the smooth conduct of experimentation as all of the work presented henceforth was conducted in the laboratory of Lovely Professional University, Phagwara, Punjab (India). Special thanks to Mr. J.Singh for guiding in hardware domain for the future expansion of the thesis. My research would not have been possible without their help.

Finally I would like to thank my sister Dr. Harmeet Kaur, brother in law Dr.Gurpreet Singh, brother Advocate Kulbir Singh Brar and sister in law Ms. Mandeep Kaur who always motivated me to contribute more to bring efficacy. Moreover my father Advocate Sukhdev Singh Brar and mother Mrs. Mohinder Kaur Brar who were always there cheering me up and stood by my side through the good and bad times. Words cannot express how gratifying I am towards my aunt Mrs. Rashmi Rampal and cousin Assistant Professor Mr.Shiven Rampal for all of the sacrifices that they have made on my behalf. The prayers of my family members were what sustained me thus far. I would also like to thank all my friends who supported me in writing and executing the complete thesis. They incented me to strive towards my goal. At the end I would like express appreciation to my loved one who spent sleepless nights with and was always standing for my support in the moments when there was no one to answer my queries.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

A	—	Accepted Value
ACM	—	Association for Computing Machinery
B	—	Bifurcations
DT	—	Distortion Tolerance
E	—	Experimental Value
e	—	Error Approximation
EER	—	Equal Error Rate
EFD	—	Existing Fingerprint Database
EL	—	ElGamal Based Scheme
EPR	—	Error Percentage
FAR	—	False Acceptance Rate
FFT	—	Fast Fourier Transform
FMR	—	False Match Rate
FNR	—	False Non Match Rate
FRR	—	False Reject Rate
FTA	—	Failure to Acquire Rate
FTC	—	Failure to Capture Rate
FTX	—	Failure to Extract Rate
GAR	—	Genuine Acceptance Rate
GM	—	Geometric Mean
GUI	—	Graphical User Interface
H	—	Hash Based Scheme
HTTP	—	Hypertext Transfer Language
LSHF	—	Linear Symmetric Hash Function
M	—	Minutiae Points

MATLAB	—	Matrix Laboratory
NFD	—	Noisy Fingerprint Database
NGMS	—	Number of Genuine Matching Scores
NGRA	—	Number of Genuine Recognition Attempts
NIMS	—	Number of Imposter Matching Scores
NIRA	—	Number of Imposter Recognition Attempts
NIST	—	National Institute of Standards and Technology
p	—	Password
PKI	—	Public Key Infrastructure
R	—	RSA Based Scheme
RA	—	Recognition Accuracy
RNA-FINNT	—	Reduced Number of Angles Fingerprint Hash Algorithm
RTFD	—	Real Time Fingerprint Database
SMR	—	Self Match Rate
SQL	—	Structured Query Language
SSL	—	Secured Socket Layer
T	—	Terminations
t	—	Threshold Fixed
TAR	—	True Acceptance Rate
TCP/IP	—	Transmission Control Protocol/ Internet Protocol
THV	—	Threshold Value
TRR	—	True Reject Rate

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

1

Introduction

CHAPTER – 1

INTRODUCTION

1.1 OVERVIEW OF THE TOPIC

World is growing every single day and the development of technology has affected all the surfaces of growth. Technology has benefited in the expansion of all scientific areas like physics, chemistry, biology, finance, medicine, data analysis etc. With the advancements of technology people come to know that it could bring ease to their daily course of activities. This need motivated the software programmers to develop softwares which could be used to incorporate ease at work and bring effectiveness in the potential of individual. This drastic boom in computer industry resulted in developing graphical user interface applications in the field of computer methodologies. But main concern for these graphical user interfaces is to provide complete security to the users. Mainly authentication process is significantly used for strong security and privacy of the users.

Authentication is possible with various identity authentication parameters but biometrics based authentications are not vulnerable to attacks by the intruders. Biometrics based graphical user interfaces provide burly security when employed in security critical applications of computer vision also. This focused upon two main challenges in front of programmers: one is to design a system for image processing which could work on vectors and matrix and could have more interactivity and second is to provide strong security and privacy to the legitimate users in the public insecure network.

Creation of tools like MATLAB, Khoros, Afni, MRIcro, MrGray etc and with implementation of various identity authentication parameters like passwords, smart cards, fingerprint, iris, speech, face recognition etc resulted in achieving these challenges. But further challenge is to choose the best tool and identity authentication parameter for strongest security and privacy for the legitimate user.

MATLAB allows easy matrix manipulation, plotting of data and functions, creating graphical user interfaces so this tool is used in the thesis for designing a system for image processing and it substantiates its qualitative approach using image processing for

identity authentication. So thesis focuses upon identifying best identity authentication scheme with strong security and privacy to the users. Thesis contributes into two major ACM (Association for computing Machinery) Classifications: Security and Privacy as main focus on security services with authentication through biometrics and Computing Methodologies as main focus on computer vision with tasks through biometrics [1].

1.2 HYPOTHESIS OF THE STUDY

The main supposition or proposed explanation made in the thesis on the basis of limited evidence as a starting point for further investigation is i.e Hypothesis of study: Public Network is the most insecure network. While legitimate user communicates through the public network there is problem in sustaining security and privacy as intruders could apply various attacks to impersonate the identity. So there is need to have Ideal Authentication Scheme which should be derived through a new algorithm which results in diminution of errors for the enhancement in the authentication and identification process of legitimate user over the public network. Result would be advancing science with respect to pattern recognition and contributing for security and privacy through authentication and computing methodologies with tasks through biometrics.

1.3 OBJECTIVES OF THE STUDY

The objectives of the thesis are as follows:

- Advancing science with respect to pattern recognition in the areas of security and privacy and computer methodologies
- Deriving a New Fingerprint Hash Algorithm (RNA-FINNT) with diminution in the percentage or approximation of error resulting in Ideal Authentication Scheme
- Augmentation of security and privacy of legitimate user by improving the overall recognition accuracy of the identity authentication parameter

1.4 SCOPE OF THE STUDY

Thesis focuses upon subject matter of biometrics in security and privacy and computer methodologies by main focus on authentication and computer vision through biometrics respectively. As per the ACM classification on computing systems following is the scope of thesis [1]:

1. **Security and Privacy:** The biometrics based authentications are significantly used for user authentication. Thesis proposes a biometric based graphical user interface which could withstand various attacks when employed in security critical applications and is not vulnerable to security requirements illustrated with fingerprint authentication [2]. Thesis contributes in the security and privacy classification of computer by ACM in the form of authentication through biometrics.

2. **Computer Methodologies:** Methodologies mainly focus upon the application areas of computation. Thesis contributes in the computer vision application area through biometrics. Computer vision analyzes high dimensional data by extracting, processing and understanding the images in order to produce some information. Thesis contributes in the computer methodologies classification of computer by ACM in the form of computer vision through biometrics.

3. **Intersection of Computing Classification Systems:** Thesis intersects two main computer system classifications of ACM security and privacy and computer methodologies by authentication and computer vision through biometrics.

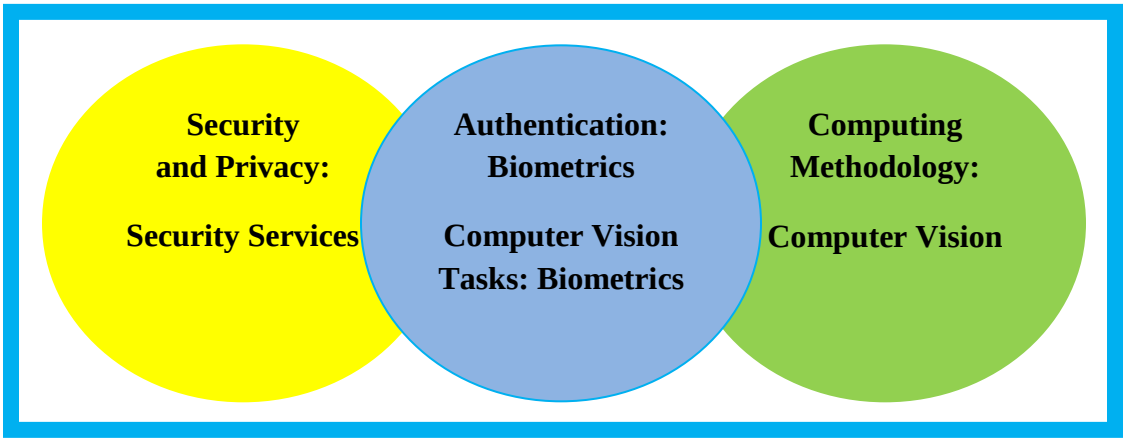

Figure 1 : Scope of the Thesis

1.5 FLOW OF METHODS AND TECHNIQUES

One of the purposes of the thesis is to learn new information about image processing, implementation of new fingerprint algorithm (RNA-FINNT) through MATLAB and validation of algorithm by verifying conditional requirements so there are many ways to

support this learning process. Structured and unstructured data gathering processes e.g helping tools, written materials, research papers on previous topics, internet, Mathworks tool both are followed for deriving the information. Complete literature review is done and decision on the application part of the learning is done in the thesis. Review includes technologies and techniques for fingerprint authentication, experimentation and result analysis of comparative study of technologies and techniques for fingerprint authentication, fingerprint algorithms, deriving a new fingerprint hash algorithm (RNA-FINNT) and making fingerprint match more authentic than the existing on the basis of performance indicators like False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage. Advancing science in the field of pattern recognition is the application part of the thesis. In order to validate the application Graphical User Interface with ideal authentication parameter has been designed for identity authentication and verification. This complete process is executed with the help of MATLAB tool. After preparing the menu bar complete coding is done in MATLAB, details of possible constraints and errors faced are also mentioned in the thesis. Complete process of developing the application for enhancing pattern recognition using MATLAB for identity authentication and verification is followed by experiments on different fingerprints and results are mentioned. Comparative analysis of existing fingerprint algorithms and techniques is done and augmentation of pattern recognition is proved by embedded new algorithm (RNA-FINNT) through experiments and results. Analysis of fingerprint algorithms on the basis of performance indicators like False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage substantiates augmented pattern recognition with RNA-FINNT. Thesis concludes that analysis of fingerprint algorithms proved diminution in error percentage or approximation in RNA-FINNT and thesis points out the areas of the future development and expansion. Finally thesis contributes in the security and privacy and computer methodologies classification of computers by ACM with main focus on authentication and computer vision through biometrics.

2

Review of Literature

CHAPTER – 2

REVIEW OF LITERATURE

Generally all standard methods for identity authentication for security mainly rely upon public-key infrastructure (PKI) [3]. There also exists a class of authenticated key-exchange protocols [4]. These are based on passwords which human has to memorize but these are vulnerable to offline dictionary attacks [5][6]. Whenever data is transferred through transport layer it has to pass through two layers:

- Record Protocol [7]

(It encapsulates higher level protocols (Hypertext Transfer Protocol) and maintains reliability, confidentiality and compresses the message which is transferred [8])

- Handshake Protocol [9]

(It sets up secure channel between server and client. It provides complete information to record protocol [10]. It performs mutual authentication [11])

Critical points of current knowledge, theoretical and methodological contributions are evaluated in this chapter and substantive findings are derived.

2.1 ATTACKS AND SECURITY REQUIREMENTS

Users make use of passwords over a network for security. Organizations use Secured Socket Layer Protocol in their virtual private network for security of legitimate user at Transport Layer [12]. Even though the security seems to be strong but intruders perform various attacks for hacking the passwords. Users should never share passwords and they are always advised to make strong passwords. With strong passwords at the front end the systems use authentication schemes at the back end and the security is ensured [13]. But even these authentication schemes could not withstand all the security requirements and are vulnerable to attacks. These intrusions cause insecurity to the stored passwords of users.

2.1.1 Attacks

Following are the details of different kinds of attacks which authentication schemes should not be vulnerable. Certain attacks with respect to authentication are:

1. Denial of Service Attack [14]

The legitimate user is denied access of resources. Information used for verification is falsified. So login would be unsuccessful because the malicious user intentionally disrupts service to a computer or network resource.

2. DNS Poisoning [15]

DNS Server receives a question from some malicious computer and in return server replies. If the answer gets matched then server completely trusts the computer. Result is that the traffic on the internet can be intercepted, rerouted or impersonated.

3. Forgery Attack [16]

Attacker attempts to modify intercepted communications to masquerade the legal user is falsifying the verification information. It is impersonation attack which has corrupt data.

4. Man in the Middle Attack [17]

In an untrusted public network the sensitive data sent to or received by a user from the router is ruined through deployment of injections or key manipulations by the intruders. It happens when different clients share the same secret or they may create fake certificates.

5. Ping of Death [18]

Malicious ping is sent by the computer. If the IP address of machine to be attacked is known to the attacker then this attack is easily done. Only oversized packets are to be transferred which results in buffer overflow, crashing and data fragmentation.

6. IP Spoofing [19] [20]

False IP address is communicated over the network and attacker assumes a new identity so the replies generated by the destination would automatically sent to attacker. Attacker maintains the protocol requirements so it exploits trust relationships between the routers.

7. Parallel Session Attack [21]

A valid login message is created by the intruder out of some eavesdropped communication of the user. There is no need to know the user's password it could be created through valid login of legitimate user.

8. Replay Attack [21]

Previous communication of the legitimate user is stored by the intruder. On the basis of the stored information impersonation is done. The intercepted messages are replayed and finally intruders capture the traffic of the network. Even the encrypted intercepted messages are replayed and intruder gets the login.

9. Ping Broadcast [22]

Ping is sent to all the hosts present in the network mentioning the IP address of machine to be attacked. Finally there is flood of responses for the attacked machine and the system is unable to operate or sometimes even gets locked.

10. Password Guessing Attack [23]

Guess is made through the stored authentication messages. Majority passwords have low entropy so they could be easily guessed.

11. Server Spoofing [24]

Sensitive data is manipulated by the intruder and they pretend to be server. Intruders masquerade the data of the legitimate user. As TCP/IP does not provide any mechanism to prove the authentication of server and client so the data becomes vulnerable to attack.

12. Session Hijacking [25]

Traffic of the network is routed to the false server by the intruder. It is done through address resolution protocol poisoning of the router. Data is injected into an unencrypted server; origin of the malicious user is hidden in this attack as it is based on host and network both.

13. Smart Card Loss Attack [26]

Smart card of the legitimate user if lost or stolen then the attacker could easily modify the stored password through password guessing attacks, dictionary attacks.

14. Smurf Attack [27]

The target network generates large number of PING requests. It is a DOS attack but not operating system specific. Ping broadcasting is done which results in flood of responses.

15. Stolen Verifier Attack [28]

Attacker steals the passwords (hashed code) from the server and impersonates the legitimate user to login into the system.

16. Teardrop Attack [29]

It is a kind of denial of service attack. In it the packet is divided into fragments. Confusing offset value in the second or later fragment is stored by the intruder which could result in system crash.

2.1.2 Security Requirements

Certain security requirements for network security with respect to authentication are:

1. Forward Secrecy [30]

This requirement ensures even if the secret key is revealed then also stored passwords are secure in the system. Repetitive use of keys should not be there from the same or different data resource.

2. Mutual Authentication [31]

It is a kind of authentication which is done mutually by Server and Client. This type of authentication withstands server spoofing.

3. Confidentiality [32]

It is a kind of requirement which ensures that data accessed and read over the network or transmitted over the network should only be done by authorized users.

4. Integrity [32]

In this requirement of network security the modifications done in the data transmitted should be done by authorized users to increase the authenticity.

5. Availability [32]

This requirement ensures the availability of data should be only to the authorized users in the network while transmission or communication.

From the specification of attacks and security requirements it is clear that trusted paths are required for complete network security. Security functions and users can easily communicate between each other with trusted paths [33]. This review originated need to analyze the existing trusted paths parameter schemes like passwords etc.

2.2 EXISTING PASSWORD AUTHENTICATION SCHEMES

There are few authentication schemes which run at the back end of the system to enhance the security level of the passwords. Current data security and cryptographic techniques or schemes for password authentication and there algorithmic details are:

1. **RSA Based Scheme** (Proposed by Rivest, Shamir and Adleman in 1978 it is public key cryptosystem. It is used for encryption. Its security is based on factoring large or huge numbers) [34]. Process is:

- Take two prime numbers *p* and *q* and consider as private keys,
- Multiply them and compute *N i.e p * q = N* which is public key.
- Calculate *(p-1) (q-1)* and *c*hoose one relative prime number *e* (Public Key).
- Compute *c* by $M^e (mod\ N)$ on the basis of Chinese Remainder Theorem.
- *c* is the encoding which is sent by *B* to *A.*
- *A* calculates on the basis of Fermat's Little Theorem i.e *ed=1(mod (p-1) (q-1))* and $c^d\ (mod\ N)$ and decode the message
- *M* is generated.
- If this generated *M* is same as the send message then authenticity is proved otherwise someone is trying to impersonate the legitimate user.

But this scheme is vulnerable to and could not withstand the mutual authentication security requirement.

2. **ElGamal Based Scheme** (Proposed by ElGamal in 1985 it is public key cryptosystem used for encryption [35]. Discrete logarithmic values are calculated taking finite numbers into consideration. It is an alternative to RSA [36]. Process is:

- Take prime number q and two random numbers g and x such that g and $x < q$.
- Compute $p = 2^k q+1$ by picking another random number k
- Compute $y= {}^{gx} \bmod q$
- x is the private key. p,g *and* y are public key and M is message sent by A to B.
- Calculate $a = y^k M \bmod p$ and $b = g^k \bmod p$ and the output would be (a,b).
- Now decryption would be performed that M would be computed that either $M = a$ *or* $M = b^x$

Encryption under this scheme requires exponentiations twice but decryption only requires one exponentiation. Three steps are followed in this scheme: Setup (generating public and private or secret key), Encrypt (takes message and public key as input and produces cipher text) and Decrypt (takes cipher text and secret key and produces message).

But the scheme is vulnerable to attacks like dictionary attack, password guessing attack, parallel session attack and could not withstand the mutual authentication which is the security requirement while transmitting data from client to server or vice versa.

3. **Hash Based Scheme** (Various types of hashing is used in this scheme which would enhance the performance of the transmission) [37]. Ways of hashing are:

- One way Hashing i.e $y = h(x)$.
- Direct Hashing i.e hashing of source and destination address using XOR gate. Checksum of the internet is performed at the end.
- Table based Hashing i.e traffic is separately loaded and split on the transport layer.

A message with arbitrary length is taken as an input and a fixed length message is produced as an output during the implementation of one-way or direct hash scheme. Example: $y = h(x)$ which takes message x having arbitrary length as input and returns fixed length hash value y as output. Sender assumes that the message is correct. Message sent is appended with hash value at the source and at the receiving end re-computing of hash value is done along with authentication [38]. Process is:

- Take block data of any size and hash scheme *h* would be applied to it.
- *h* would take arbitrary length input and would produce a fixed-length output.
- It is very easy to compute $h(x)$ for any given value of x. *(There exists a polynomial-time algorithm that on input x outputs h (x))*
- But if $h(x)$ is given, it becomes infeasible to find x. *(There is negligible probability to find inverse of x under h in polynomial time algorithm)*
- Even if $h(y) = h(x)$ then also it is computationally infeasible to find that $y \neq x$. It is because of the weak collision resistance at the transport layer. *(With some non-negligible probability, all inverting algorithms fail to invert functions)*
- Now even if the transport layer has strong collision resistance it is computationally infeasible to find any pair (x,y) such that $h(x) = h(y)$. *(There is a negligible success in inverting functions by any efficient algorithms)*

The scheme is vulnerable to smart card loss attack but could very well withstand the requirement of mutual authentication.

Overall comparison of all the schemes on the basis of attacks and security requirements as mentioned in Table 1 and Table 2 of Chapter 3 proved that hash based scheme is the strongest of all the schemes. It can withstand all the security requirements but is vulnerable to only smart card loss attack. So here raises the question that amongst all the identity authentication parameters which is most appropriate and acceptable for implementation of trusted paths. Trusted paths are used in order to prevent the use of password grabbers and session grabbers which is a kind of Trojan horse program that is used to request the passwords from users and software that intercepts the communication between system and the user respectively. With the choice of most appropriate identity

authentication parameter it is possible to meet all security requirements defined in the thesis and it would not be vulnerable to attacks. Moreover user should never provide the security information to another user except the trusted paths.

2.3 MOST ACCEPTABLE IDENTITY AUTHENTICATION PARAMETER

Gartner Survey of 2002 focused that fingerprint recognition could be made more foolproof with security chip card applications [39]. But what if the chip card gets stolen so there is need to identify the most appropriate and acceptable identity authentication parameter. Whenever there is a public network the identity authentication parameters are required for mutual authentication between client and server. As there are many identity authentication parameters like password, smart card, fingerprint, pass phrase etc so there was need to conduct a Survey for analyzing the most appropriate and acceptable parameter. Questionnaire was framed for smooth conduct of the survey and organizations like Colleges, Universities, Courts, Banks and Schools are the part of the Survey. Brief introduction regarding the cause of survey and its importance was given to the participating sample of users. Vast response was given by users to the Survey as it was completely concerned about the security of transactions and data being transmitted in the most insecure public network. Sample size of the survey is 500. On three different basis the survey was analyzed [40]:

- Choice of the user on the basis of acceptability
- Choice on the basis of Gender
- Choice on the basis of Age

Below stated is the complete analysis of the survey depending upon the question asked and the highest agreed reply of the users. Explanation of the most accepted answer is given through pictorial representation in the form of Chart. Following answers prove the most acceptable identity authentication parameter [40]:

Depending on the questionnaire password is the most common and accepted authentication method for online transactions which is generally used by the users *(Figure 2)*.

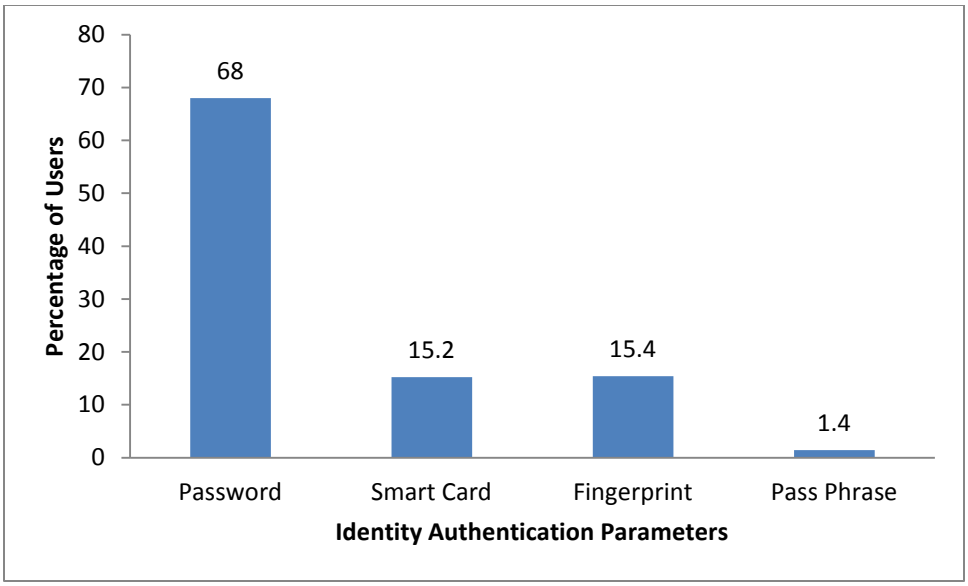

Figure 2 : Most common and accepted authentication parameter

Depending on the questionnaire security is the most concerning challenges in online transactions *(Figure 3)*.

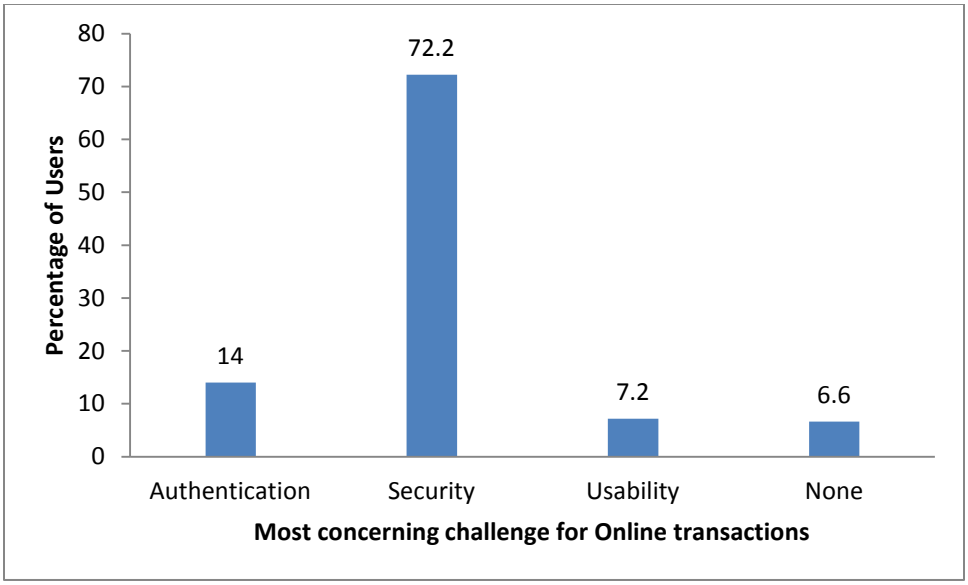

Figure 3: Most concerning challenges in online transactions

Depending on the questionnaire passwords and tokens have medium security during online transactions *(Figure 4)*.

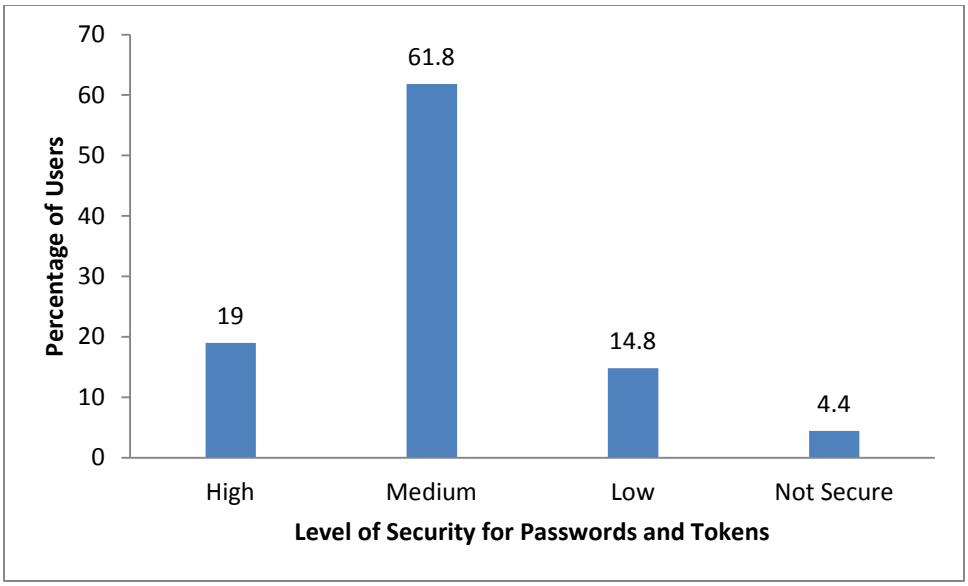

Figure 4: Level of security for passwords and tokens

Depending on the questionnaire users perceive usability of passwords and tokens at medium level during online transactions *(Figure 5)*.

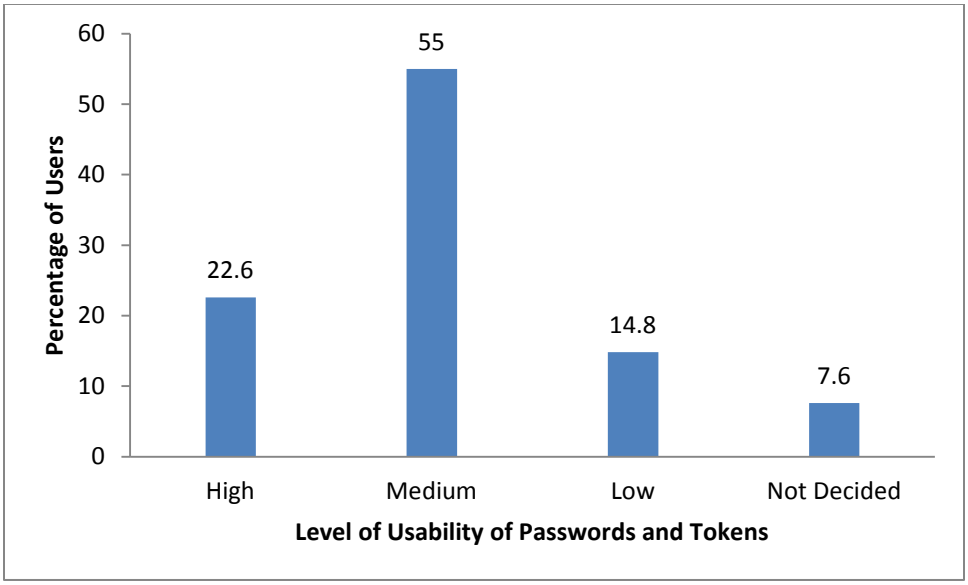

Figure 5: Level of usability of passwords and tokens

Depending on the questionnaire in future users would prefer fingerprint as authentication parameter for online transactions *(Figure 6)*.

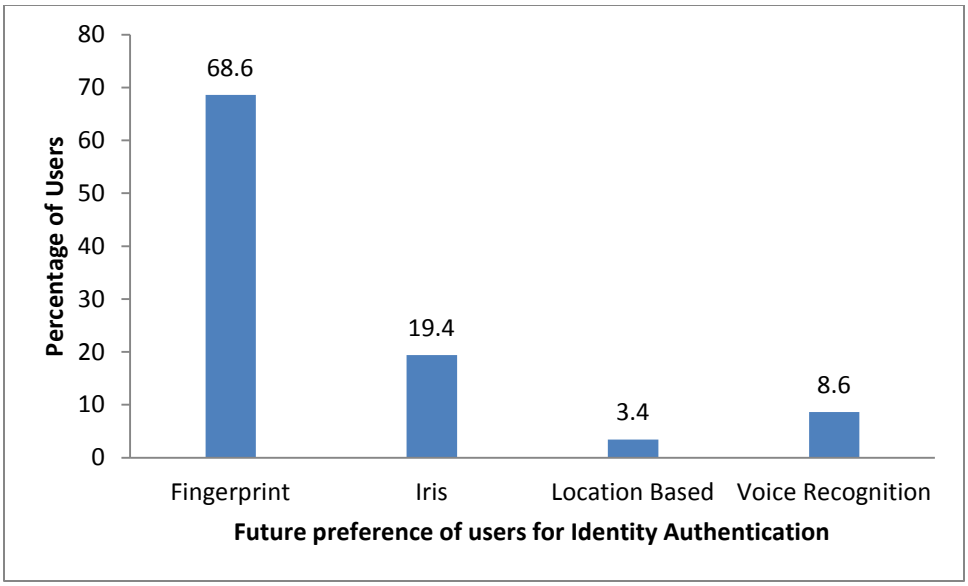

Figure 6: Future preference of users for identity authentication

Depending on the questionnaire the acceptability for security and privacy would be at highest level if fingerprint is used as an authentication type *(Figure 7)*.

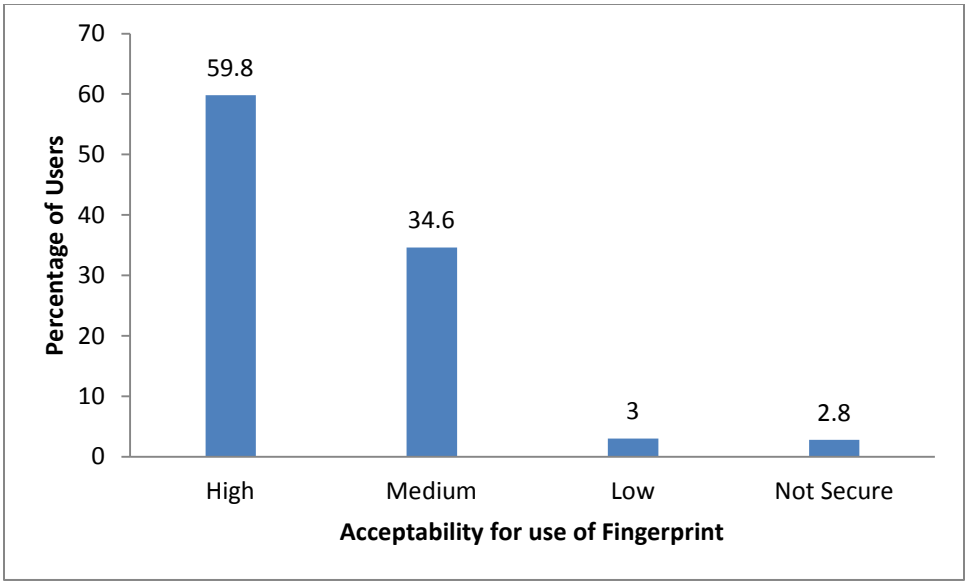

Figure 7: Acceptability for use of fingerprint

Depending on the questionnaire all of the above are expected by majority of the users for secure transactions *(Figure 8)*.

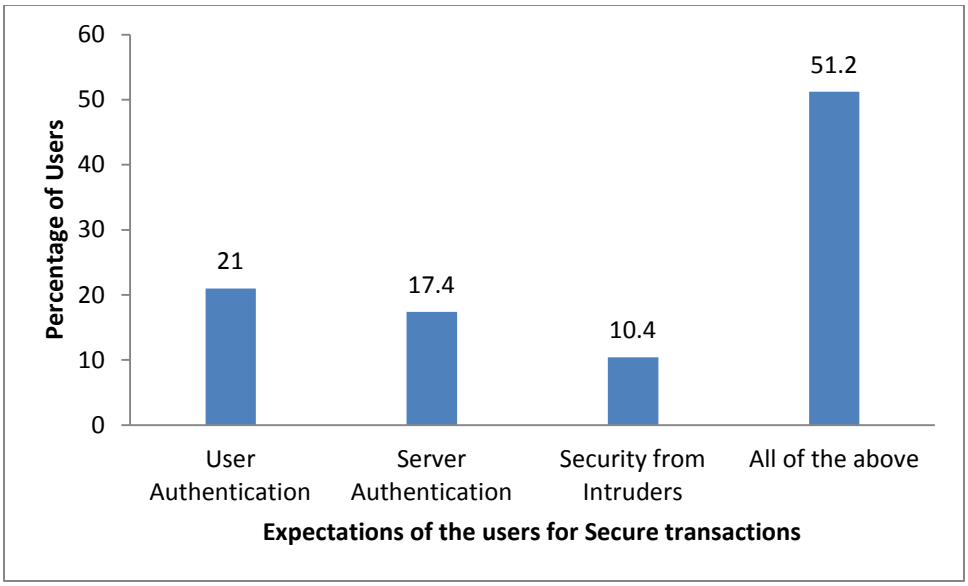

Figure 8: Expectations of the users for secure transactions

Depending on the questionnaire if fingerprint is used as the authentication parameter in online transactions then possibility of acceptance of data being completely secure is very high *(Figure 9)*.

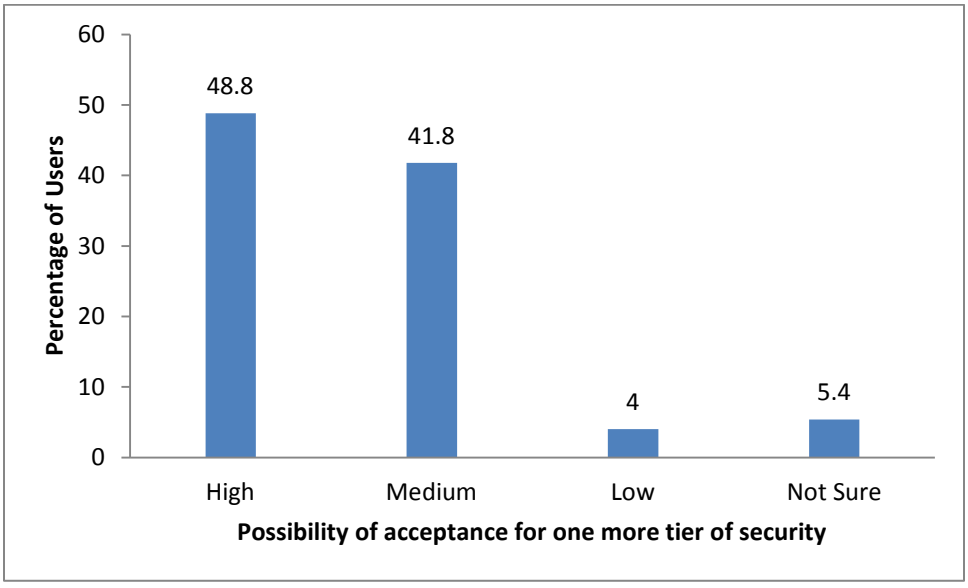

Figure 9: Possibility of acceptance for one more tier of security

Depending on the questionnaire by adding one more tier for enhancing security may result in some additional cost, so the possibility of acceptance to bear that nominal cost is at medium level by the users *(Figure 10)*.

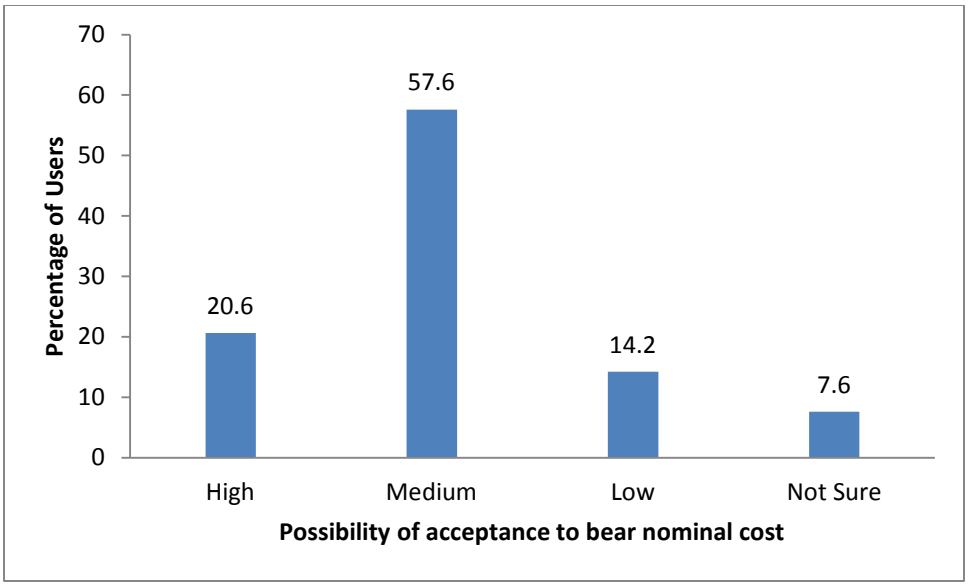

Figure 10: Possibility of acceptance to bear nominal cost

Depending on the questionnaire any prototype resulting in complete security then the possibility of user's willingness to purchase is at high. Users can bear additional cost for getting complete security *(Figure 11)*.

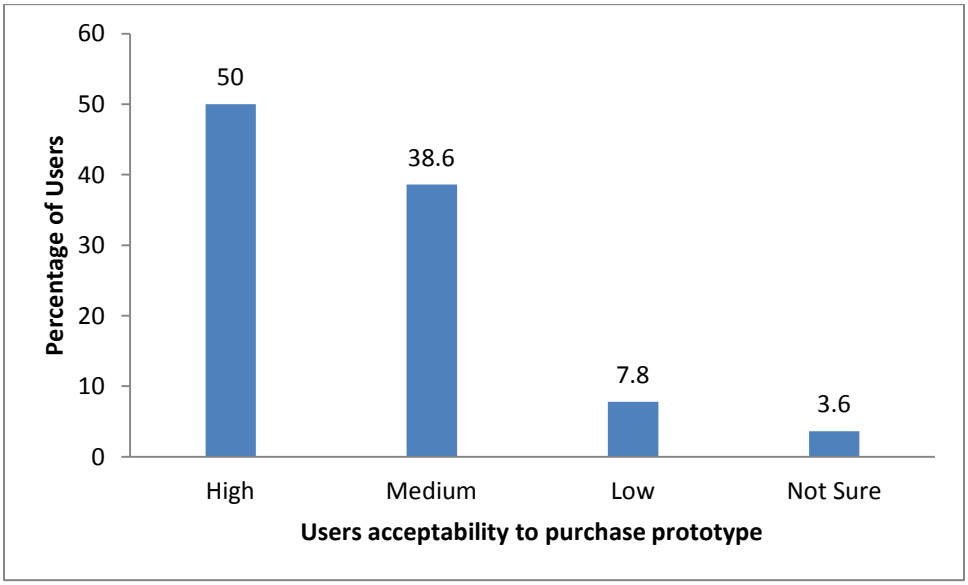

Figure 11: Users acceptability to purchase prototype

As per the results of the survey the most appropriate and acceptable parameter is fingerprint for data being transmitted in the most insecure public network. Result is

analyzed on the basis of choice of the user on the basis of acceptability, choice on the basis of Gender and choice on the basis of Age. From the analysis of the survey following are the results [40]:

- Passwords are generally used by users for online transactions.
- Most concerning challenge in online transactions is security.
- Medium security is with the passwords and tokens.
- Users needs enhancement of security.
- Users will accept fingerprint as authentication parameter for online transactions in future.
- With fingerprints security and privacy would be at highest level.
- Majority users want user authentication, server authentication and security.
- Data would be completely secure with use of fingerprints.
- Users are ready to bear cost for enhancing security.
- Users accept to bear nominal cost for new prototype which results in complete security.

Gartner Survey of 2013 also focused upon revival of biometrics in banking: Heralding a New Era in mPayments [41]. Gartner Survey of 2013 matches the results of our survey done in 2012. This survey leads to analyze the types of fingerprints.

2.4 TYPES OF FINGERPRINTS

After smooth conduct of survey it was proved that fingerprint is the most acceptable identity authentication parameter and it should be used for future transactions. Here originated the need to know about different types of fingerprints [42]. Fingerprint schema is classified into six categories:

Arches: Ridge enters from one side, in the center it makes a wave and then flows in the opposite side. The pattern of the arch is made up of ridges which lie one above the other in a general arching formation *(Figure 12)*.

Tented Arch: Angle is there in the arch. The pattern consists of at least one up thrusting ridge and it tends to bisect superior ridges at right angles either more or less *(Figure 13)*.

Figure 12: Arch Schema

Figure 13: Tented Arch Schema

Right Loop: It has one or more free recurving ridges in the loop. There is one delta also. Depending upon which hand loop pattern comes from and impression is taken defines the direction. If the ridges flow in from the side of the little finger then it would be an 'ulnar' loop *(Figure 14)*.

Left Loop: If the ridges flow in from the side of the thumb then it would be a 'radial' loop. It may be a combination of two loops pointed in opposite directions. It resembles to the shape of eye but is so unique that it needs to be considered separately *(Figure 15)*.

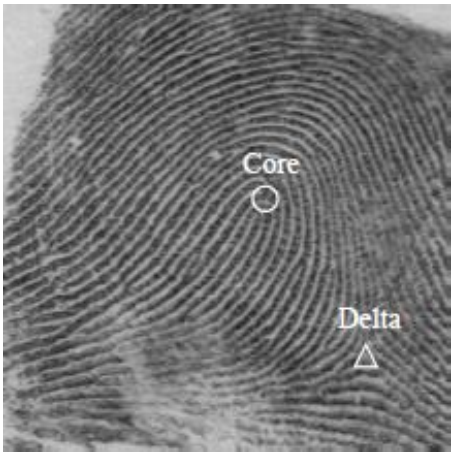

Figure 14: Right Loop Schema

Figure 15: Left Loop Schema

Twin Loop: It has more than two free curving ridges and one delta. The placing of hand palm for fingerprint defines if the recurving ridges originate from the little finger or

thumb side or not. Depending upon the loop pattern it is assured that fingerprint is ‘ulnar’ or ‘radial’ *(Figure 16)*.

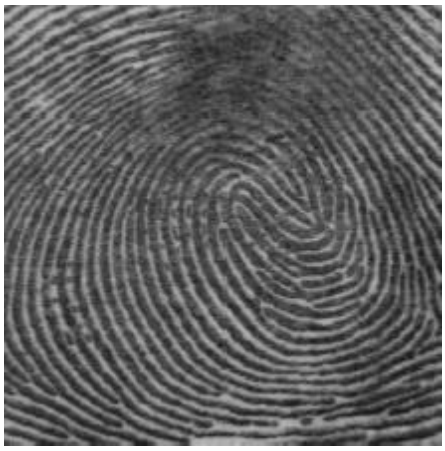

Figure 16: Twin Loop Schema

Figure 17: Whorl Schema

Whorl: Any fingerprint that consists of two or more delta’s is whorl. Two points of delta are there and pattern has one or more free recurving ridges. When the line of the fingerprint disc is placed on the two points of delta then it will bisect at least one of the ridges which belong to the core group *(Figure 17)*.

Following are the technologies used for extraction of fingerprint images: Correlation (in it the image itself is used as the template) [43]: It is very easy to recreate fingerprint from these templates so it will give access to unauthorized users so ultimately it is not safe to use. Texture Descriptors (it uses fingerprint texture): in a compact fixed length vector the global and local features of a fingerprint are captured which would be finger code. Minutiae Descriptors (these are the set of unique features in finger print): Bio hashing is mainly used to replace the template based matching (Correlation). These are set of unique points on the fingerprint and none of the individual has the same number of minutiae points at the same location [44].

Everyone falls into one of the above said types of fingerprint like arches, tented arch, right loop, left loop, twin loop and whorl [45]. Within these types of fingerprints there are more than thirty different minutiae points [46]. This makes fingerprint unique and none of the individual has the same number of minutiae points on the same place. So in the thesis fingerprint is used as an identity authentication parameter and technology used is minutiae descriptors [47].

2.5 NEED FOR GENERATING IDEAL AUTHENTICATION SCHEME

To authenticate the legitimate user various authentication schemes could be used. As per the survey done the most acceptable and appropriate identity authentication parameter is fingerprint. So while generating an ideal authentication scheme fingerprint has to be part of that and fingerprint should be capable of doing mutual authentication [48]. In this thesis it is proposed that Ideal authentication scheme can have either assimilation of password with fingerprint or only fingerprint could be used. Details are as follows:

1. **Assimilation of Password and Fingerprint** [49]**:** After analyzing the security requirements and attacks it is proved that password alone cannot provide strong security. So another identity authentication parameter needs to be assimilated with password for enhancement of security. This thesis suggests assimilating fingerprint with the password. Both the identity parameters are to be extracted and stored as hash code in the database. Example: In online banking the security of the user lie on passwords initially the user login and then the profile login. If fingerprint is assimilated along with password then during the session login of user security would be enhanced.

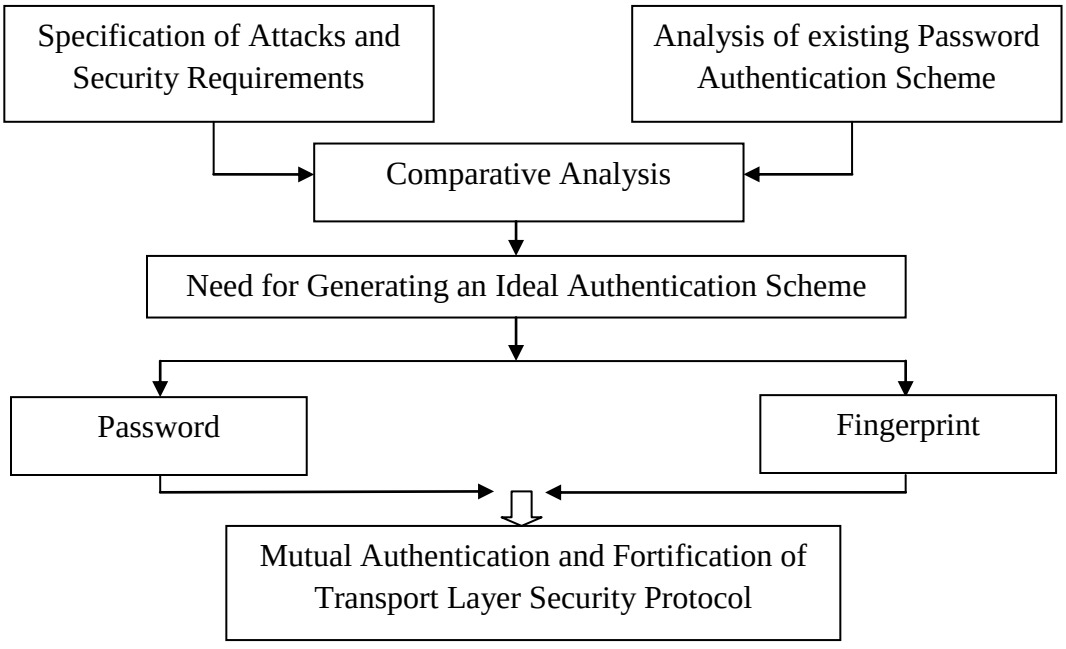

Figure 18 : Generating Ideal Authentication Scheme

2. **Fingerprint as Identity Authentication Parameter** [50]**:** Analysis of survey proved that most acceptable and appropriate identity authentication parameter is fingerprint. So in order to fortify the security fingerprint would result as an ideal authentication parameter. Instead of password fingerprint should be implemented. It will result in bio-hashing and possibility of its unauthorized access is nil. For justifying that fingerprint alone can be used as an ideal authentication parameter study of all the fingerprint algorithms is required. Comparative analysis of all the fingerprint algorithms and technologies would substantiate that fingerprint is an ideal identity authentication parameter.

So to generate an ideal identity authentication parameter comparative analysis of all the fingerprint algorithms along with their technologies and techniques used for authentication is required.

2.6 TECHNOLOGIES AND TECHNIQUES FOR FINGERPRINT AUTHENTICATION

Substantiating that fingerprint is the ideal identity authentication parameter the details of technologies and techniques used for fingerprint authentication are:

1. Singularity Detection

In year 1980 the singularity detection extracted the minutiae points automatically but sometimes extracts the noise during the process [51]. So to avoid noise enhancement algorithm was implemented and based on local ridge orientation and the frequency the structures of ridges and furrow was improved.

2. Edge Detection

In year 1986 it was proposed that localization and numerical optimization of ridges is important for capturing human characteristics with the help of any biometric machine. A detector was proposed in 1986 which uses adaptive threshold to eliminate the streaking of contours in edges [52]. The output derived from this detector is combined using feature synthesis but it took too much of time for computation of large responses.

3. Graph Matching

In year 1986 some other researchers defined those minutiae points in two ways: Ridges and Intersect. The end points are the ridges and joining of ridges is intersect [53]. Encoding the location of minutiae points is done with topological relationship of fingerprint images represented in graph. Graphs were successful because they resulted in less noise, rotation and distortion [54]. But problem was that it was done manually so ridge breaks were ignored.

4. Directional Image

In year 1987 transformation results in change of direction of fingerprint image and brings uniformity in the local gray scale levels but performance is not good. Moreover directional image is used for segmentation of the original image and performs best [55]. During process of fingerprint extraction the histogram is created for directional image and segmentation.

5. Filter Design

In year 1989 filter design were used for fingerprint extraction and matching. Detailed process was: specification of user's image, local ridge orientations, smoothing of ridges, enhancement of the fingerprint image, matching of masked filters and finally post processing to reduce noise [56]. In year 2000 scaling, translation and rotation is done for multiple representations of fingerprints and gabor filters were used to compute the average absolute deviation.

6. Structural Matching

In year 1990 the researchers focused upon identifying the distortions occurred in the fingerprint image for which they proposed the use of structural model for fingerprints. Ultimately automated fingerprint recognition system was developed for structural model for fingerprints [57]. But again it was having less speed and distortions were not completely addressed.

7. Localized Spatial Filters

In year 1990 localized spatial filters were proposed. It modulates by 2-D Gaussian functions. But its use originated the need of sampling and quantization densities but has not focused upon effects of quantizing the filter coefficients when implemented in biometrics [58].

8. Texture Analysis and Optical Flow

In year 1990 there was problem in detecting the orientation but later on it was resolved by using least square sense. For segmentation of texture and optical flow when the image is extracted using biometrics computations are to be performed in the spatial domain without doing the Fourier transformation [59].

9. Gabor Filters

Multichannel and spatial frequency domains are characterized by Gabor filters. For segmentation unsupervised square error clustering algorithm is used. Clustering algorithm performed texture discrimination so ultimately texture segmentation algorithm based upon Gabor filters was used. Enhanced version of Gabor filter improved Gabor function [60]. It optimized the standard deviation and the filter window size.

10. Genetic Algorithm

In year 1992 the problem of effective optimization was solved by using genetic algorithms. This algorithm works on probability transition rules and coding of parameter sets. Process of genetic algorithm include: initialization, evaluation of complete parameter set, reproduction, crossover and mutation [61]. It also used Gabor filters to optimize the ridge frequency with standard deviation and resulted in enhancement of fingerprint image.

11. Directional Fourier Filtering

In year 1994 focus upon the size of fingerprint was made and if the fingerprint image is of full size then Fourier domain filtering is done. It is done with 2-D fast Fourier transform (FFT). So Directional Fourier filtering uses full image and for enhancing

binary images thresholding was introduced [62]. This filter removes unwanted information or noise from the fingerprint image.

12. Non Linear Dynamical System

In Directional Fourier filtering thresholding was introduced but because of this need of restoration and halftoning for the formation of animal patterns was originated [63]. For this novel non linear dynamical system called M-lattice system was used. Initial experiment was done on Zebra stripes. M-lattice system was closely related to cellular neural network and hop field network [64]. Mostly M-lattice system was useful in engineering applications because of its efficiency and large signal boundedness.

13. Adaptive Flow Orientation

Structural features are extracted with flow orientation. Adaptive filters are designed with flow fields [65]. With the help of adaptive filters exact location of the ridges could be identified by using waveform projection. In the post processing stage features of fingerprint are extracted with morphological operator [66]. Later on improvement on the accuracy and speed was proposed. The existing Hough transform was having difficulties in implementation so new hierarchical Hough transform algorithm was proposed which is faster and accurate [67].

14. Gray Scale Minutiae Detection

In the year 1997 work upon the intersect (where two ridges meet) was done, and the extracted intersect points were converted into gray scale by gray scale minutiae detection. The problem with this algorithm was when already intersected ridges once again interest at some other location. They produced the same minutiae value [68]. So overall it resulted in having false minutiae points. Enhancement of this algorithm was done that it searched the minutiae point by computing the tangent direction along with section and direction with length.

15. Multimodal Biometric System

Till 1999 all the biometric machines consisted of either filters or non linear dynamical system [69]. But in year 1999 multimodal biometric system was developed in which

integration of various biometric machines was done at the decision level [70]. This system identified the ridge ending and bifurcations of the fingerprint.

16. Smart Cards

In year 2002 smart cards were used for identity authentication along with biometrics. The system which used smart cards worked in three phases: registration, login and verification [71]. In year 2006 remote user authentication scheme was proposed with smart cards on very low computation cost. On same parameters mutual authentication was proposed in year 2010 but in year 2011 strong authentication scheme was proposed which used password and random numbers [72] [73].

17. Cryptographic Key Generation

In year 2004 instead of password and security PIN a strong cryptographic key based biometric machine was proposed. In this data was extracted through biometric machine and generates cryptographic keys and distinguishable features of fingerprint [74].

18. Fuzzy Extractors

In year 2004 the noisy data extracted by biometric machine was given as input but was not reproducible and uniformly distributed [75]. To bring uniformity fuzzy extractors were used to tolerate errors and reproduce biometric inputs without any error and risk of security.

19. Onion Layer Algorithm

In year 2008 the nested convex polygon of minutiae points were constructed then fingerprint matching and verification was done [76]. This is called onion layer algorithm in which fingerprint was divided into equal classes. This algorithm resulted accurate and was very fast but did not use core and delta points for computations [77]. In year 2011 it was proposed that in order to have fast result of search the database should be split into smaller parts. Ultimately false acceptance rate and false rejection rate was reduced [78].

20. Single Hamming Distance Matcher

In year 2009 a much faster multimodal biometric identification system was proposed. It was much accurate and less costly than the system proposed in year 1999 [79]. It used single hamming distance matcher for verification of the extracted fingerprint images.

21. Local Alignment

In year 2009 a novel minutiae based method was proposed which could be used to match the deformed fingerprint. Local alignment means two sets of minutiae are framed [80]. Possibility of any overlapped region which is used to generate new referencing minutiae points is there. For reckoning of minutiae point's threshold is used.

22. Hierarchical Filtering

In year 2011 a novel structural fingerprint based hierarchical filtering method was proposed. In this method first fingerprint with low collision and long structural information were generated and then filters were used for matching [81]. This method was fast and accurate. But in year 2013 focus was more on criminal identification so SVM-KERNEL method was used [82].

2.7 FINGERPRINT ALGORITHMS

After focusing on technologies and techniques the details of all fingerprint algorithms were required. For identifying an ideal algorithm the analysis is done on the basis of performance indicators False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage. Few algorithms also focus upon the distortion tolerance. The details of all fingerprint algorithms are:

1. Phase Based Image Matching Fingerprint Recognition Algorithm

This algorithm is used when fingerprint is robust and has low quality and uses two dimensional discrete Fourier transformation [83][84][85]. Computational results are [86]: EER = .0118 and EPR = 1.18. The values are captured with pressure sensitive sensor of size 384 X 256 pixels having 330 fingerprint images from 30 individuals with 11 impressions for each finger [86].

2. Feature Based Matching Fingerprint Algorithm

This algorithm is used for matching length, orientation, coordinates of the midpoint and average intensity of fingerprint [87]. The values derived through this algorithm are better than 1/3 of the size of the image. Computational results are [86]: EER = .0094, THV = 0.046 and EPR = 0.94. The values are captured are of size 384 X 256 pixels having 330 fingerprint images from 30 individuals with 11 impressions each [86]. Space and time complexity of algorithm is O(n).

3. Standardized Fingerprint Recognition Model

This algorithm synthesizes the template of the fingerprints and if the quality of the image is poor then it removes the complexity [88][89]. Computational results are [90]: FMR = 3.57, FRR = 5, FAR = 3.57 and FNR = 5. GAR = 95 so FRR = 100 - GAR = 100 – 95 = 5%. The database is DB4 FVC2004 with low quality images. Size of fingerprint images is 288 X 384 pixels with 100 individuals, 8 impressions of each finger in total 800 fingerprints [90].

4. Cluster Fingerprint Recognition Algorithm

This algorithm is used for large databases and worked in steps: enrolment, identification and feedback [91]. Computational results are [92]: Penetration Rates are 29.48% and 29.69%. It has 18 clusters for experiment and database is NIST DB4. Size of fingerprint images are 480 X 512 pixels, total 2000 pairs of fingerprints [92]. Space and time complexity of the algorithm is O(n).

5. Fuzzy Vault Scheme Based Fingerprint Recognition

This algorithm is used to identify theft in the social networks or public networks because it has reliable information security mechanisms. It is a kind of biometric cryptosystem which stores only transformed version of the template [93]. Computational results of this algorithm are [75] [93]: FMR = 0.5, FRR = 26.4, FAR = 0.5 and FNR = 26.4.

6. Genetic Algorithm for Fingerprint Matching

This algorithm is used when two impressions of the same finger are extracted and it gives optimal transformation [94]. Computational results are [94]: FMR = 10, FRR = 15, FAR = 10 and FNR = 15. It works on NIST DB4. Size of fingerprint images are 480 X 512 pixels. In total it has 2000 pairs of fingerprints [94]. GAR = 85% so calculated FRR = 100 – GAR = 100 – 85 = 15% [94]. Space and time complexity of the algorithm is $O(m^2)$. Paper states how to tolerate reasonable distortions even in the state of transformations, occlusion and clutter [94].

7. Minutiae Based Matching Fingerprint Recognition Algorithm

This algorithm is very consistent and highly acknowledged [95]. This algorithm used minutiae detection using crossing numbers and midpoint ridge contour method. Minutiae points are more extracted when used with midpoint ridge contour method [96]. Computational results of this algorithm are [86]: EER = 0.0481 and EPR = 4.81. The values stated are captured with pressure sensitive sensor of size 384 X 256 pixels. It contains 330 fingerprint images from 30 individuals with 11 impressions for each finger [86]. Space and time complexity of minutiae based matching fingerprint recognition algorithm is $O(n^2)$.

8. Orientation Estimation Algorithm for Fingerprint

This algorithm is used to improve fingerprint enhancement, classification, and singular points extraction [97]. When this algorithm is implemented with gradient then there is no guarantee of the correctness of ridge [98]. Computational results of orientation estimation algorithm are [99]: Accuracy Percentage = 98, Average Error = 2.50 and Average Execution Time = 16. Scanner used for this experiment is Futronics FS88 and the fingerprint image is 320 X 480 pixels. It has 60 individuals as subject and 10 impressions from two thumbs each so in total 600 fingerprints [99].

9. Novel Algorithm for Detecting Singular Points from Fingerprint Images

This algorithm is used for reconstructing the orientation field. The analysis of singular points are done with topology theory in 2D manifold and states that same number of core

and delta are desired on each fingerprint in this algorithm[100]. Computational results with this algorithm having database FVC2002 DB1_B and FVC2002 DB2_B are [101]: Minimum Processing Time = 2.21 and 2.44, Maximum Processing Time = 4.52 and 7.12, Average Processing Time = 3.14 and 4.52 respectively. Two different sensors were used for these two databases "TouchView II" by Identix and "FX2000" by Biometrika, respectively. Fingerprint image resolution is 32 X 32 pixels [101].

10. Fingerprint Enhancement

This algorithm is used to improve the clarity of ridge and furrow structures through ridge orientation and frequency [102][103]. It calculates the goodness index of extracted minutiae and improves the overall accuracy of the verification process [104][105]. Computational results of fingerprint enhancement algorithm are [106]: Equal Error Rate = 0.202 and Time Cost Per Image = 7.1Sec. Database used in this experiment is FVC2004 DB1. Fingerprint image resolution is 640 X 480 pixels. It has 10 individuals and 8 impressions per finger are taken so in total 80 fingerprint images [99].

11. Grid Hash Fingerprint Recognition Algorithm

This algorithm is used for satisfying protection on the basis of diversity, revocability, noninvertibility and performance [107]. It uses grid based 3-tuple quantization technique. Computational results of this algorithm are [43]: False Match Rate = 1.52, False Reject Rate = 18.32, False Accepatance Rate = 1.52 and False Non Match Rate = 18.32. Database used for this experiment is standard FVCC2002 [43]. Space and time complexity of the grid hash algorithm is O(n log n).

12. Angle Hash Fingerprint Recognition Algorithm

This algorithm is used to match one fingerprint with many fingerprints. Steps used are: enrollment and authentication. Complete database is matched with each and every fingerprint present so consumed more time and resulted in delay [108]. Computational results of this algorithm are [43]: FMR = 1.23, FRR = 14.61, FAR = 1.23 and FNR = 14.61. Database used for this experiment is standard FVCC2002 [43].

13. Minimum Distance Hash Fingerprint Recognition Algorithm

This algorithm focused upon enhancement of the performance while matching one fingerprint with complete database. It was done with hashing [107]. This algorithm used core as local point and reference as global point. It overall improved the performance, speed and accuracy [108]. Computational results of this algorithm are [43]: FMR = 1.87, FRR = 20.32, FAR = 1.87 and FNR = 20.32. Database used for this experiment is standard FVCC2002 [43].

Overall review of all algorithm substantiated that there was need to have a new fingerprint hash algorithm which should result with error percentage, average processing time and average matching time better in comparison to other algorithms.

2.8 NEED OF NEW FINGERPRINT HASH ALGORITHM

Review of fingerprint algorithms was done on the basis of performance indicators like False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage for different applications. It begins the need to derive a new fingerprint hash algorithm which should result in less percentage of error than existing. While considering the Angle hash algorithm the calculation of number of angles is very large [49]. The overall performance is evaluated on the basis of error percentage, average processing time and average matching time. Majority of the algorithms discussed have dependency upon either core/ reference/ delta point so comparison of these algorithms resulted in research gaps which substantiated need for new fingerprint hash algorithm [109]:

1. **False Matching Rate:** If there is a template existing in the database for a particular fingerprint then it is compared with the input pattern of that particular fingerprint. The probability of the system to incorrectly match this comparison is false matching rate. Stated below is the formula for computation [109]:

$NIMS: Number\ of\ Imposter\ Matching\ Scores$

$NIRA: Number\ of\ Imposter\ Recognition\ Attempts$

$$FMR(t_1, t_2) = \frac{NIMS1 \leq t_1 \cap NIMS2 \leq t_2}{NIRA}$$

2. **Equal Error Rate:** When false match rate and false non match gives the same output that point is referred as equal error rate (EER) [109].

$$EER\ Value = FMR(i) = FNR(i)$$

$$Example: FMR = 0.3638\ and\ FNR = 0.3638\ then\ EER = 0.01$$

3. **Threshold Value:** We pre define some value to execute the experiment is called threshold. Whenever some results are computed that are compared with this pre defined value to check the performance of the system. If it does not match the condition then the result would be poor performance[109].

4. **False Acceptance Rate:** When we have some existing pattern in the database for a particular fingerprint then the input pattern is compared with that existing template. The probability of the system which fails to detect a match between these templates existing and input is the false acceptance rate. Its computation is done on the basis of Failure to Acquire Rate (FTA gives frequency of failing to acquire a biometric feature), Failure to Capture Rate (FTC gives the frequency of failing to capture a sample) and Failure to Extract Rate (FTX gives frequency of failing to extract a feature from sample) [109].

$$FTA = FTC + FTX\ (1 - FTC)$$

$$NIMS: Number\ of\ Imposter\ Matching\ Scores$$

$$NIRA: Number\ of\ Imposter\ Recognition\ Attempts$$

$$FMR(t_1, t_2) = \frac{NIMS1 \leq t_1\ \hat{}\ NIMS2 \leq t_2}{NIRA}$$

$$FAR = FMR\ (1 - FTA)$$

5. **False Reject Rate:** The input pattern is again compared with the existing template of that fingerprint. The probability of the system which fails to detect a match between both of these patterns is false reject rate. Its computation is done on the basis of Failure to

Acquire Rate (FTA gives frequency of failing to acquire a biometric feature), Failure to Capture Rate (FTC gives the frequency of failing to capture a sample) and Failure to Extract Rate (FTX gives frequency of failing to extract a feature from sample) [109].

$$FTA = FTC + FTX\ (1 - FTC)$$

$$NGMS: Number\ of\ Genuine\ Matching\ Scores$$

$$NGRA: Number\ of\ Genuine\ Recognition\ Attempts$$

$$FNR(t_1, t_2) = \frac{NGMS1 \geq t_1\ \cup NGMS2\ \geq\ t_2}{NGRA}$$

$$FRR = FTA + FNR\ (1 - FTA)$$

6. **False Non Match Rate:** The input pattern is compared with the existing template of the database and the probability of the system which fails to detect a match between these templates is the false non match rate [109].

$$NGMS: Number\ of\ Genuine\ Matching\ Scores$$

$$NGRA: Number\ of\ Genuine\ Recognition\ Attempts$$

$$FNR(t_1, t_2) = \frac{NGMS1 \geq t_1\ \cup NGMS2\ \geq\ t_2}{NGRA}$$

7. **Error Percentage:** The error percentage is also known as fractional difference. It is measured on the basis of experimental value stated as *E* in comparison to the true or accepted value stated as *A* [109]. Sometimes even the precision rate would also result in calculating the error percentage. Average of two extracted values is taken. So the formula for error percentage and difference between error percentage is:

$$Error\ \% = \frac{|E - A|}{A}$$

$$Difference\ \% = \frac{|E_1 -\ E_2|}{\left(\frac{E_1 +\ E_2}{2}\right)}$$

Any algorithm which could have values more appropriate and near to accuracy would be an ideal authentication algorithm. It developed the need to have a new fiingerprint hash algorithm which should have values of False Matching Rate and False Acceptance Rate as minimum and Equal Error Rate, Threshold Value, False Reject Rate, False Non Match Rate, Error Percentage as least. Overall performance is measured on the basis of conditions set for error percentage, average processing time and average matching time. In order to derive new fingerprint hash algorithm the conditions for performance evaluation should be fixed. Review of above stated algorithms in Section 2.7 on the basis of points of Section 2.8 is done and below stated are the conditions to be met by new fingerprint hash algorithm: Error Percentage should be less than 10, Average processing time should be less than 10 seconds and Average matching time should be less than 0.1 seconds.

2.9 NEED FOR VIRTUALIZATION OF MULTI SERVER ENVIRONMENT

After reviewing fingerprint algorithms it was decided that values would be extracted using fingerprint [110]. But then the question rose that how these values are to be stored? Generally values of all identity authentication parameters are stored in the database at the back end in Server [111]. But IP or Server spoofing could be implemented by intruders to falsify the information of the server [112]. But if multiple servers would be used then Server spoofing could not be implemented as only one IP address has to be used for spoofing the server [113][114]. Enhancement of security would be there if at the back end multi server environment could be created [115][116]. In order to have multi server environment SQL Server is needed at the back end and environment would be set with virtualization [117][118]. Steps for creating are [119]:

1. Connection is established with the Server after opening the First Instance of SQL SERVER.
2. Connection is established with the Server after opening Second Instance of SQL SERVER.
3. Connect First SQL Server Instance with Second SQL Server Instance.
4. Create Linked Server in First SQL SERVER Instance to Access the Databases of Second SQL SERVER Instance.
5. Press ok to save all the details.

6. Linked Server has been created in First SQL SERVER Instance. Do check in Server Objects of First Instance of SQL SERVER->Open Linked Server there you find your Linked Server name.

While storing the values of identity authentication parameters hash function would be used so that unauthorized access could not be done at the server. Example: Index finger first impression hash code value would be stored at Server 1 second impression hash code value would be stored at Server 2. When intruder would spoof Server 1 then the value stored at Server 2 is secure or vice versa [120]. So overall data stored using virtual multi server environment is secure in the public network.

2.10 SUBSTANTIATION OF AUGMENTED SECURITY AND PRIVACY

During review of literature it was found that augmentation of security and privacy is the main concern for all the users in the public network as it is the most insecure network. If fingerprint would be used as identity authentication parameter then extracted values would be stored with hash code in the database at the back end. In order to substantiate that stored value is true there is need to derive steps for augmentation.

For creating session between client and server login phase is required and fingerprint of the client would be extracted for completing the login phase. While extracting the fingerprint the reckoning of minutiae points are required because this would substantiate the augmentation of security and privacy of legitimate user. Total number of bifurcations and terminations are to be counted. More number of minutiae points matching with the extracted fingerprint will substantiate that it is a legitimate user. After deciding that there is need of deriving a new fingerprint hash algorithm the review resulted that this algorithm should result in reckoning the bifurcations and terminations. Then raised the question that what would be the application area for this new fingerprint hash algorithm or ideal authentication scheme?

2.11 APPLICABILITY OF IDEAL AUTHENTICATION SCHEME

The application areas of ideal authentication scheme are the main part of literature review. Applications would define the scope of new fingerprint hash algorithm. The main focus of ideal authentication scheme is to maintain confidentiality, integrity, authentication, availability and do the traffic analysis. The application areas are:

1. **Online Banking** – An identifier and password are required to access online banking facility. While username and password is entered by the legitimate user then server verifies the details from the verification table because the data initially is stored in the verification table by the server. While verification if it gets matched then access is given otherwise not. If fingerprint would be used either in place of password or assimilated with the password then security would be very strong. Fingerprint is the biological feature of the individual so unauthorized access is not possible.

2. **Student Attendance System** – Generally in schools, colleges, institutes and universities manual system is followed to take attendance of the student. In manual system possibility of proxy is highest and manipulations with the data could be easily done. So to make the attendance system more secure biometric attendance system should be followed. Machine could be placed at the entrance of the classroom and all students would be asked to mark attendance through biometric machine. This will ensure the security of the student and no manipulations could be done.

3. **Library Management System** - In most of the libraries the manual system for issuing and receiving the books is followed but in few libraries automated system is followed. In this automated system the software for library management is installed on the computer and through bar code the books are being issued. The identity card of the student is used for authentication. But there is a possibility that identity card of the students gets stolen or lost so in that case any malicious user can access the library. So in order to identify the legitimate user fingerprint identity authentication parameter should be used. This will ensure the security of the student and no manipulations could be done.

4. **Fortification of transport layer security protocol** – All the transactions which are done online e.g e-commerce, e-banking, e-shopping needs complete security. All these transactions are done at the transport layer of the International Standard Organization – Open System Interconnection model. This layer is responsible for creating a session between client and server. For this session mutual authentication is required which means client should authenticate that server is legitimate and vice versa. In order to fortify the transport layer security fingerprint would be used for session creating or login. Whenever any malicious user would try to intrude then because of multi server

environment used at the back end it would be detected. So only legitimate user can create sessions at the transport layer.

2.12 MATLAB AND ITS FEATURES

'Matlab' name comes from two words: matrix and laboratory. MathWorks (producer of Matlab), defines it as technical computing language. It is mostly used for high-performance numeric calculations and visualization [121]. MATLAB is very easy to use environment which has integration of computing, programming, signal processing and graphics. In this environment the problems and solutions both are expressed by using mathematical notation. Complex mathematical problems could be easily solved in this environment [122]. MATLAB is also used for analyzing data, modeling and simulation and making statistical representation. It has its various implementation areas like:

- biology,
- chemistry,
- economics,
- medicine, etc.

The main features of MATLAB are: extensibility (new applications could be created), toolboxes (Desktop Tools and function library), high-level array language (arrays, structures, unions), graphics (image processing, visualization) and external interfaces (coding in other languages could be done) [123] [124].

MATLAB has image processing toolbox function which is used for processing the images. GUI is defined as a set of techniques and mechanisms which are used between program and user to create an interactive communication [125]. It gives a pleasant working environment to the user with best possible combinations of colors and alignments. GUI should be simple and easily understandable by an average programmer [126]. Every function, button or any other object should be clearly defined and should have its meaning [127]. Good interface is quiet simple; it limits the number of functions or actions.

Complete review of literature resulted to identify the research gaps present in the review. The thesis focus would be to fill these research gaps.

3

Identification of Research Gaps based on Literature Review

CHAPTER – 3

IDENTIFICATION OF RESEARCH GAPS BASED ON LITERATURE REVIEW

After review of the literature it is found that to substantiate the augmented security in the public network there is need to derive an ideal authentication scheme. The thesis proposes a new fingerprint hash algorithm to be used as an ideal authentication scheme in a public network. The following work flow is adopted in the thesis to identify the research gaps based on review:

3.1 Analysis of Survey in which it is decided that which is the most acceptable identity authentication parameter for the user.

3.2 Comparison of existing password authentication schemes and to analyze which of the scheme could be best suitable for most acceptable identity authentication parameter. The comparison of the schemes should be done on the basis of attacks and security requirements to which they are vulnerable or could withstand. It should be found out that how many attacks and security requirements are possible on each authentication scheme and if some change in its usage is done, does it affect the attacks and security requirements?

3.3 Comparison of technologies and techniques for fingerprint so that the problems of the conventional systems could help in generating and ideal technology or algorithm for fingerprint.

3.4 Comparison of fingerprint algorithms on the basis of performance indicators False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage. This analysis would derive a result that which of the conventional system followed till date has problems and which are the best. It will also generate a possibility of deriving new algorithms which would overcome the problems of conventional systems.

3.5 Deriving new ideal authentication scheme which should have most acceptable identity authentication parameter used in it and should overcome the problems of conventional systems and should substantiate augmented security.

3.1 ANALYSIS OF SURVEY

The analysis of the responses to the questionnaire discussed in review of literature on the basis of Choice of the user on the basis of acceptability, gender and age is done and following are the details [40]:

i. Generally users use Password as the most common and accepted authentication method for handling their online transactions.

ii. While handling the online transactions security is the most concerning challenges.

iii. During online transactions Passwords and Tokens have medium security. So user needs new identity authentication parameter which enhances security.

iv. During online transactions users perceive usability of passwords and tokens at medium level. So user needs new identity authentication parameter which enhances security.

v. Future preferences of users would be fingerprint as authentication parameter for online transactions. It substantiates augmented security in the public network.

vi. When fingerprint is the authentication type then security and privacy would be at highest level. So fingerprint would be either assimilated with the password for adding one more tier of security at the transport layer or could be used alone for fortifying security. For complete security fingerprint should be used as an authentication parameter.

vii. Majority of the users expect user, server authentication and security from intruders for secure transactions while using online mode either for e-banking, e-purchasing or e-communication etc. If user and server authenticate each other then mutual authentication would be done. Mutual authentication implemented

with fingerprint will surely enhance security while creating session between client and server. It will result in security from intruders at the transport layer.

viii. The possibility of acceptance of data being completely secure is highest if fingerprint is used as the authentication parameter in online transactions. The assimilation of fingerprint with passwords would add one more tier of security in the online transactions. This assimilation would result in fortification of the transport layer. But if fingerprint is implemented alone as identity authentication parameter then unauthorized access would never be done and it will enhance security.

ix. Some additional cost could be there if one more tier for enhancing security is added, so users possibility of acceptance to bear that nominal cost would be at medium level. Majority users agree to bear the nominal cost if included for augmented security.

x. The prototype which either have assimilation of password and fingerprint or fingerprint alone would result in complete security for e-banking, e-purchasing or e-communication etc then the possibility of user's willingness to purchase that is at maximum. Users accept to bear additional cost for having complete security in online transactions.

Overall analysis of Survey is that users generally use passwords for online transactions and it is the most acceptable identity authentication parameter but passwords are vulnerable to attacks and could not withstand all security requirements. So for complete security users are accepting fingerprint as an ideal identity authentication parameter because it withstands most of the security requirements. Mutual authentication between client and server could be implemented well with fingerprint. Even assimilation of fingerprint with password could be used for augmented security. So fingerprint will be an Ideal Authentication Parameter. Users are even ready to bear additional nominal cost over the prototype which should result in enhanced security. User and Server authentication which is mutual authentication along with security from intruders is required by all the users and it is possible with fingerprints.

3.2 COMPARISON OF EXISTING PASSWORD AUTHENTICATION SCHEMES

These existing password authentication schemes use either password or smart card for proving the user's identity over the network for security but from the below said table it is very well verified that these schemes are vulnerable to smart card loss attack and could not withstand mutual authentication security requirements [34].

Table 1 : Comparative Analysis of Existing Password Authentication Schemes

RSA Based Scheme = R ElGamal Based Scheme = EL Hash Based Scheme = H

Y: Supported N: Not Supported

S.No	Attacks and Security Requirements	R	EL	H
Attacks				
1	Denial of Service Attack	Y	Y	Y
2	DNS Poisoning	Y	Y	Y
3	Forgery Attack	Y	Y	Y
4	Man in the Middle Attack	Y	Y	Y
5	Ping of Death	Y	Y	Y
6	IP Spoofing	Y	Y	Y
7	Parallel Session Attack	Y	Y	Y
8	Ping Broadcast	Y	Y	Y
9	Password Guessing Attack	Y	Y	Y
10	Server Spoofing	Y	Y	Y
11	Replay Attack	Y	Y	Y
12	Session Hijacking	Y	Y	Y
13	Smart Card Loss Attack	Y	Y	N
14	Smurf Attack	Y	Y	Y
15	Stolen Verifier Attack	Y	Y	Y
16	Teardrop Attack	Y	Y	Y
Security Requirements				
1	Forward Secrecy	Y	Y	Y
2	Mutual Authentication	N	N	Y
3	Confidentiality	Y	Y	Y
4	Integrity	Y	Y	Y
5	Availability	Y	Y	Y

For complete security the authentication scheme should withstand all security requirements including mutual authentication [35]. Comparative analysis proves that Hash based scheme withstands all security requirements, it is vulnerable to smart card loss attack only so it can be an ideal authentication scheme if any ideal authentication parameter could be used with this scheme [37]. Comparative analysis of all the existing password authentication schemes with the security requirements and attacks which it could not satisfy and is vulnerable to is in the above mentioned table (*Table 1*) [50].

Research Gap 1: Data is completely secure if fingerprint is used as the authentication parameter in public insecure network. From Survey it is proved that fingerprint could be an ideal authentication parameter so implementation of fingerprint with hash based scheme would substantiate augmented security. To get enhanced security fingerprint could be assimilated with passwords or used alone. It would add one more tier of security in the online transactions on the network. The only gap remains is mutual authentication when fingerprint is used as identity authentication parameter with new algorithm using hash based scheme.

Comparative analysis of password alone with assimilated fingerprint algorithms is done and number of possible attacks is found out [128]. The comparative analysis on the basis of security requirements and attacks which it could not satisfy and is vulnerable to is in the below mentioned table (*Table 2*) [128]:

The comparison in Table 2 states that denial of service is possible with *p, f(g), f(a)* and *f(m),* DNS poisoning is possible with *p* but not with *f(g), f(a) and f(m),* forgery attack is possible with *p, f(g), f(a)* and *f(m),* man in the middle attack is possible with *p, f(g), f(a)* and *f(m),* ping of death is possible with *p, f(g), f(a)* and *f(m),* IP spoofing is possible with *p, f(g), f(a)* and *f(m),* parallel session is possible with *p, f(g), f(a)* and *f(m),* ping broadcast is possible with *p, f(g), f(a)* and *f(m),* password guessing is possible with *p* but not with *f(g), f(a) and f(m),* server spoofing is possible with *p, f(g), f(a)* and *f(m),* replay is possible with *p, f(g), f(a)* and *f(m),* session hijacking is possible with *p, f(g), f(a)* and *f(m),* smart card loss is possible with *p, f(g), f(a)* and *f(m),* smurf is possible with *p, f(g), f(a)* and *f(m),* stolen verifier is possible with *p, f(g), f(a)* and *f(m)* and tear drop is possible with *p, f(g), f(a)* and *f(m).*

Table 2: Comparative study of attacks and security requirements with assimilation of fingerprint with password

Y: Supported **N: Not Supported**

S.No	Attacks and Security Requirements	*p*	*f(g)*	*f(a)*	*f(m)*
	Attacks	**Pass-word**	**Fingerprint with grid hash algorithm**	**Fingerprint with angle hash algorithm**	**Fingerprint with minimum distance hash algorithm**
1	Denial of Service Attack	Y	Y	Y	Y
2	DNS Poisoning	Y	N	N	N
3	Forgery Attack	Y	Y	Y	Y
4	Man in the Middle Attack	Y	Y	Y	Y
5	Ping of Death	Y	Y	Y	Y
6	IP Spoofing	Y	Y	Y	Y
7	Parallel Session Attack	Y	Y	Y	Y
8	Ping Broadcast	Y	Y	Y	Y
9	Password Guessing Attack	Y	N	N	N
10	Server Spoofing	Y	Y	Y	Y
11	Replay Attack	Y	Y	Y	Y
12	Session Hijacking	Y	Y	Y	Y
13	Smart Card Loss Attack	N	N	N	N
14	Smurf Attack	Y	Y	Y	Y
15	Stolen Verifier Attack	Y	Y	Y	Y
16	Teardrop Attack	Y	Y	Y	Y
	Total Number of Attacks	15	13	13	13
	Security Requirements				
1	Forward Secrecy	Y	Y	N	Y
2	Mutual Authentication	**N**	**Y**	**Y**	**Y**
3	Confidentiality	Y	Y	Y	Y
4	Integrity	Y	Y	Y	Y
5	Availability	Y	Y	Y	Y
	Total Number of Security requirements	4	5	4	5

Research Gap 2: If fingerprint is implemented alone as identity authentication parameter then the possibility of reduction in attacks is maximum. The gap in research is the need to generate a new fingerprint hash algorithm which has reduction in error percentage. This algorithm could be assimilated with password for fortifying security or could be used with fingerprint alone.

This originated need to compare technologies and techniques used for fingerprint. The problems of existing fingerprint technologies and techniques would help in deriving an ideal algorithm with fingerprint.

3.3 COMPARISON OF TECHNOLOGIES AND TECHNIQUES FOR FINGERPRINT

This section of the thesis focuses upon all the technologies and techniques used for fingerprint. Benefits of the methodology and problems associated are discussed in details. Below mentioned table does the complete analysis:

Table 3: Comparative study of technologies and techniques for Fingerprint

S.No	Technologies and Techniques for Fingerprint	Benefits of Methodology	Problems
1	Singularity Detection [51]	Automatic extraction and matching of minutiae points of the fingerprint	Noisy data in the image will hinder the performance of the extraction of minutiae
2	Edge Detection [52]	With feature synthesis the responses from smaller operators are used to predict the larger operator responses	Large responses if computed by biometric machines it takes time
3	Graph Matching [53] [54]	Results in less rotation, noise and distortion of fingerprint	With manual computation ridge breaks are surely ignored and even sometimes in the computerized system

S.No	Technologies and Techniques for Fingerprint	Benefits of Methodology	Problems
4	Directional Image [55]	For segmentation of the original image the directional image is used	Performance deteriorates when implemented on gray scale level image
5	Filter Design [56]	Noise is reduced from boundaries and background of the fingerprint images	Can't detect frames of reference and problems are there with storage cost, additional processing, robustness due to multiple representations
6	Structural Matching [57]	Considering the features which are extracted from the fingerprint it is based on the local structural relations	Distortions were not completely addressed because of less speed
7	Localized Spatial Filters [58]	Modulates by 2-D Gaussian functions, orientation bandwidths and spatial frequency	It needs sampling and quantization due to the discrete frequencies of the filters
8	Texture Analysis and Optical Flow [59]	Local neighbourhoods need orientation and it used least square sense	Without Fourier transformation the computation is performed for spatial domain and the problem remains with Eigen value
9	Gabor Filters [60]	It covers spatial frequency domain and multichannels	Texture discrimination is performed by a human but not always.
10	Genetic Algorithm [61]	Searching is performed on complete set and optimization problems are solved	Takes too much time in optimizing the standard deviation of fingerprint ridge frequency
11	Directional Fourier Filtering [62]	It is done with 2-D fast Fourier transform (FFT) and was effective on all modern image processing systems of that period	During extraction the thresholding stage is required for enhancement

S.No	Technologies and Techniques for Fingerprint	Benefits of Methodology	Problems
12	Non Linear Dynamical System [63] [64]	It is called M-lattice system in which restoration and halftoning for scanned fingerprint images is done simultaneously	Due to large signal boundedness and efficiency of enhancing fingerprint image it is only used for engineering applications
13	Adaptive Flow Orientation [65] [66] [67]	Reliable method for extracting structural features from the fingerprint images	For performance evaluation manual comparison is done for computing Goodness index
14	Gray Scale Minutiae Detection [68]	Used for extracting two ridges intersection which are minutiae and its conversion into gray scale	Problem lies with extraction of false minutiae points from the fingerprint
15	Multimodal Biometric System [69] [70]	It was used to integrate multiple biometrics at the decision making level and human recognition on the basis of fingerprint/ face recognition/ speech	Too much of efficiency is required to analyze the anatomical variation by nature amongst the human beings
16	Smart Cards [71] [72] [73]	Useful with three phase authentication which are registration, login and verification.	Instead of timestamps random numbers are used for registration
17	Cryptographic Key Generation [74]	Strong cryptographic key based is used rather than password and framework generates stable bitstream	System consumes too much of time for bitstreaming
18	Fuzzy Extractors [75]	It tolerates error because the data is uniformly random and could be used as a key for cryptographic applications	Very less percentage of error is tolerated by this uniformly random data
19	Onion Layer Algorithm [76] [77] [78]	The fingerprint matching and verification is performed by nested convex polygon of minutiae points	For searching or matching large/complex databases are split into smaller parts and their computation more time is taken

S.No	Technologies and Techniques for Fingerprint	Benefits of Methodology	Problems
20	Single Hamming Distance Matcher [79]	It is less costly during implementation and is faster multimodal biometric identification system	Unimodal system was already available but it utilized a single hamming distance matcher for verification of fingerprint and iris fusion system
21	Local Alignment [80]	Could also be used to match deformed fingerprint and even non linear distortions over the fingerprint	To count the number of matched minutiae tight thresholds are used
22	Hierarchical Filtering [81] [82]	It is fast and quiet accurate and comparable to conventional methods	Any fingerprint could only be used for searching if it is first generated with long structural information and low collision

Research Gap 3: The problems of existing technologies and techniques substantiated that there is need to derive a new fingerprint hash based algorithm by overcoming the drawbacks of the existing algorithms and diminution in error approximation.

This originated need to analyze existing fingerprint algorithms based upon False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage. This comparison would help in finalizing the parameters required for deriving a new fingerprint hash algorithm and would substantiate augmented security with it.

3.4 COMPARISON OF FINGERPRINT ALGORITHMS

The comparison of existing fingerprint algorithms is done on the basis of False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage performance indicators [49]. The algorithms compared on the basis of performance indicators are Phase Based Image Matching [83] [84] [85] [86], Feature Based Matching [86] [87], Standardized Fingerprint Recognition Model [88] [89] [90], Cluster Fingerprint Recognition [91] [92], Fuzzy Vault Scheme Based Fingerprint Recognition [75] [93], Genetic Algorithm for Fingerprint Matching

[94], Minutiae Based Matching [86] [95] [96], Orientation Estimation Algorithm for Fingerprint [97] [98] [99], Novel Algorithm for Detecting Singular Points from Fingerprint Images [100] [101], Fingerprint Enhancement [99] [102] [103] [104] [105] [106], Grid Hash Fingerprint Recognition [43] [107], Angle Hash Fingerprint Recognition [43] [108] and Minimum Distance Hash Fingerprint Recognition Algorithm [43] [107] [108] explained in Section 2.7 of Chapter 2. The values derived may vary on the basis of environment set for experiments. The symbol of # used in the table states that values are not derived in the experiment of that paper. So table comprises of computed values in the stated references. The values for the performance indicators are:

Table 4: Comparison of existing fingerprint algorithms

S.No	***Algorithms***	***fmr***	***eer***	***fnr***	***far***	***frr***	***thv***	***epr***
1	Phase based fingerprint algorithm [83] [84] [85] [86]	#	0.0118	#	#	#	#	1.18
2	Feature based fingerprint algorithm [86] [87]	#	0.0094	#	#	#	0.046	0.94
3	Standardized fingerprint recognition model[88] [89] [90]	3.57	#	5	3.57	5	#	#
4	Fuzzy vault scheme based fingerprint recognition[75] [93]	0.5	#	26.4	0.5	26.4	#	#
5	Genetic algorithm for fingerprint matching [94]	10	#	15	10	15	#	#
6	Minutiae based fingerprint algorithm [86] [95] [96]	#	0.0481	#	#	#	#	4.81
7	Fingerprint enhancement [99] [102] [103] [104] [105] [106]	#	0.202	#	#	#	#	20.2
8	Grid hash algorithm[43] [107]	1.52	#	18.32	1.52	18.32	#	#
9	Angle hash algorithm[43] [108]	1.23	#	14.61	1.23	14.61	#	#
10	Minimum distance hash algorithm [43] [107] [108]	1.87	#	20.32	1.87	20.32	#	#

As per the detailed literature review in Chapter 2 of the thesis of all the algorithms complete comparative analysis on the basis of False Matching Rate = *fmr*, Equal Error Rate = *eer*, Threshold Value = *thv*, False Acceptance Rate = *far*, False Reject Rate = *frr*, False Non Match Rate = *fnr* and Error Percentage = *epr* performance indicators is done. Explanation of all performance indicators is given below graphically but overall this comparison substantiates the below mentioned gaps/points:

Research Gap 4: Phase Based Image Matching and Feature Based Matching are least in error percentage but the reviewed paper has combination of both the algorithms [83] [84] [85] [86] [87].Minutiae Based Matching Algorithm is the second least in error percentage [86] [95] [96]. The research gap is that new fingerprint hash algorithm should have error percentage either better than these or less than 10.

Graphical representation of each performance indicator is given below which substantiates this point and sets an environment to meet the above stated conditions.

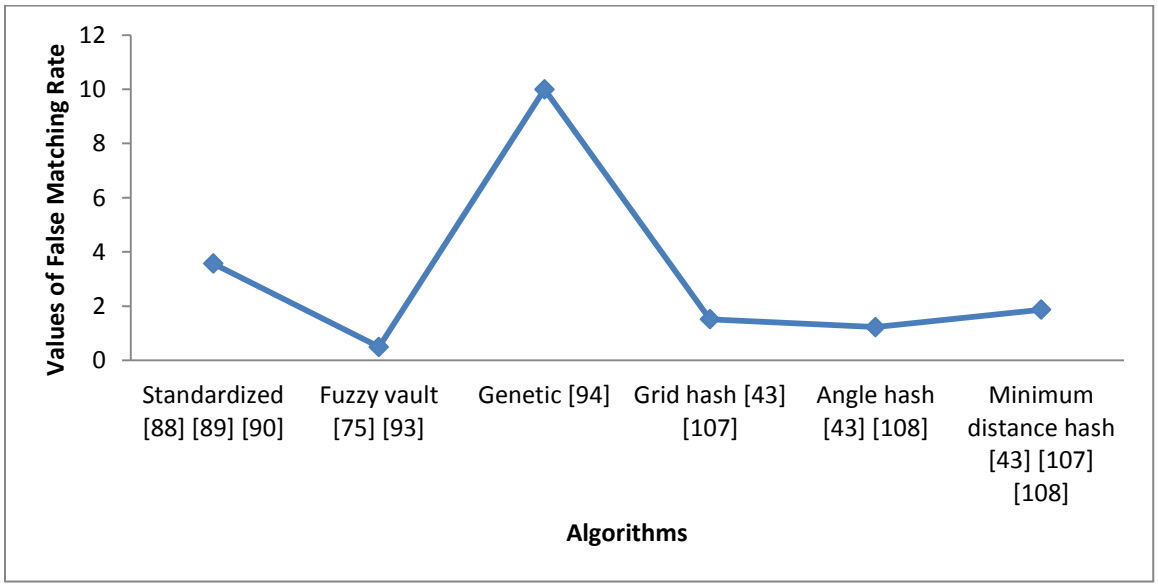

Figure 19: False Matching Rate

Performance indicator is explained in Section 2.8 of Chapter 2. After complete experimentation using all algorithms following are the approximate calculated values for False Matching Rate *(fmr)*: [88] [89] [90] = 3.57, [75] [93] = 0.5, [94] = 10, [43] [107] = 1.52, [43] [108] = 1.23, [43] [107] [108] = 1.87.

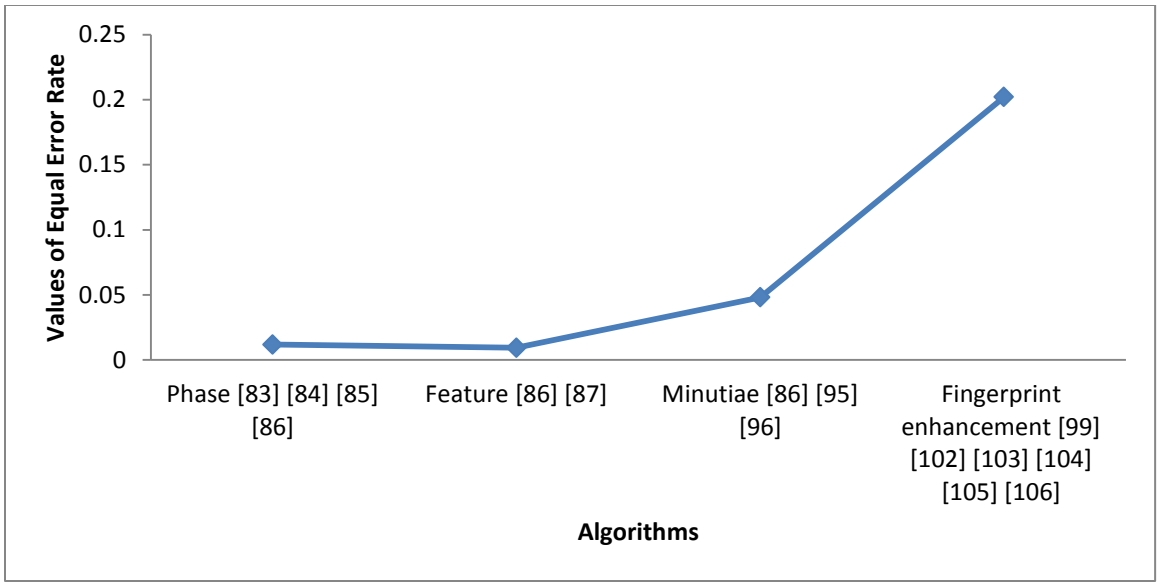

Figure 20: Equal Error Rate

After complete experimentation using all algorithms following are the approximate calculated values for Equal Error Rate *(eer)*: [83] [84] [85] [86] = 0.0118, [86] [87] = 0.0094, [86] [95] [96] = 0.0481 and [99] [102] [103] [104] [105] [106] = 0.202.

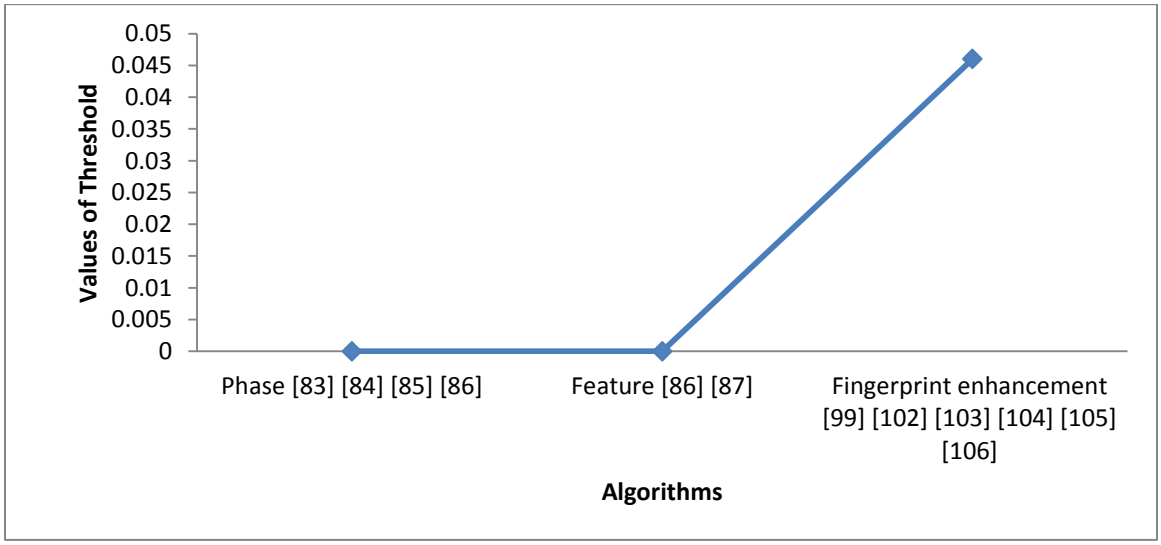

Figure 21: Threshold Value

After complete experimentation using all algorithms following are the approximate calculated values for Threshold Value *(thv)*: [83] [84] [85] [86] = 0, [86] [87] = 0.046, [86] [95] [96] = 0 and [99] [102] [103] [104] [105] [106] = 0.

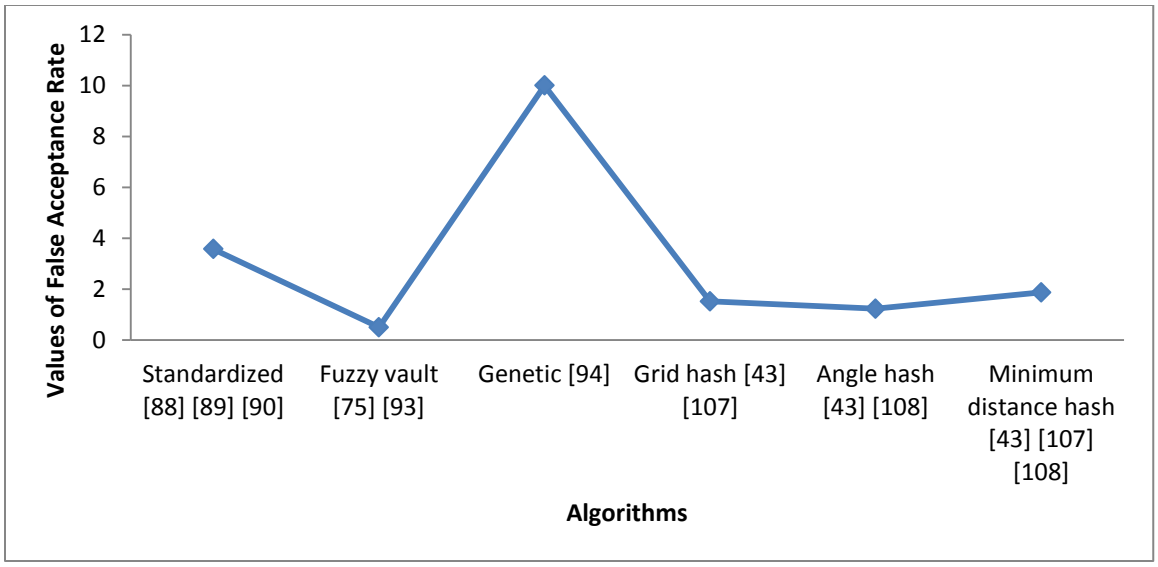

Figure 22: False Acceptance Rate

After complete experimentation using all algorithms following are the approximate calculated values for False Acceptance Rate *(far)*: [88] [89] [90] = 3.57, [75] [93] = 0.5, [94] = 10, [43] [107] = 1.52, [43] [108] = 1.23, [43] [107] [108] = 1.87.

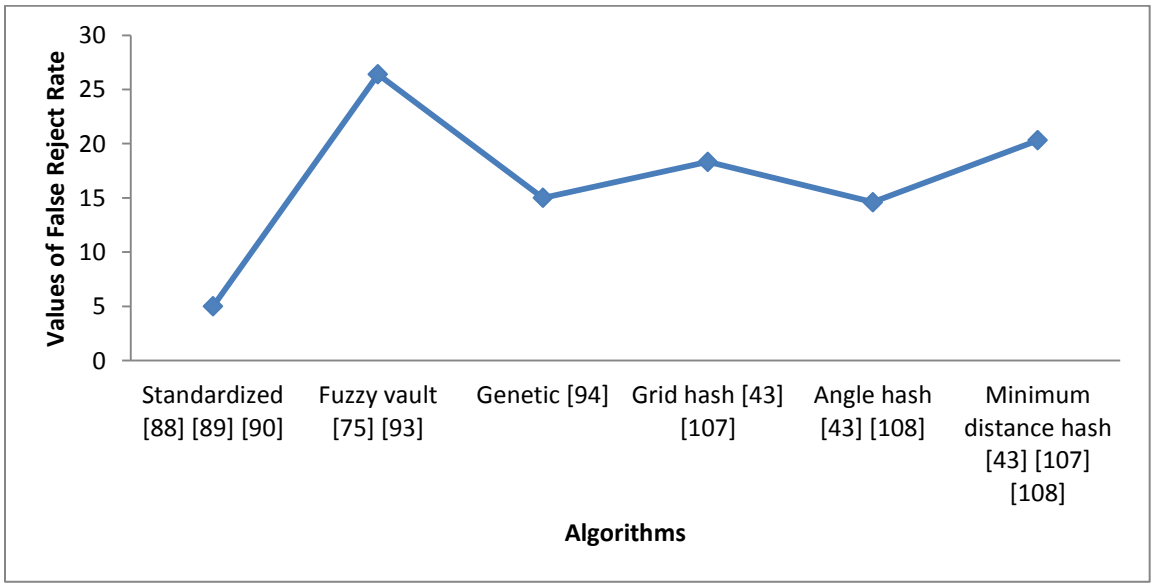

Figure 23: False Reject Rate

After complete experimentation using all algorithms following are the approximate calculated values for False Reject Rate *(frr)*: [88] [89] [90] = 5, [75] [93] = 26.4, [94] = 15, [43] [107] = 18.32, [43] [108] = 14.61, [43] [107] [108] = 20.32.

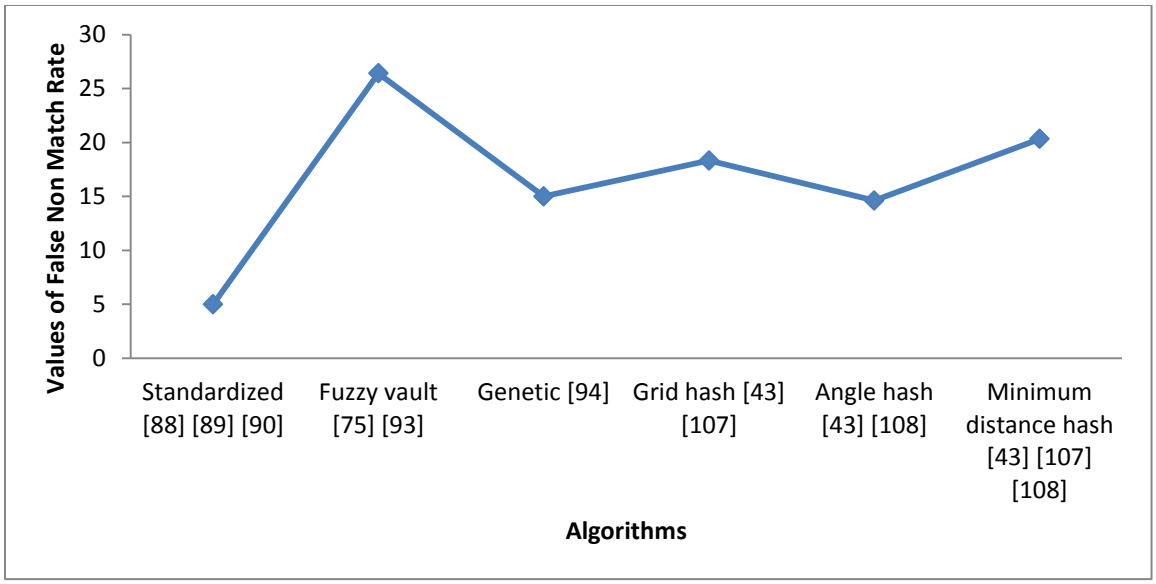

Figure 24: False Non Match Rate

After complete experimentation using all algorithms following are the approximate calculated values for False Non Match Rate *(fnr)*: [88] [89] [90] = 5, [75] [93] = 26.4, [94] = 15, [43] [107] = 18.32, [43] [108] = 14.61, [43] [107] [108] = 20.32.

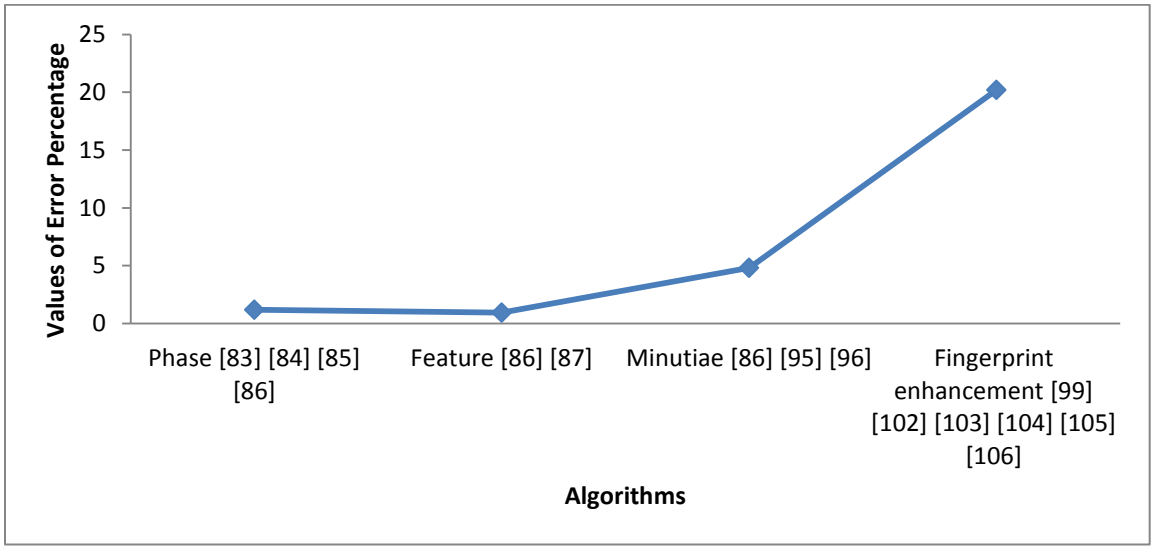

Figure 25: Error Percentage

After complete experimentation using all algorithms following are the approximate calculated values for Error Percentage *(epr)*: [83] [84] [85] [86] = 1.18, [86] [87] = 0.94, [86] [95] [96] = 4.81 and [99] [102] [103] [104] [105] [106] = 20.2.

All performance indicators state that results substantiates that Phase Based Image Matching and Feature Based Matching are least in error percentage but the reviewed paper has combination of both the algorithms [83] [84] [85] [86] [87]. Minutiae Based Matching Algorithm is the second least in error percentage [86] [95] [96].

Table 5 : Result of best algorithms

S.No	*Algorithms*	*eer*	*thv*	*epr*
1	Phase based fingerprint algorithm [83] [84] [85] [86]	0.0118	#	1.18
2	Feature based fingerprint algorithm [86] [87]	0.0094	0.046	0.94
3	Minutiae based fingerprint algorithm [86] [95] [96]	0.0481	#	4.81
4	Orientation estimation algorithm for fingerprint [97] [98] [99]	*Average Processing Time is 16*		
5	Novel algorithm for detecting singular points from fingerprint images [100] [101]	*Average Processing Time as 3.14*		

Research Gap 5: Orientation Estimation Algorithm for Fingerprint and Novel Algorithm for Detecting Singular Points from Fingerprint Images have minimum average processing time as 16 and 3.14 respectively [97] [98] [99] [100] [101]. Overall accuracy of Orientation Estimation Algorithm for Fingerprint is 98% [97] [98] [99]. So the new fingerprint hash algorithm should have either greater or equal to accuracy percentage than Orientation Estimation Algorithm for Fingerprint. The research gap is that the new fingerprint hash algorithm should have average processing time less than 10 seconds.

Research Gap 6: The research gap is that the new fingerprint hash algorithm should have average matching time as less than 0.1 seconds.

It states that new fingerprint hash algorithm should be best upon the parameters like Equal Error Rate, Threshold Value, False Reject Rate, False Non Match Rate and Error Percentage. Moreover new algorithm should have more accuracy percentage than existing and should fill all the research gaps as mentioned in Table 6 Section 3.5.

3.5 RESEARCH GAPS

This chapter of the thesis identifies the research gaps based on the complete literature review done in the Chapter 2. Following table consolidates the research gaps:

Table 6 : Research Gaps

S.No	*Analysis of Literature Review*	*Research Gap*
1	Table 1	Mutual authentication required when fingerprint is used as identity authentication parameter with new algorithm using hash based scheme
2	Table 2	Need to generate a new fingerprint hash algorithm with reduction in error percentage
3	Table 3	Need to derive a new fingerprint hash based algorithm by overcoming the drawbacks of the existing algorithms and diminution in error approximation
4	Table 4	New fingerprint hash algorithm should have error percentage less than 10
5	Table 5	New fingerprint hash algorithm should have average processing time less than 10 seconds
6	Table 5	New fingerprint hash algorithm should have average matching time as less than 0.1 seconds

These research gaps as per Table 6 are filled in the later chapters of the thesis.

3.6 DERIVING NEW IDEAL AUTHENTICATION SCHEME

Ideal authentication scheme signifies that it should have most acceptable identity authentication parameter used in it and should overcome the problems of conventional systems and should substantiate augmented security. Following steps are used to derive new ideal authentication scheme:

1. From section 3.1 of the thesis it is derived that fingerprint is an ideal authentication parameter and should be used for identity authentication. So fingerprint would be used in ideal authentication scheme.

2. From section 3.2 it is proved that hash based scheme is best for enhanced security because it withstands mutual authentication. So fingerprint should be used with hash based scheme. But if assimilation of fingerprint is done with password which is most acceptable existing identity authentication parameter then it could not withstand all required security requirements. Depending upon the comparative analysis the possibility of attacks and security requirements by the intruders is 90.47% with only password, 85.71% when password is assimilated with grid hash fingerprint algorithm, 80.95% when password is assimilated with angle hash fingerprint algorithm and 85.71% when password is assimilated with minimum distance hash fingerprint algorithm. So new fingerprint hash based algorithm should have less percentage and possibility of attacks as compared to these.

3. From section 3.3 the benefits and problems associated with the existing technologies and techniques for fingerprint and compared and it is found that new fingerprint hash algorithm should be capable to overcome the drawbacks of these existing algorithms and techniques and diminution in error approximation.

4. From section 3.4 all the fingerprint algorithms are compared and parameters required for new fingerprint hash algorithm are finalized. Parameters finalized are False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage. New fingerprint hash algorithm should give best results on the basis of these parameters. Comparison resulted that Phase Based Image Matching and Feature Based Matching are least in error percentage but the reviewed paper has combination of both the algorithms [83] [84] [85] [86] [87]. Minutiae Based Matching Algorithm is the second least in error percentage [86] [95] [96]. Orientation Estimation Algorithm for Fingerprint and Novel Algorithm for Detecting Singular Points from Fingerprint Images have minimum average processing time as 16 and 3.14 respectively [97] [98] [99] [100] [101]. Overall accuracy of Orientation Estimation Algorithm for Fingerprint is 98% [97] [98] [99]. This analysis resulted that new fingerprint hash algorithm should result in more accuracy than these best

algorithms existing. Moreover new algorithm should have more recognition accuracy percentage and acceptable distortion tolerance than existing and should satisfy the conditions stated below:

- Error Percentage < 10
- Average Processing Time < 10 seconds
- Average Matching Time < 0.1 second.

This fingerprint hash algorithm would be an ideal authentication algorithm used with ideal authentication scheme.

5. From section 3.5 all research gaps are identified after complete literature review done in Chapter 2.

So from this identification of research gaps it is derived that there is need of new fingerprint hash algorithm which should use hash as authentication scheme and should give maximum accuracy and should perform best in False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage.

4

New Fingerprint Hash Algorithm (RNA-FINNT)

CHAPTER – 4

NEW FINGERPRINT HASH ALGORITHM: RNA-FINNT

The identification of gaps from Chapter 3 resulted in generating a new fingerprint algorithm which should have hash based scheme used in it, should have very less percentage of error, percentage of accuracy should be more and should result good for the set performance indicators. The work in the thesis has derived a new fingerprint hash algorithm named as RNA-FINNT (Reduced Number of Angles Fingerprint Hash Algorithm) [49].

4.1 HASHED FINGERPRINT IDENTITY PARAMETER WITH RNA-FINNT

This algorithm uses fingerprint as identity authentication parameter and scheme used is hash based. Table 1 of Chapter 3 states that hash based scheme cannot withstand smart card loss attack so that is why fingerprint is used as identity authentication parameter. The hash based scheme is not vulnerable to mentioned attacks in Chapter 2 Section 2.1.1 and can't withstand all the security requirements mentioned in Chapter 2 Section 2.1.2 [50]. So hash based scheme is an ideal authentication scheme and RNA-FINNT uses hash based scheme. In Chapter 2 Section 2.5 the assimilation of fingerprint with password was reviewed but as per Table 2 of Chapter 3 this methodology was not successful [50]. When password is assimilated with grid hash fingerprint algorithm then it is vulnerable to 15 attacks out of 18 in total stated [128]. When password is assimilated with angle hash fingerprint algorithm then it is vulnerable to 14 attacks out of 18 in total stated [128]. When password is assimilated with minimum distance hash fingerprint algorithm then it is vulnerable to 15 attacks out of 18 in total stated [128]. So Chapter 3 proved that either fingerprint should be used alone as identity authentication parameter or password should be assimilated with RNA-FINNT algorithm. RNA-FINNT would execute in following manner [49]:

RNA – FINNT: Reduced Number of Angles Fingerprint Hash Algorithm

- Take fingerprint through sensor
- Divide fingerprint into grid of squares
- Count the number of minutiae points (M) in each square
- If the number of M < = 2 then the same value would be converted into hash code and would be stored in the matrix
- But if M>2 then by picking one M at random angle calculation would be done
- The output would be stored as a matrix which would have different values for each square of the grid
- Either the square of the grid would have minutiae count as hash code value or the angle of the M would be hash code.
- Overall the stored value would be

$$(\alpha_1, A_1, \alpha_2, A_2, \alpha_3, \text{----------}, A_m, \alpha_n)$$

Explanation of RNA-FINNT

i. For the very first time the fingerprint of the user would be taken by the Sensor (*Figure 26*).

ii. The fingerprint would be divided into possible number of grid of squares and the number of minutiae points (M) in each square would be counted (*Figure 27*).

Figure 26: Scanned Image

Figure 27: Fingerprint divided into Grid of Squares

iii. If the number of M < = 2 then the same value would be converted into hash code and would be stored in the matrix (*Figure 28*).

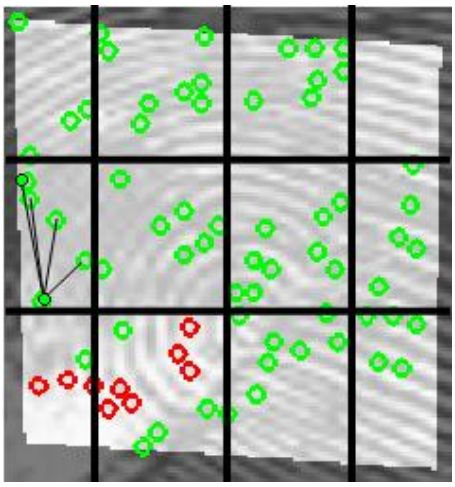

Figure 28: Extraction of Terminations and Bifurcations

iv. But if M>2 then by picking M at random the angle values would be computed. Global feature core or delta would not be included in this computation rather one of the M would act as central point and connection between all the M in specific square of the grid would be generated.

v. Slope of line would be calculated and formula of angle calculation would be used. Line would be generated between M. One of the M would be (*cx, cy)* and the second M would be *(dx, dy)*. Position of the *M* would be *(x,y)*. Now if it is the *ith* M, then position of the point would be *(xi,yi)*.

Formula for calculating slope of the line is:

$$M1 = y1 - cy / x1 - cx \qquad M2 = y1 - dy / x1 - dx$$

Further calculate the angle for this with the use of following formula:

$$\alpha = tan^{-1} M1 - M2 / 1 + M1.M2$$

And the calculated angle would be converted into hash code and stored in the matrix:

$$(\alpha_1, \alpha_2, \alpha_3, \text{----------}, \alpha_n)$$

And the output of the angles would be stored in the matrix which would be the hash code.

vi. So RNA-FINNT would give output as a matrix which would comprise of different values for each square of the grid. Either the square of the grid would have minutiae count as hash code value or the angle of the M would be hash code.

vii. And moreover all the squares of the grid would execute in parallel which would help in rapid execution.

viii. Overall the stored value would be

$(\alpha_1, A_1, \alpha_2, A_2, \alpha_3, \text{----------}, A_m, \alpha_n)$

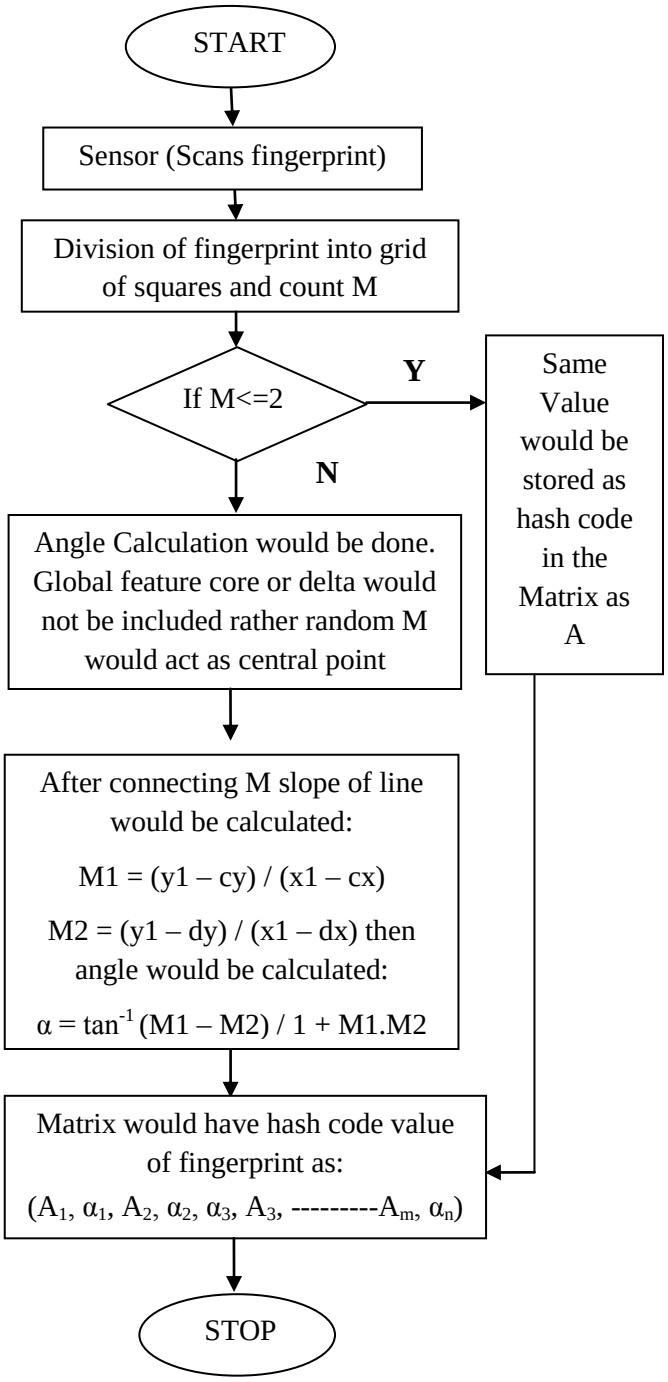

Figure 29: Execution Flowchart of RNA-FINNT

Virtualization in the multi server environment mentioned in Chapter 2 Section 2.9 gives details for implementation of mutual authentication and generating RNA-FINNT resulted in filling of the research gap 1. RNA-FINNT implemented for mutual authentication is possible through multi server environment for enhanced security.

4.2 RNA-FINNT ALGORITHM FINGERPRINT MATCH

There may be a possibility that when authenticity is to be proved then fingerprint could not match because every time client could not place the finger at the same location and in the same way. So when RNA-FINNT would execute it would definitely generate a different hash code value every time. For this the thesis proposes following processes amongst which one would be followed for fingerprint matching so that authenticity process could be enhanced:

I. **Linear Symmetric Hash Function:** This function would be executed on the basis of following mentioned steps and would result in enhanced authenticity.

1. Initial hash value of fingerprint is already stored at the server.
2. For fingerprint every time same fixed input could not be given because client could not place finger in the same way and location as it was done initially.
3. When fingerprint is given as input, RNA-FINNT would execute and output *Z* would be derived.
4. Now this *Z* is not going to match with the original stored value at the server so Linear symmetric hash function would be executed.
5. Linear symmetric hash function (LSHF) would run and generate value *Y* [129].

LSHF would execute: Suppose that two fingerprints originating from one finger differ by scale and rotation. If M are represented on a complex plane, then scaling and rotation can be expressed by function:

$f(z) = rz + t$

Let $(c_1, c_2, c_3, \ldots\ldots, c_n)$ be the set of M of index finger (first time) and $(c_1', c_2', c_3', \ldots\ldots, c_n')$ be the set of M of index finger (second time) then transformation would be done with function

$f(z) = rz + t$

such that $c_i' = f(c_i') = r(c_i') + t$ *where* $i = 1,2,3,\ldots\ldots,n$

Functions for minutiae positions would be:

$h_1(c_1, c_2, c_3,\ldots\ldots, c_n) = (c_1, c_2, c_3,\ldots\ldots, c_n)$

$h_2(c_1, c_2, c_3,\ldots\ldots, c_n) = (c_1^2, c_2^2, c_3^2,\ldots\ldots, c_n^2)$

……

$h_m(c_1, c_2, c_3,\ldots\ldots, c_n) = (c_1^m, c_2^m, c_3^m,\ldots\ldots, c_n^m)$

This hash function would work in linear symmetric way so the result would be generated symmetrically. When *r* and *t* are found then higher order hash functions could be used to check if the fingerprints match. Then the function would result as follows:

$h_3' = r^3h_3 + 3r^2th_2 + 3rt^2h_1 + nt^3$

For checking either the result matches or not following steps would run [129]:

- At the time of enrollment M are extracted and *K* symmetric hash functions are evaluated.
- The result after enrollment is stored in the server (database).
- In order to match again M are extracted, *K* symmetric hash functions are evaluated and passed to server for matching.
- By using values of first two hash functions the transformation parameters *r* and *t* would be found.
- Remaining K-2 hash functions values would be used to verify that minutiae set is matching or not.

6. Y generated would match with the initially stored value if it is a legitimate user.

So linear symmetric hash function is used to verify either the client is legal or not. And this function executes in the process of mutual authentication with the help of fingerprint as identity authentication parameter. Transformation is used in the LSHF.

II. **Bio Hash Function:** Fingerprint is not the combination of pixels like screen rather it is combination of curves which we see on every fingerprint. So in order to match the fingerprint we need skeleton of the original fingerprint image and then number of curves could be calculated. Bio hash function could be used with principal curve to generate the skeleton of the original image. The curve should satisfy the following stated properties:

1. It should never intersect itself. This property could be met by removing false minutiae points extracted on the image.

2. It should have finite length inside any specific area. This could be met by dividing the fingerprint image into the grid of squares of equal size.

This function uses Linear Least Square to compute the translation rotation and equal error rate of the fingerprint. First Euclidean distance between the points is used and then following algorithm is to be executed to match the fingerprint [130]:

- Take Euclidean distance between points
- Start a loop to calculate h and h', h would be used to calculate normal distance and h' would be used to calculate transformed distance. For i =1 to n,

  $h_1' = rh_1 + t$, $x_i = \text{sum}(h_i)$, $y_i = \text{sum}(h_i')$

- Calculate transformed, rotation and equal error rate on the basis of following equations:

$$t = \frac{\sum_i x_i^2 \sum_i y_i - \sum x_i \sum x_i y_i}{n \sum_i x_i^2 - (\sum_i x_i)^2} \quad , \quad i = 1,2, \dots \dots \dots \dots, n$$

$$r = \frac{\sum_i x_i y_i - \sum_i x_i \sum_i y_i}{n \sum_i x_i^2 - (\sum_i x_i)^2} \quad , \quad i = 1,2, \dots \dots \dots \dots, n$$

$$E = \sum_i (y_i - (t + r x_i)) \quad , i = 1,2, \dots \dots \dots \dots, n$$

We consider that if points are extracted two times from the same finger then they would be different in transformation and rotation. In order to match that it belongs to the same person scaling and rotation is done and minutiae points from one fingerprint could be obtained from another fingerprint.

III. **RNA-FINNT:** Fingerprint is a combination of arches, ridges and whorls. So in order to match the fingerprint original fingerprint image has to be taken again. In this thesis RNA-FINNT is used for fingerprint match. Extraction of terminations and bifurcations is to be done second time and values of coordinates and angles are to be stored in the database. The process of matching would be done by comparing coordinate and angle values of first time and second time extraction of terminations and bifurcations between each other. If more than 75% of the values gets matched it is the same fingerprint image otherwise malicious.

4.3 PROOF OF REDUCTION IN ERROR

Minutiae points considered for fingerprint matching in the forensic labs are hardly 8 to 12. The fingerprint is considered matched if only 8 minutiae points get matched [131]. So existing algorithms as discussed in Chapter 2 Section 2.7 focuses on only extracting either 8 or 12 minutiae points. But RNA-FINNT helps in extracting more than 15 minutiae points. Generally minutiae points on a fingerprint if counted result as 30 but as the algorithms consider only 8 minutiae points than 30% is the error percentage already exists in the identity authentication process [131]. But even if 12 minutiae points are considered by existing fingerprint algorithms then some mathematical calculation is required to justify that error percentage would be reduced from 30%. Explanation of reduction in error percentage is given below [131]:

$$Reduction\ in\ Error\ for\ Existing\ Algorithms = r_1(e)$$

$$Reduction\ in\ Error\ for\ RNA - FINNT\ Algorithm = r_2(e)$$

$$Error\ Percentage = e(p)$$

$$Overall\ Reduction\ in\ Error(When\ tm(p)\ are\ increased) = \Delta r(e)$$

$Number\ of\ Minutiae\ Points = m(p),$

$Increase\ in\ Number\ of\ Minutiae\ Points = \Delta m(p)$,

$Total\ Number\ of\ Minutiae\ Points\ for\ Consideration = tm(p)$,

$New\ Calculated\ Error\ Percentage = e_1(p)$,

Proof*: *For Existing Algorithm

$m(p) = 8$, $e(p) = 30$, $\Delta m(p) = 4$,

$tm(p) = m(p) + \Delta m(p) = 8 + 4 = 12,$

$$e_1(p) = \frac{(e(p) * m(p))}{tm(p)} = \frac{30*8}{12} = 20 \quad \text{..... (1)}$$

$i.e\ New\ Calculated\ Error\ Percentage\ is\ 20.$

$$r_1(e) = e(p) - e_1(p) = 30 - 20 = 10 \quad \text{..... (2)}$$

Basic consideration is if only 8 minutiae points are considered for computation than error percentage is 30%. But if 12 minutiae points are considered for computation then according to (1) error percentage would be 20%. So according to (2) the overall reduction in error percentage when number of minutiae points are 12 is 10.In RNA-FINNT more than 12 minutiae points are considered so the error percentage reduces as the number of minutiae points into consideration is increased. If 15 minutiae points are considered then following is the error percentage [131].

Proof*: *For RNA − FINNT

$m(p) = 8$, $e(p) = 30$, $\Delta m(p) = 7$,

$tm(p) = m(p) + \Delta m(p) = 8 + 7 = 15,$

$$e_1(p) = \frac{e(p) * m(p)}{tm(p)} = \frac{30*8}{15} = 16 \quad \text{..... (3)}$$

$i.e\ New\ Calculated\ Error\ Percentage\ is\ 16.$

$r_2(e) = e(p) - e_1(p) = 30 - 16 = 14$ ….. **(4)**

$\Delta r(e) = r_2(e) - r_1(e) = 14 - 10 = 4$

i.e. Overall Reduction in Error when *tm(p)* is increased is 4. According to (3) the error percentage would be 16 when 15 minutiae points are considered. According to (4) the overall reduction in error percentage in RNA-FINNT is 14. So this proves that when number of minutiae points would be increased then overall error percentage would be reduced. There is overall reduction in error percentage when number of minutiae points are increased [131].

As per Equation (2) number of minutiae points considered were 12 and reduction in error percentage is 10. As per Equation (4) number of minutiae points considered were 15 and reduction in error percentage is 14. So, overall reduction in error percentage would be calculated by subtracting equation (2) from equation (4) [131]:

$\Delta r(e) = r_2(e) - r_1(e) = 14 - 10 = 4$

$i.e\ Overall\ Reduction\ in\ Error\ when\ tm(p) is\ increased\ is\ 4.$

Overall reduction in error when RNA-FINNT is used is 4%. This substantiates that RNA-FINNT is an ideal authentication algorithm with reduced error percentage. Proof of reduction in error percentage resulted in filling of the research gap 2.

4.4 DIMINUTION IN ERROR APPROXIMATION

Diminution in error approximation is proved with the help of two experiments. Experiment 1 validates the diminution in error approximation with RNA-FINNT and Experiment 2 validates the diminution in error approximation with the assimilation of Password with RNA-FINNT.

1. **Diminution in error approximation with RNA-FINNT:** It is validated through Table 2 of Chapter 3. Total number of attacks from Table 2 of Chapter 3 considered for experiment is 18. Out of total 18, password is affected by 16 attacks, fingerprint (extraction with Grid Hash Algorithm) is affected by 15 attacks, fingerprint (extraction with Angle Hash Algorithm) is affected by 14

attacks and fingerprint (extraction with Minimum Distance Hash Algorithm) is affected by 15 attacks [128]:

Total Attacks = 18 $p = 16, f(g) = 15, f(a) = 14, f(m) = 15$

For validating the diminution in error approximation mathematical calculations would be required and count of number of attacks on RNA-FINNT needs to be calculated. All 18 attacks were tried on RNA-FINNT and after experimentation it is found that total 8 number of attacks are possible on RNA-FINNT and that are denial of service attack, forgery attack, ping of death, mutual authentication, parallel session attack, ping broadcast, session hijacking and tear drop attack. Hence diminution in error approximation with RNA-FINNT is proved.

2. **Diminution in error approximation with assimilation of Password with RNA-FINNT:** For validation of diminution in error approximation with assimilation of password with RNA-FINNT following steps are required [128]:

Error Approximation = e

Password = p

Total Number of defined Attacks and Security Requirements = n

Number of Attacks on p = t (p)

Error Approximation in p = p (e)

Grid Hash Algorithm used for extracting Fingerprint = f (g)

Number of Attacks on f (g) = t (f (g))

Error Approximation in f (g) = f (g) (e)

Total Number of Attacks and Security Requirements possible if p is assimilated with:

f (g) = p (f (g))

Total Error Percentage with p(f (g)) = te (pg)

Total Number of defined Attacks and Security Requirements are n but for assimilation are:

$p(f(g)) = n(p(f(g)))$

Angle Hash Algorithm used for extracting Fingerprint $= f(a)$

Number of Attacks on $f(a) = t(f(a))$

Error Approximation in $f(a) = f(a)(e)$

Total Number of Attacks and Security Requirements possible if p is assimilated with:

$f(a) = p(f(a))$

Total Error Percentage with $p(f(a)) = te(pa)$

Total Number of defined Attacks and Security Requirements are n but for assimilation are:

$p(f(a)) = n(p(f(a)))$

Minimum Distance Hash Algorithm used for extracting Fingerprint $= f(m)$

Number of Attacks on $f(m) = t(f(m))$

Error Approximation in $f(m) = f(m)(e)$

Total Number of Attacks and Security Requirements possible if p is assimilated with:

$f(m) = p(f(m))$

Total Error Percentage with $p(f(m)) = te(pm)$

Total Number of defined Attacks and Security Requirements are n but for assimilation are:

$p(f(m)) = n(p(f(m)))$

RNA-FINNT Hash Algorithm used for extracting Fingerprint $= f(r)$

Number of Attacks on f (r) = t (f (r))

Error Approximation in f (r) = f (r) (e)

Total Number of Attacks and Security Requirements possible if p is assimilated with:

f (r) = p (f (r))

Total Error Percentage with p (f (r))= te (pr)

p (f (r))= n (p (f (r)))

Step 1: Each Identity Authentication Parameter is calculated for total percentage of number of Attacks and Security requirements.

$$p(e) = \left(t(p) \div n \times 100\right) = 16 \div 18 \times 100 = 88.8 = 89$$

$$f(g)(e) = \left(t\left(f(g)\right) \div n \times 100\right) = 15 \div 18 \times 100 = 83.3 = 83$$

$$f(a)(e) = \left(t\left(f(a)\right) \div n \times 100\right) = 14 \div 18 \times 100 = 77.7 = 78$$

$$f(m)(e) = \left(t\left(f(m)\right) \div n \times 100\right) = 15 \div 18 \times 100 = 83.3 = 83$$

$$f(r)(e) = \left(t\left(f(r)\right) \div n \times 100\right) = 8 \div 18 \times 100 = 44.4 = 44$$

Step 2: When p is assimilated with each Identity Authentication Parameter i.e *f* (*g*), *f* (*a*), *f* (*m*), *f* (*r*) than calculate the count of all the Attacks and Security requirements.

$$p\left(f(g)\right) = t(p) + t\left(f(g)\right) - \left(t(p) \cup t\left(f(g)\right)\right) = 16 + 15 - 18 = 13$$

$$p\left(f(a)\right) = t(p) + t\left(f(a)\right) - \left(t(p) \cup t\left(f(a)\right)\right) = 16 + 14 - 18 = 12$$

$$p\left(f(m)\right) = t(p) + t\left(f(m)\right) - \left(t(p) \cup t\left(f(m)\right)\right) = 16 + 15 - 18 = 13$$

$$p\left(f(r)\right) = t(p) + t\left(f(r)\right) - \left(t(p) \cup t\left(f(r)\right)\right) = 16 + 8 - 18 = 6$$

Step 3: Result of Step 2 states that only 6 numbers of attacks are possible if p is assimilated with *f* (*r*) *i.e.* it becomes an Ideal Password Authentication Scheme. So *p* (*f* (*r*)) is best for Identity Authentication.

Step 4: When p is assimilated with each Identity Authentication Parameter i.e $f(g)$, $f(a)$, $f(m)$, $f(r)$ than calculate error percentage.

$$te(pg) = p(e) + f(g)(e) - n\left(p\left(f(g)\right)\right) = 89 + 83 - 100 = 72$$

$$te(pa) = p(e) + f(a)(e) - n\left(p\left(f(a)\right)\right) = 89 + 78 - 100 = 67$$

$$te(pm) = p(e) + f(m)(e) - n\left(p\left(f(m)\right)\right) = 89 + 83 - 100 = 72$$

$$te(pr) = p(e) + f(r)(e) - n\left(p\left(f(r)\right)\right) = 89 + 44 - 100 = 33$$

Step 5: Result is derived from Step 4 that only 33% of error would be there if assimilation of p with $f(r)$ is implemented *i.e.* Ideal Password Authentication Scheme. When password is assimilated with fingerprint (extraction with Grid Hash Algorithm) the error approximation is 72%, fingerprints (extraction with Angle Hash Algorithm) the error approximation is 67%, fingerprints (extraction with Minimum Distance Hash Algorithm) the error approximation is 72% and fingerprint (extraction with RNA-FINNT Hash Algorithm) the error approximation is 33% [128].

Overall result derived is that in ideal authentication scheme the number of minutiae points extracted is more than 12 so the reduction in error percentage is 4% and in ideal password authentication scheme the diminution in error approximation on the basis of attacks and security requirements is just 33%. Computation of diminution in error approximation resulted in filling of the research gap 3.

The computation of all the values on the basis of set performance indicators like False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage is done in Chapter 6 for performance evaluation and validation of RNA-FINNT.

4.5 BENEFITS OF RNA-FINNT

Reduced Number of Angles Fingerprint Hash Algorithm does not depend upon core points so provides the following benefits:

1. During computation the global feature or core point is not used so it has resulted in **reduced number of angles** (RNA).
2. In the grid of squares any point could be picked at random for calculating the angle values so it has resulted in **removal of dependency**.
3. All the grid of squares executes in **parallel** so the speed of computation is much **faster** than the existing algorithms.
4. It has resulted in the **reduction in error** percentage (explained in Section 4.3) so the overall **efficiency** of the system while execution is increased.
5. It has resulted in **diminution in error approximation** with either only RNA-FINNT or assimilation of password with RNA-FINNT implementation (explained in Section 4.4).
6. It has resulted in the **Fortification of Transport Layer Security Protocol** by enhancing the authentication process (explained in Section 2.11 of Chapter 2).

The overall benefits of RNA-FINNT result that it has enhanced the authentication and verification process.

4.6 COMPLEXITY OF RNA-FINNT

The review of time and space complexity of various algorithms is done in Chapter 2 but the comparative study of the existing algorithms with RNA-FINNT is required to show the overall time and space complexity of RNA-FINNT.

Table 7: Complexity of RNA-FINNT in comparison to other algorithms

S.No	Algorithms	Time Complexity	Space Complexity
1	Feature based fingerprint algorithm [86][87]	O(n)	O(n)
2	Cluster Fingerprint Recognition [91] [92]	O(n)	O(n)
3	Genetic algorithm for fingerprint matching [94]	$O(m^2)$	$O(m^2)$
4	Minutiae based fingerprint algorithm [86][95][96]	$O(n^2)$	$O(n^2)$
5	Grid hash algorithm [43][107]	O(n log n)	O(n log n)
6	RNA-FINNT [49]	O(n)	O(n)

The complete experimentation using RNA-FINNT is done in Chapter 5 and Table 8 is derived on the basis of performance indicators of algorithms (explained in Section 2.7 and 2.8 of Chapter 2) to analyze the recognition accuracy of the existing algorithms.

Table 8: Approximate Accuracy Analysis of Existing Algorithms

S.No	**Values**	**Cluster Fingerprint Recognition [91] [92]**	**Orientation estimation algorithm for fingerprint [97] [98] [99]**	**Novel algorithm for detecting singular points from fingerprint images [100] [101]**
1	***fmr***	Penetration Rates are 29.48% and 29.69%.	Average Processing Time is 16.	Average Processing Time as 3.14.
2	***eer***			
3	***thv***			
4	***far***			
5	***frr***			
6	***fnr***			
7	***epr***			

Comparison in Table 8 on the basis of set performance indicators substantiates good performance of existing algorithms but complete experimentation has to be done for RNA-FINNT in Chapter 5.

5

Experiments And Results of (RNA-FINNT)

CHAPTER – 5

EXPERIMENTS AND RESULTS OF RNA-FINNT

The literature review done in Chapter 2 about the algorithms and techniques of fingerprint used by biometric machines for human recognition stated the need for new fingerprint hash algorithm which should result in reduced error percentage in comparison to the existing algorithms. In Chapter 3 the complete comparative study of existing technologies and algorithms has shown their benefits and problems and proved that new fingerprint hash algorithm would overcome majority of these problems. Chapter 4 focused upon deriving RNA-FINNT as new fingerprint hash algorithm and proved the diminution in error approximation and overall reduction in error percentage. This chapter focuses upon the experiments and results derived through execution of RNA-FINNT. And with the results new question will arise that with embedded RNA-FINNT in biometric machines the identity authentication would enhance or not?

For performing the experiment of RNA-FINNT and substantiating the results following steps were followed:

1. Setting the environment with standards for the experiment taking into consideration the database requirements, memory requirements, fingerprint format, hardware and software requirements.
2. Prepared Graphical User Interface in MATLAB (experiment was performed in the University premises with licensed software).
3. Main menu creation in the GUI of MATLAB.
4. Prepared database taking the students and faculty of the University as the source and the database is not made available due to data protection and privacy issues. Total 50 individuals participated and 2 impressions of each individual is considered so in total 100 fingerprints were used for the experiment.
5. MATLAB implementation of RNA-FINNT Algorithm for proving the results.
6. Reckoning of the minutiae points and to prove the augmentation of trust and privacy.
7. Proving that embedded RNA-FINNT in biometric machines will enhance security.
8. Substantiation for fortified security and privacy on set performance indicators.

5.1 SETTING THE ENVIRONMENT WITH STANDARDS

Setting the standard environment for the execution of experiment of RNA-FINNT needs to focus upon database requirements, memory requirements, fingerprint format, hardware and software requirements etc. For substantiating the results following environment is set for the experiment of RNA-FINNT:

Table 9: Setting the Environment with Standards for experiment of RNA-FINNT

S.No	Environment Standards	RNA-FINNT Details
1	Performance Indicators	False Matching Rate *(fmr)*, Equal Error Rate *(eer)*, Threshold Value *(thv)*, False Acceptance Rate *(far)*, False Reject Rate *(frr)*, False Non Match Rate *(fnr)* and Error Percentage *(epr)*
2	Algorithms Evaluated	13 Algorithms compared
3	Population	Students and Faculty, average age 22 and 26 respectively
4	Fingerprint Format	Mixed format (Arch, Tented, Loop, Whorl etc) through the same Fingerprint Scanner
5	Perturbations	Mainly due to low quality fingerprint of some subjects
6	Fingerprint Scanner	Optical (Digital Persona)
7	Database Availability	Database belongs to the students and faculty of the University so cannot be made available due to data protection and privacy issues
8	Data Collection	Students and Faculty of the University are the source for experiment of RNA-FINNT
9	Database Size	50 individuals and 2 impressions of each so in total 100 fingerprints
10	Evaluation Type	Independent but supervised by the guide
11	HW/SW used for running the experiment	Intel Core i3, Windows 7
12	Best *epr*	It is the percentage calculation of *eer* (Equal Error Rate).

5.2 GRAPHICAL USER INTERFACE IN MATLAB

RNA-FINNT needs a graphical user interface to substantiate the results. This thesis used MATLAB for programming the algorithm. The experiment was executed in the laboratory of University on the licensed software [132]. The GUI of the experiment looks like *Figure 30*. The programming of the labels is done in MATLAB and details of labels are shown in *Figure 31*. The labels included are:

1. Binary Conversion (Take an RGB image which would be three dimensional, convert that RGB image to gray scale which would be two dimensional, convert gray scale image to binary image which is one dimensional, it could be done manually or automatically)
2. Thinning of Image (to identify exact ridges, loops and whorls over the fingerprint)
3. RNA-FINNT for minutiae extraction on the basis of terminations and bifurcations
4. False Minutiae to be removed (If false minutiae are extracted then remove those)

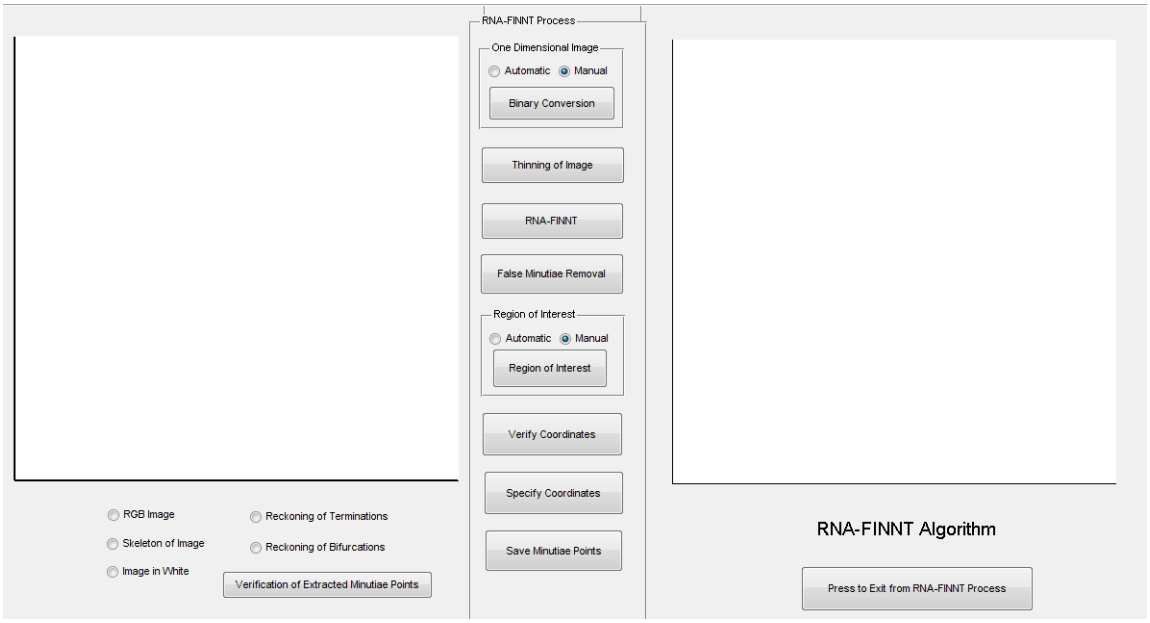

Figure 30: Graphical User Interface for execution of RNA-FINNT

5. Region of Interest (reckoning of bifurcations and terminations is to be done, it could be done manually or automatically)
6. Verification of Coordinates

7. Specification of Coordinates
8. Save the Angle values of extracted Minutiae Points

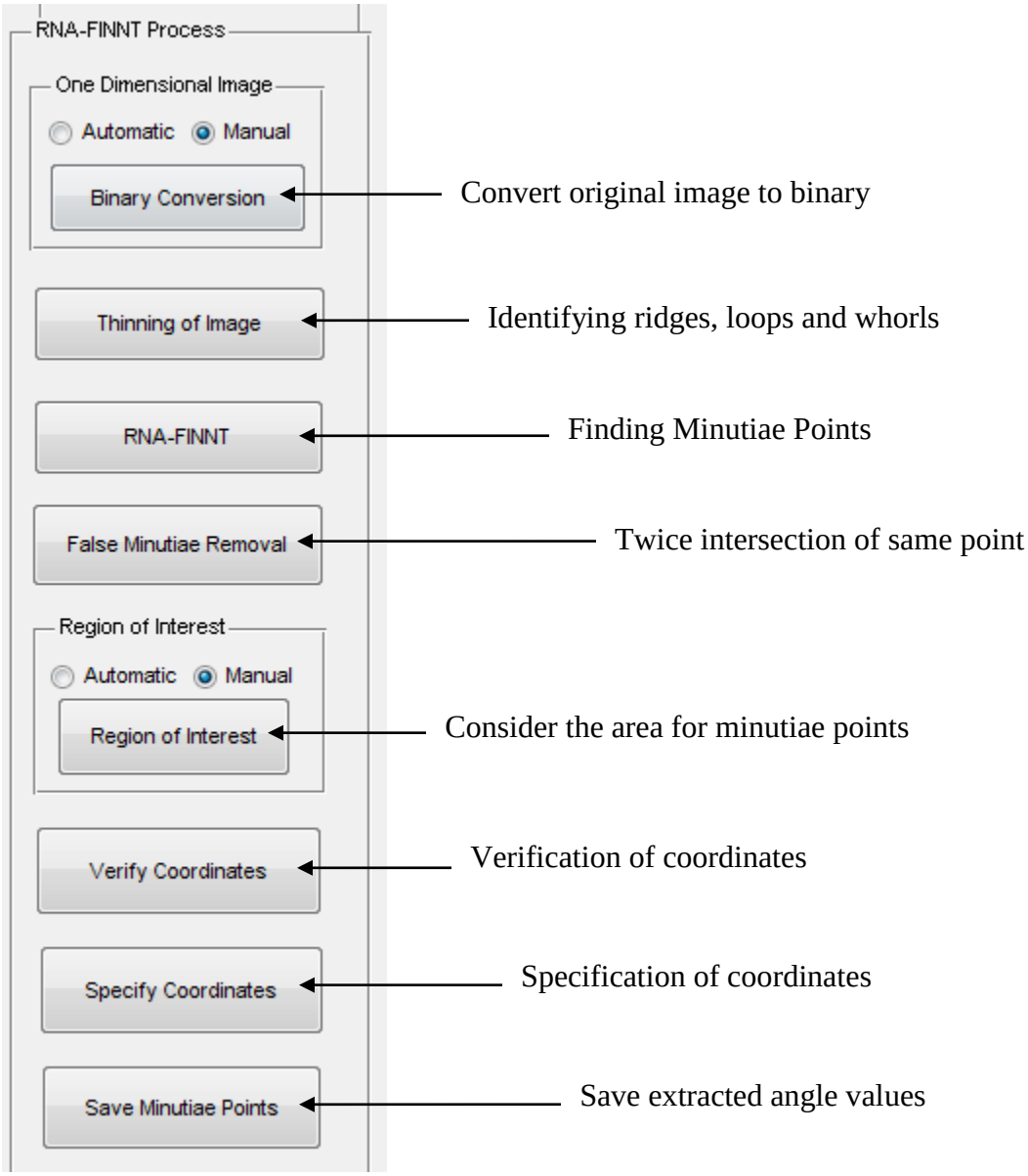

Figure 31: Labels included in GUI

5.3 MAIN MENU CREATION IN MATLAB

Main menu in the GUI states the loading of the RGB image and exporting of the minutiae points into the database (*Figure 32*). The original RGB image which is three dimensional has to be loaded with the help of Load Image function of the main menu [133]. The

function Export Minutia is used to store the calculated angle values into the database which could further be used for fingerprint match [134].

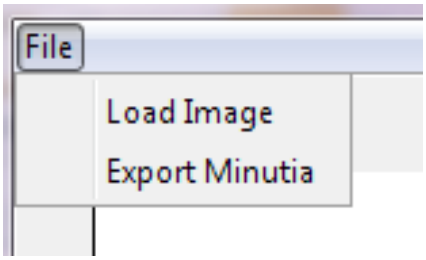

Figure 32: Main menu of GUI

To calculate the minutiae points for fingerprint matching from the original image i.e either the extracted image matches with the image stored in the database the RGB image could be displayed in the form of original image, skeleton and white image with the use of main menu of the image display (*Figure 33*). And reckoning of terminations and bifurcations of the minutiae could be done through main menu of the minutiae display for calculating the points and angle values. If the extracted points get matched with the stored image points then it is the true image otherwise malicious user.

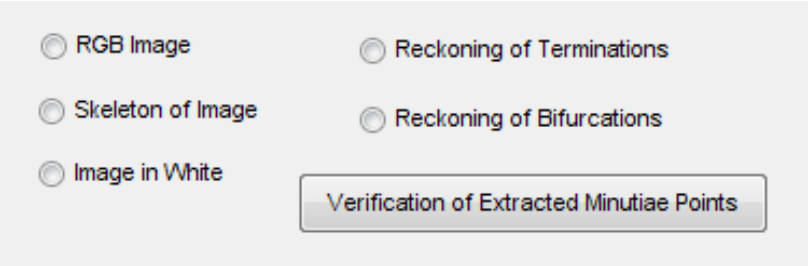

Figure 33: Verification of Extracted Minutiae Points

The main menu is created with the help of MATLAB as a tool for programming. The labels included in the GUI are executed only after the initial main menu starts. First step of the GUI is to load the RGB image which starts in the main menu.

5.4 DATABASE OF IMAGES

Experiment includes three different types of database for execution of RNA-FINNT like real time database, existing database and noisy fingerprint database:

1. **Real Time Database:** Database is prepared in the University itself by taking the students and faculty of the University as the source. The matter of data protection and privacy issues are associated with the individuals so database is not made available. It is used only for the purpose of experimentation of RNA-FINNT. Total 50 individuals participated for the smooth execution of the experiment. 2 impressions of each individual are considered, so in total 100 fingerprints were used for the experiment. The database is stored in MATLAB (*Figure 34*).

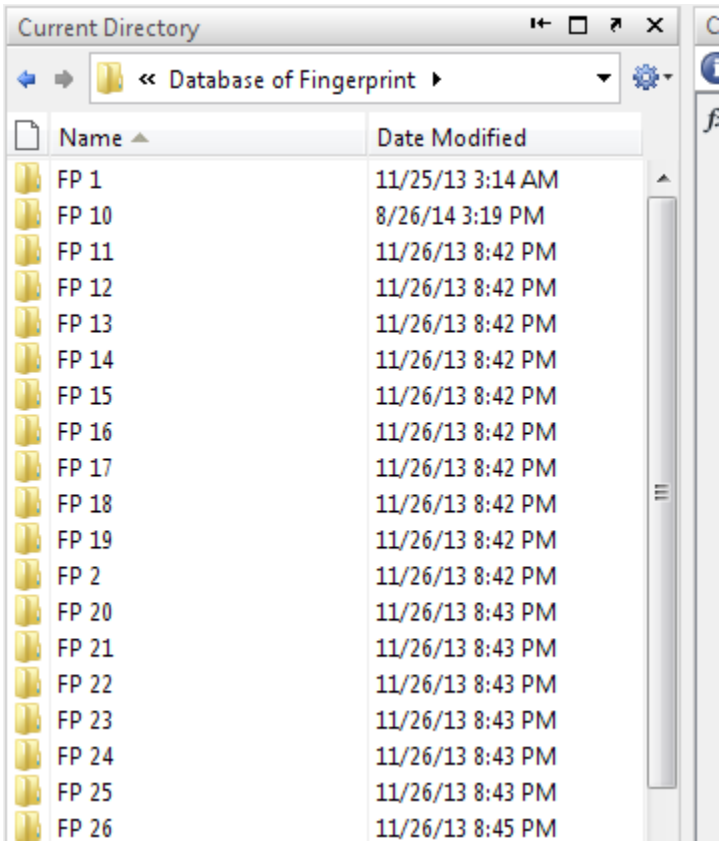

Figure 34 : Database of the Images

The format of the fingerprints extracted is mixed like Arch, Tented, Loop, Whorl etc through the same Fingerprint Scanner. Optical (Digital Persona) is used to extract the images. The perturbation faced is mainly due to low quality fingerprint of some individuals. All the fingerprints are evaluated independently but under the supervision of the guide. This database is stored with the help of Windows 7 operating system and Intel Core i3 processor.

2. **Existing Database:** In order to validate the performance of RNA-FINNT it is tested with the existing databases FVC2000, FVC2002 and FVC2004. The databases FVC2000, FVC2002 and FVC2004 have 80 fingerprint images in DB1_B, DB2_B, DB3_B and DB4_B respectively. While in this thesis 10 subjects are taken 5 images per finger considered. In total 50 fingerprint images are taken for evaluation [135][136][137][138].

3. **Noisy Fingerprint Database:** The databases are FVC2000 and FVC2002 which has few fake or noisy fingerprint images in the .bmp format and 80 fingerprint images in DB1_B, DB2_B, DB3_B and DB4_B respectively. Few sample images which have noise on it are considered for experiment. 8 impressions of each fingerprint are stored. While in this thesis 10 subjects are taken 8 impressions of each fingerprint are considered. In total 80 fingerprint images are taken for evaluation [135]This database is used in the thesis to check the fingerprint match with RNA-FINNT if fingerprint contains too much of noise [135].

5.5 MATLAB IMPLEMENTATION OF RNA-FINNT ALGORITHM

The experiment is executed using MATLAB. Complete programming is done using MATLAB. The matter of copyright is associated with the programming so the code is not made public. Only few functions are written in the thesis. The execution of the RNA-FINNT experiment is explained and shown below with the help of steps, functions of code and GUI. The steps are as follows:

1. RGB image is loaded with the function of Load Image from the main menu. This image is three dimensional so there is need to convert it into one dimensional so the exection is possible with either 0 or 1 [127] [139].

function FPGUI_OpenFn(figure, userdata, vararg)

figure : for taking the image of the fingerprint

userdata : structure for handling any input through GUI

vararg : variable for inserting arguments into the GUI

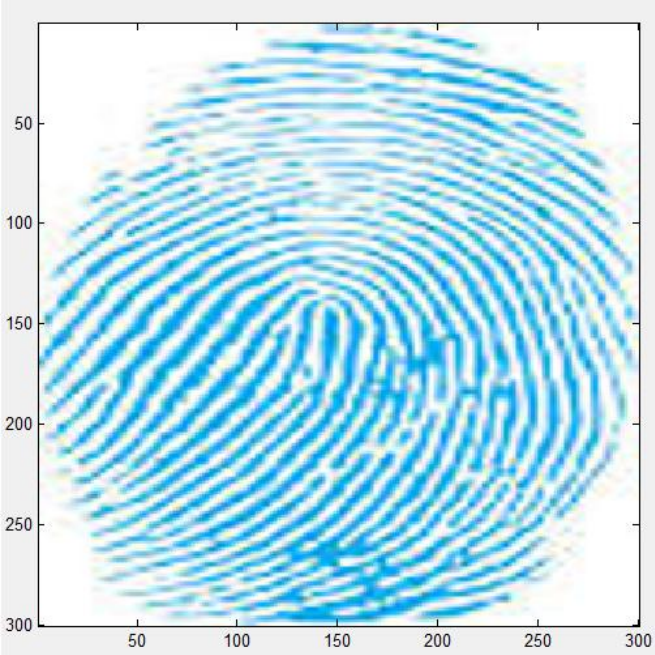

Figure 35: Original RGB Image

2. Convert the loaded image into binary. As the RGB image is three dimensional so it is first converted to two dimensional by converting the RGB image into gray scale. Then gray scale image is converted into binary image which is only one dimensional [127].

setappdata(userdata.FPGUI,'BinaryImage',BinaryImage);

.....

Convert RGB image to Gray Scale

rgb_img = imread('.bmp');*

image(rgb_img)

.....

Convert Gray Scale to Binary

I = imread('.tif');*

BW = dither(I);

imshow(I), figure, imshow(BW)

.....

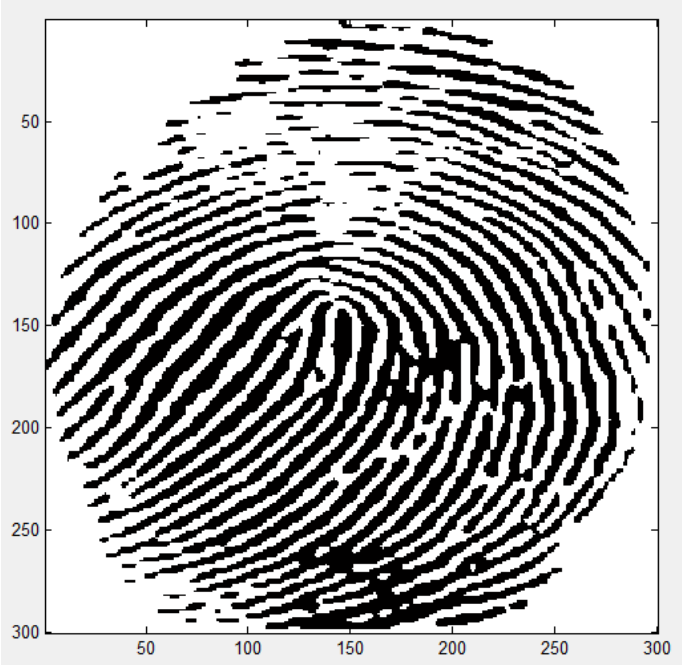

Figure 36: Conversion of Original Image into Binary Image

3. The ridges, loops and whorls etc are identified over the fingerprint by the process of thinning [127] [140].

```
I=getappdata(userdata.FPGUI,'BinaryImage');

BW = imread('*.bmp');

imshow(BW);

.....

BW2 = bwmorph(BW,'remove');

figure, imshow(BW2)

.....

BW3 = bwmorph(BW,'skel',Inf);

figure, imshow(BW3)

.....
```

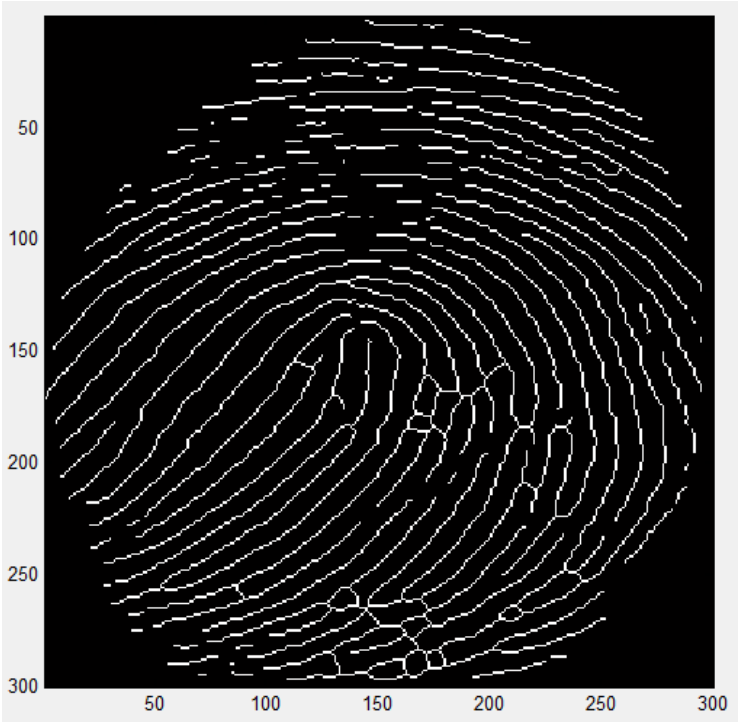

Figure 37: Thinning of the Binary Image

4. The minutiae points are found with RNA-FINNT. First the image is divided into grid of squares using Neighborhood Operation (*nlfilter)* and Block Processing Function (*blkproc*) *(Figure 38)*. In each grid the number of points is counted. If it is 2 or less than two then same count values is stored in the matrix. But if it is more than 2 then angle is calculated by finding the slope of line. This angle is also stored in the matrix. Minutiae points are the combination of terminations and bifurcations [127]. In order to increase the speed Neighborhood or Block Processing Functions columnwise processing is done (*colfilt*) *(Figure 39)*. Minutiae points are extracted *(Figure 40).*

Neighborhood Operation

I = im2double(imread('.bmp));*

f = @(x) sqrt(min(x(:)));

I2 = nlfilter(I,[2 2],f);

.....

Distinct block operations or Block Processing Function

*f = @(x) uint8(round(mean2(x)*ones(size(x))));*

I3 = blkproc(I,[7 7],f);

imshow(I3)

figure, imshow(I4);

.....

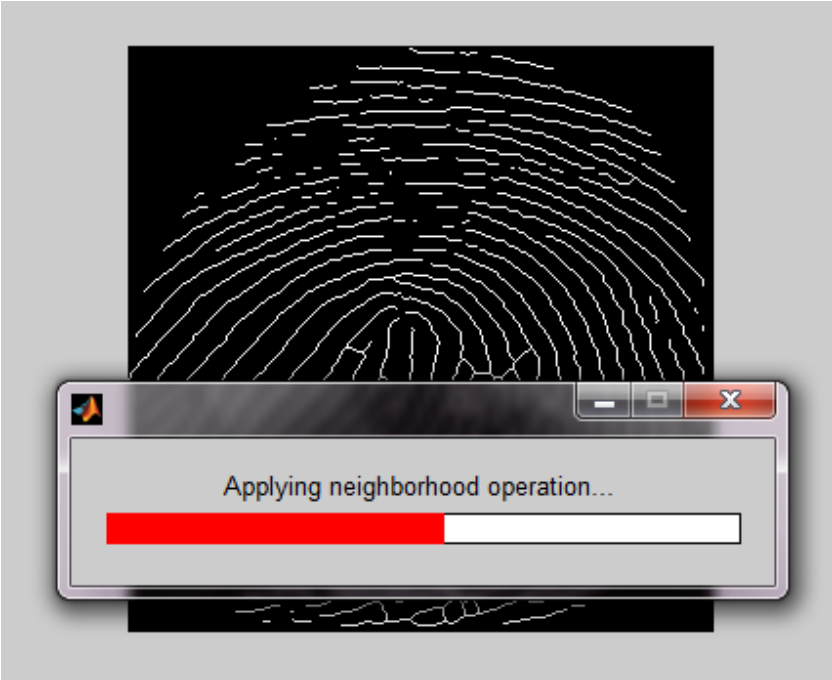

Figure 38: Neighborhood Operation

.....

Columnwise Processing to Speed Up Sliding Neighborhood or Distinct Block Operations

*f = @(x) ones(64,1)*mean(x);*

I2 = colfilt(I,[8 8],'distinct',f);

.....

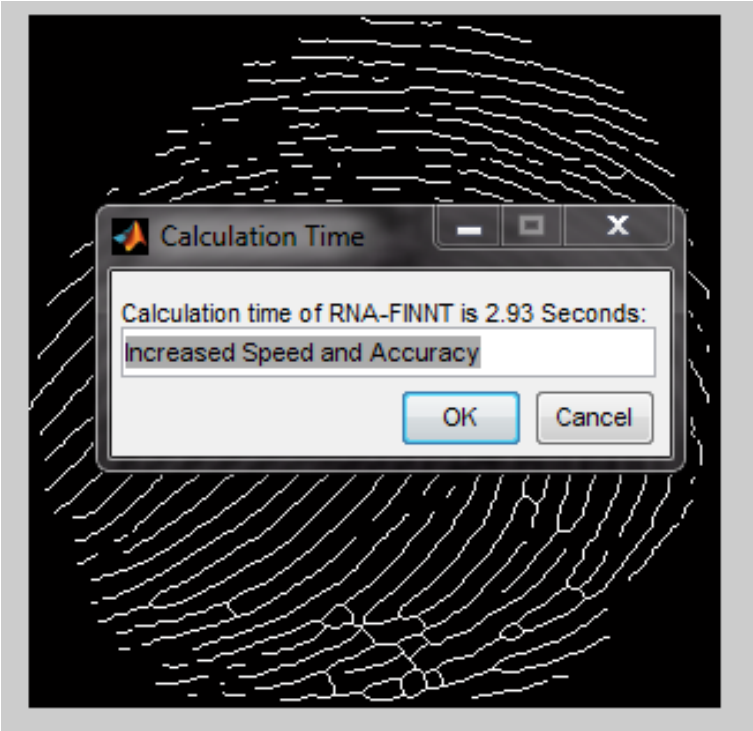

Figure 39: Column Wise Processing

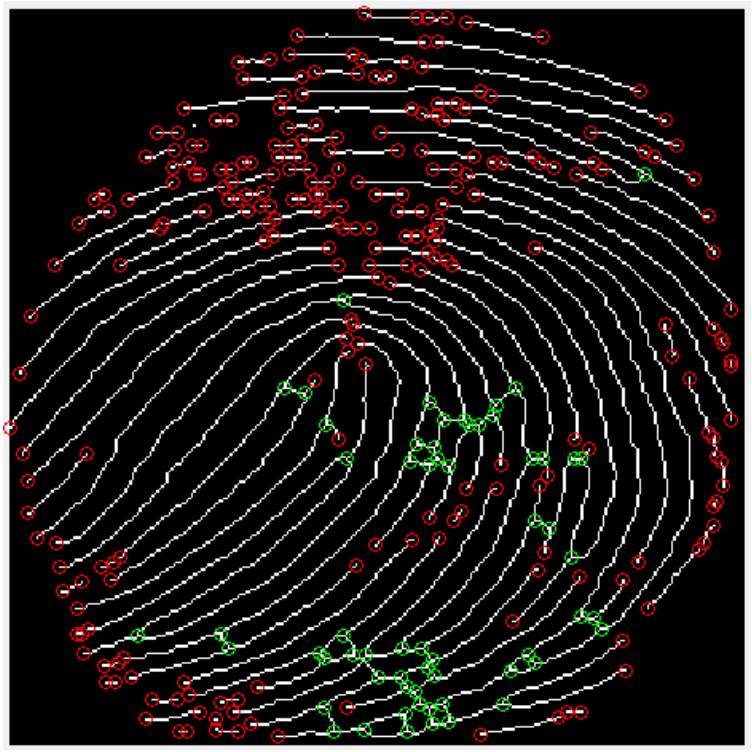

Figure 40: Minutiae points over the Fingerprint

Terminations and bifurcations representing the minutiae points are calculated and displayed on the *Figure 40*. But it comprises of even duplicate values so false minutiae points are to be removed.

5. If the minutiae point is considered in a particular grid then intersection of the same point in another grid is to be discarded. It is done with the function of remove false minutiae [127] [141].

.....

MinuSep=[CentroidSepX CentroidSepY OrientationSep];

CentFinX=getdata(handles.FPGUI,'CentFinX');

CentFinY=getdata(handles.FPGUI,'CentFinY');

OriFin=getdata(handles.FPGUI,'OrienFin');

.....

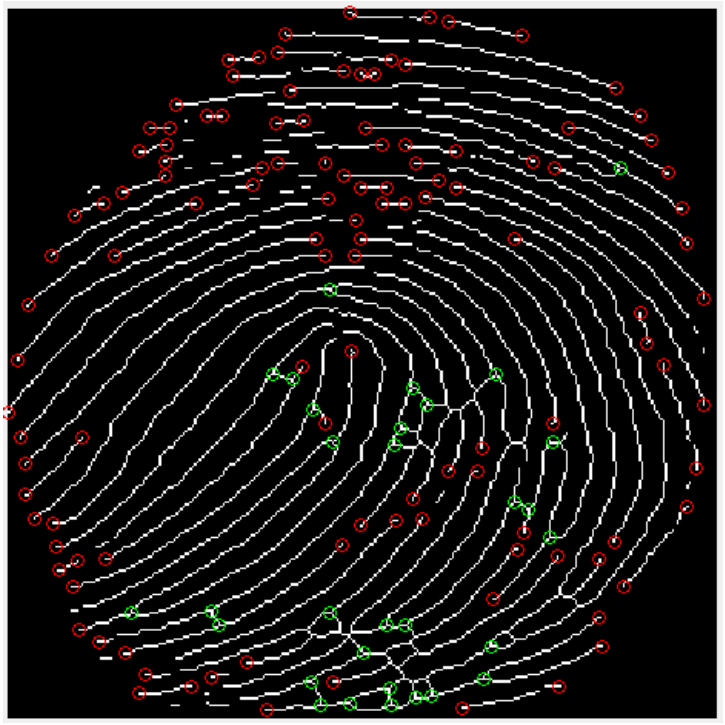

Figure 41: Remove False Minutiae points over the Fingerprint

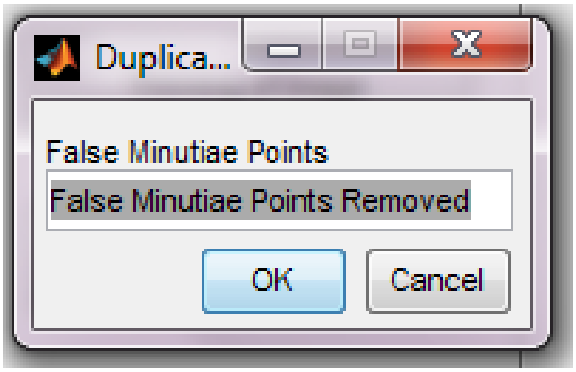

Figure 42: False Minutiae Points Removed

6. To store the fingerprint value in the database some portion of the fingerprint has to be considered. So it is taken either automatically or manually through region of interest in which reckoning of bifurcations and terminations is to be done [90] [127].

.....

[XOffset YOffset Width Height]

plot(CentFinX,CentFinY,'ro','linewidth',2)

plot(CentSepX,CentSepY,'go','linewidth',2)

set(gca,'tag','axes1')

setdata(handles.FPGUI,'CentFinX',CentFinX);

setdata(handles.FPGUI,'CentFinY',CentFinY);

setdata(handles.FPGUI,'CentSepX',CentSepX);

setdata(handles.FPGUI,'CentSepY',CentSepY);

.....

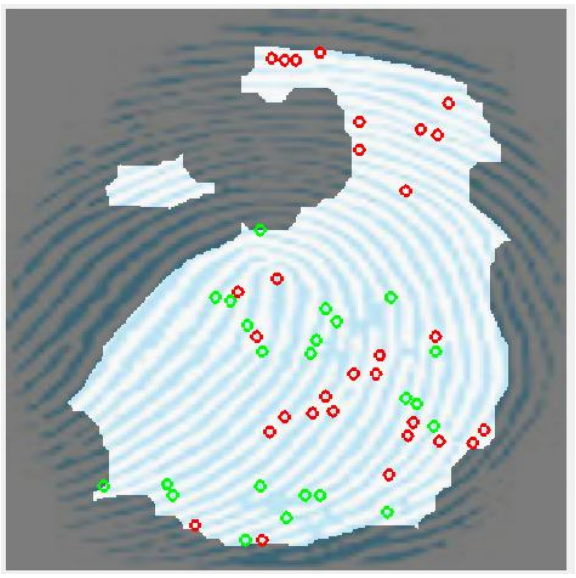

Figure 43: Region of Interest

7. The coordinate values of the fingerprint are verified with the function of orientation.

.....

load geoid;

R = refvec2mat(geoidlegend, size(geoid));

V = refmat2vec(R, size(geoid));

.....

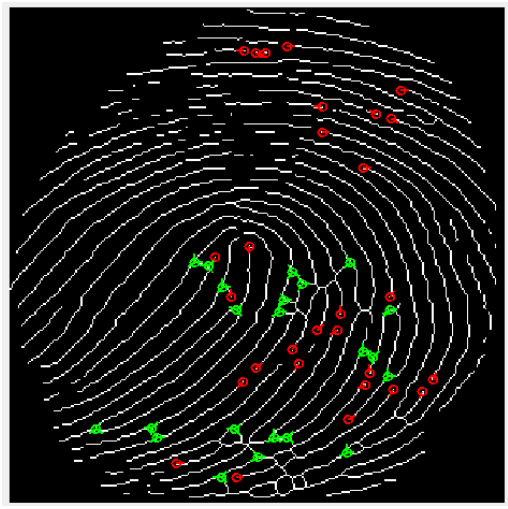

Figure 44: Verify Coordinates of the Image

8. The specific coordinates considered in the region of interest are to be validated with the function of validation [127] [142].

.....

plot(OrienLinesX,OrienLinesY,'g','linewidth',2)

range = getrangefromclass(I)

iptcheckstrs('option3',{'func_name','var_name',2)

.....

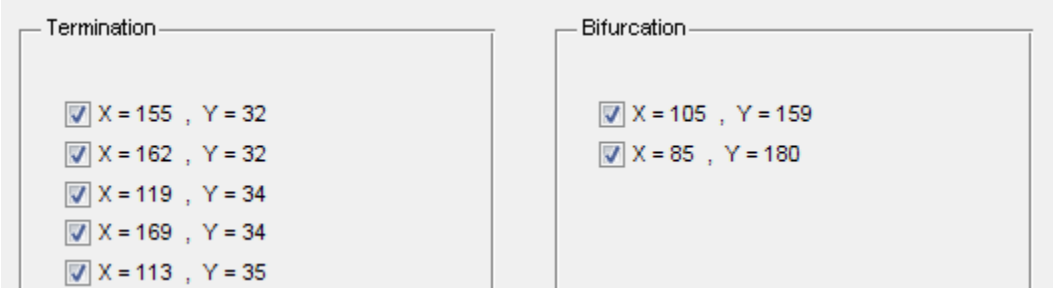

Figure 45: Specification of Coordinates of the Image

9. All the minutiae points are stored in the text file which is in turn stored in the database.

.....

function SaveMinutiae(figure, event, userdata)

prompt = {'Name of the file to be stored:'};

dlg_title = 'Enter the Minutiae Points to be stored';

num_lines = 1;

def = {'FP1 Store'};

answer = inputdlg(prompt,dlg_title,num_lines,def);

saveMinutia(answer{1},MinFin,MinSep);

.....

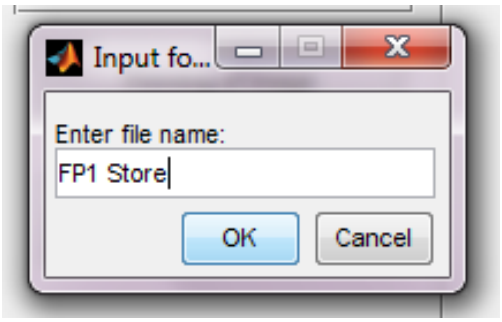

Figure 46: Mention name of the File

```
*******************************
Name: FP2_Store
Date: 2014-09-18
Reckoning of Terminations: 95
Reckoning of Bifurcations:  2
*******************************
*******************************
Reckoning of Terminations:
*******************************
X          Y      Angle
155        32     0.00
162        32     3.14
119        34     0.52
169        34     0.00
113        35     -2.62


*******************************
Reckoning of Bifurcations:
*******************************
X          Y      Angle 1      Angle 2     Angle 3
105        159    2.36         -2.36        -0.79
 85        180    2.62         0.79         -0.79
```

Figure 47: Store the Angle values in the Database

10. Whenever legitimate user would login steps from 1 to 9 would be repeated and matching with the stored values would be done as per Section 4.2 of Chapter 4. This thesis uses RNA-FINNT function for fingerprint matching rather than Linear symmetric hash function and Symmetric Bio Hash function [143] [144].

- RNA-FINNT function would run

.....

I = im2double(imread('.bmp));*

f = @(x) sqrt(min(x(:)));

I2 = nlfilter(I,[2 2],f);

.....

*f = @(x) uint8(round(mean2(x)*ones(size(x))));*

I3 = blkproc(I,[7 7],f);

imshow(I3)

figure, imshow(I4);

.....

*f = @(x) ones(64,1)*mean(x);*

I2 = colfilt(I,[8 8],'distinct',f);

.....

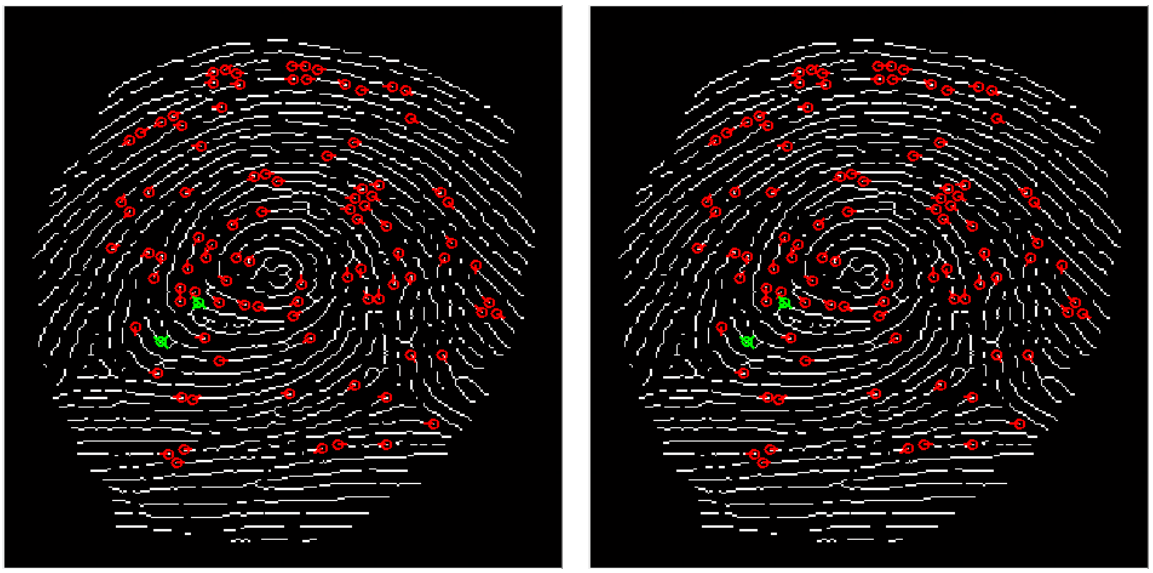

Figure 48: Matching of the Fingerprints

The image of the fingerprint extracted second time would result as similar as the extraction is done first time. It shows that fingerprint belongs to the same person. But if it does not match then the fingerprint does not belong to the same person.

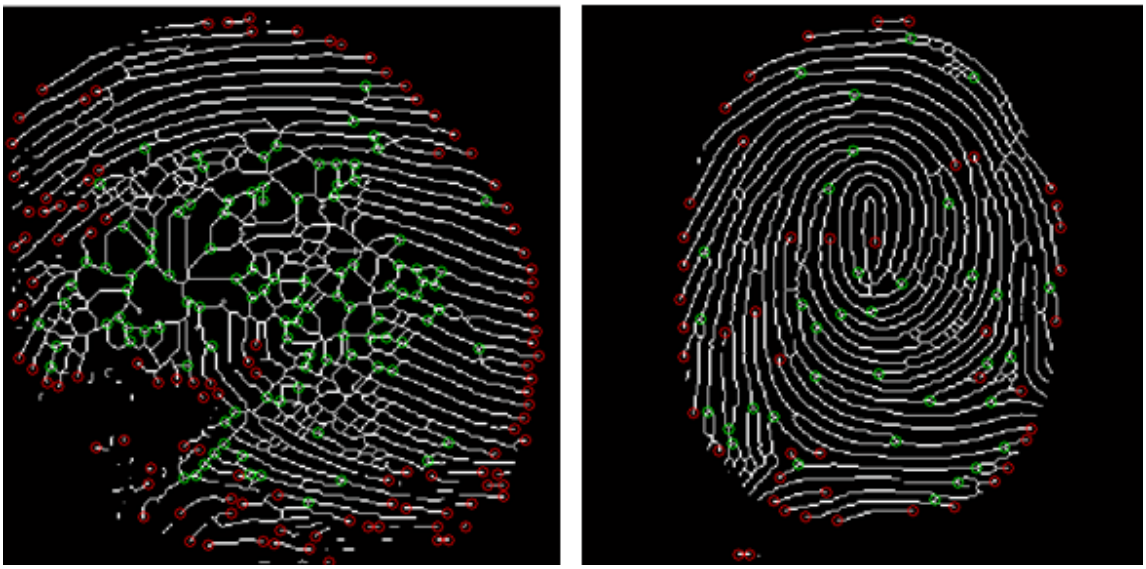

Figure 49: Non Matching of the Fingerprints

11. Compare the text files stored in the database with exact angle values also. It if matches more than 75% then it belong to the same person. But if it matches less then user are malicious. [143] [144]

.....

pof=fopen(outputfile,"a+");

if (pof==NULL) return OPEN_OUTPUT_FILE_FAIL;

if (fprintf(pof,"%8.6f\n",MatchingPerformed?similarity:-1.0)<=0)

return UPDATE_OUTPUT_FILE_FAIL;

fclose(pof);

.....

X	Y	Angle
232	16	-0.52
193	25	-0.52
87	43	3.14
229	44	-0.52

X	Y	Angle
232	16	-0.52
193	25	-0.52
87	43	3.14
229	44	-0.52

Stated are the angle values which are matching in the above stated fingerprint. It is comparative visualization of *Figure 48* for fingerprint matching.

X	Y	Angle
87	74	-2.62
210	82	-1.57
200	87	1.57
112	125	-2.09
133	126	-1.57
157	128	1.57

X	Y	Angle
120	38	3.14
133	41	-0.52
116	45	2.62
122	45	0.00
91	57	-0.52
188	59	-0.52

Stated are the angle values which are matching in the above stated fingerprint. It is comparative visualization of *Figure 49* for fingerprint matching.

The RNA-FINNT algorithm follows the above mentioned steps for identifying the legitimate user. Identity authentication and matching is performed easily with these steps. Following is the example which states that implementation of RNA-FINNT would enhance the processing. As per Section 2.11 of Chapter 2 the applicability is discussed and this example focuses upon the substantiation of the same.

Example to Substantiate the Enhancement:

Minutiae Points are unique points on the fingerprint of the legitimate user. And no one has the same number of points at the same location of the fingerprint. Whenever a session is to be created between the Client and Server the legitimacy of each other is proved through mutual authentication. Client will authenticate Server as legitimate and vice versa. The database at the Server will comprise of angle values stored for individual client in the form of hash code as per step 9 of Section 5.5. Whenever a malicious user will try to intrude the session between client and server then extraction of their minutiae points from their fingerprint will be done as per step 4 of Section 5.5. These extracted values through RNA-FINNT will now be matched with the stored value in the database as per step 10 of Section 5.5. And it is but obvious that these values will never match as

nobody will have same angle values because of the uniqueness of the minutiae points. This proves the enhancement of security in the public network.

The application part discussed in Section 2.11 of Chapter 2 is proved here with the execution of RNA-FINNT. RNA-FINNT resulted in the enhancement of biometric machines also as the error percentage reduces as per Section 4.3 of Chapter 4. It is capable to with stand mutual authentication, forward secrecy and is not vulnerable to denial of service attack, forgery attack, password guessing attack, parallel session attack, replay attack, stolen verifier attack, DNS Poisoning, IP Spoofing, Server Spoofing and Phishing. These results are verified through the above stated experiment on the students and faculty of the University through a human recognition or identity authentication system. In this system the extraction of the fingerprint minutiae points is done and value is stored into the database in a way that intruders should not be capable of hijacking the sessions.

5.6 RECKONING MINUTIAE POINTS AUGMENTS TRUST AND PRIVACY

Public network is the most insecure network. When identity authentication is done in the public network lot of intrusion is possible. This states that when transaction is being accomplished over the transport layer it has the maximum risk. Secured Socket Layer is generally implemented in the virtual private network of organizations for enhancement in the security but it does not completely eradicate the security threats for legitimate users. So security has to be implemented at the authentication level only so that possibility of intrusion could be diminished [127]. When fingerprint is used as identity authentication parameter then entry or authentication level security could be easily implemented. So RNA-FINNT should be implemented at the authentication level. Steps of Section 5.5 should be followed for identity authentication and matching the fingerprint values.

RNA-FINNT used for identity authentication augments trust and privacy of legitimate user as intrusion is diminished at the authentication level only and it results in enhanced security over the Public Network. Transactions could be easily done at the transport layer as implementation of RNA-FINNT fortifies the transport layer [127]. Augmentation of trust and privacy is possible with the exact reckoning of terminations and bifurcations on

the fingerprint for identity authentication. The skeleton of the fingerprint image is required to visualize the terminations and bifurcations.

function Skel_Callback(hObject, eventdata, handles)

if get(hObject,'value')==1

set(handles.OImage,'value',0)

set(handles.WImage,'value',0)

end

.....

function OImage_Callback(hObject, eventdata, handles)

if get(hObject,'value')==1

set(handles.WImage,'value',0)

set(handles.Skel,'value',0)

end

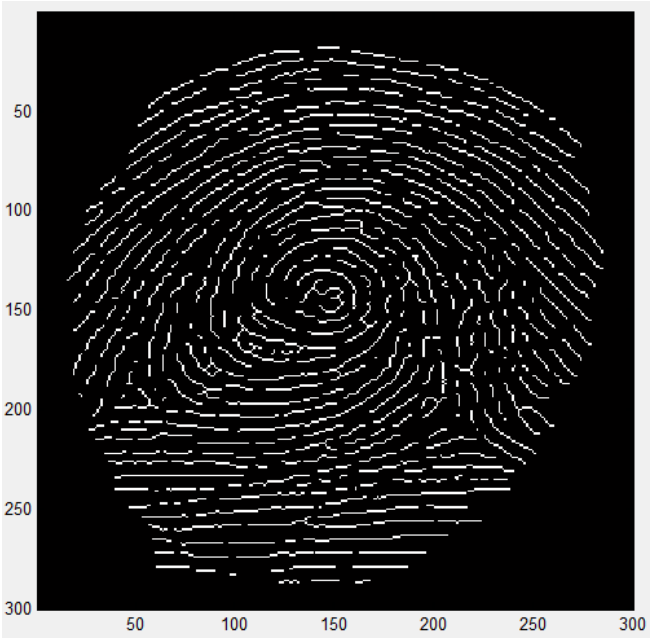

Figure 50: Skeleton of the Fingerprint Image

Proving the augmentation of trust and privacy reckoning of terminations and bifurcations in the grid of squares with original image and white image of the legitimate user is required. Following steps are followed for proving augmentation of trust and privacy:

1. Reckoning the Terminations
2. Reckoning the Bifurcations
3. Specification of Terminations and Bifurcations
4. White Image representation of Terminations and Bifurcations

1. **Reckoning the Terminations:** Counting of the ridge values is done. When the ridge is at the end point of the arch then it is the termination. Function used for reckoning the terminations is [90] [127]:

```
TFin=(L==1);

TFinLab=bwlabel(TFin);

propFin=regionprops(TFinLab,'Cent');

CentFin=round(cat(1,propFin(:).Cent));

CentFinX=CentFin(:,1);

CentdFinY=CentFin(:,2);

axes(handles.axes)

plot(CentFinX,CentFinY,'row')

    ..............................
```

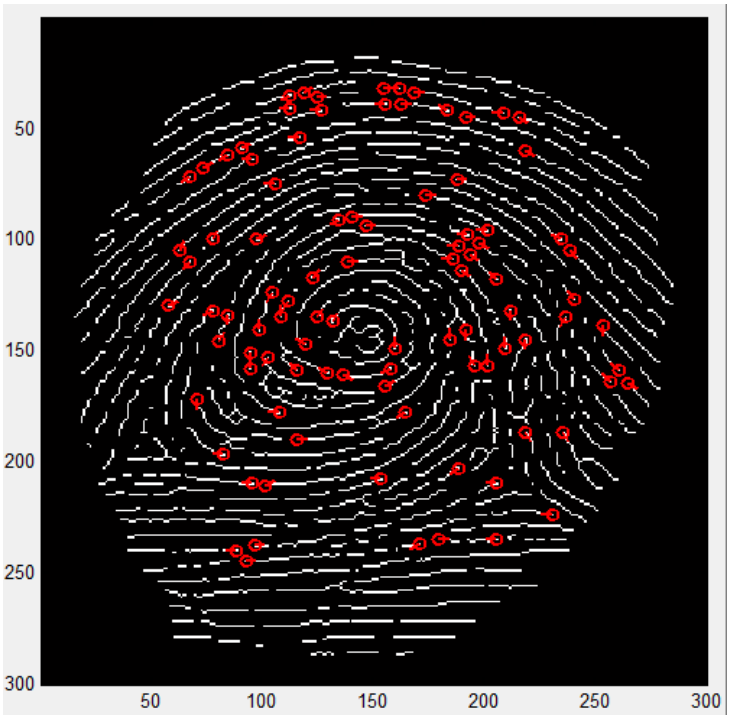

Figure 51: Reckoning of Terminations

2. **Reckoning the Bifurcations:** Counting of the interested ridge values is done. When the ridges intersect at a particular point of the arch then it is called bifurcations. Function used for reckoning the bifurcations is [127] [142]:

BSep=(L==3);

BSepLab=bwlabel(BSep);

propSep=regionprops(BSepLab,'Cent','Image');

CentSep=round(cat(1,propSep(:).Cent));

CentSepX=CentSep(:,1);

CentSepY=CentSep(:,2);

plot(CentSepX,CentSepY,'Column')

.....

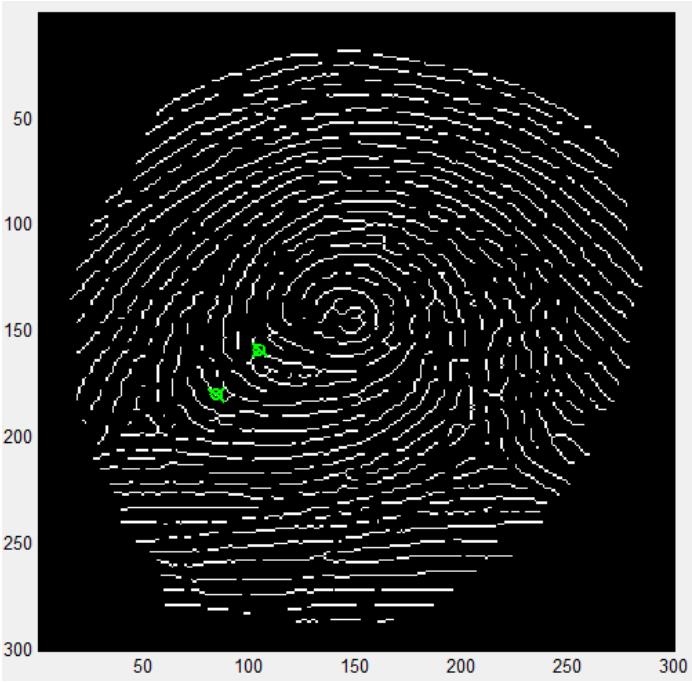

Figure 52: Reckoning of Bifurcations

3. **Validation of Terminations and Bifurcations:** Specification of the coordinate values of terminations and bifurcations is validated with the following function [127] [143]:

function Valid_Callback(figure, event, userdata)

CentX=getappdata(userdata.FPGUI,'CentX');

CentY=getappdata(userdata.FPGUI,'CentY');

CentX=getappdata(userdata.FPGUI,'CentX');

OFin=getappdata(userdata.FPGUI,'OFin');

OSep=getappdata(userdata.FPGUI,'OSep');

I=getappdata(userdata.FPGUI,'OriginalImage');

ValidGUI(I,CentX,CentY,OFin,CentX,CentY,OSep);

.....

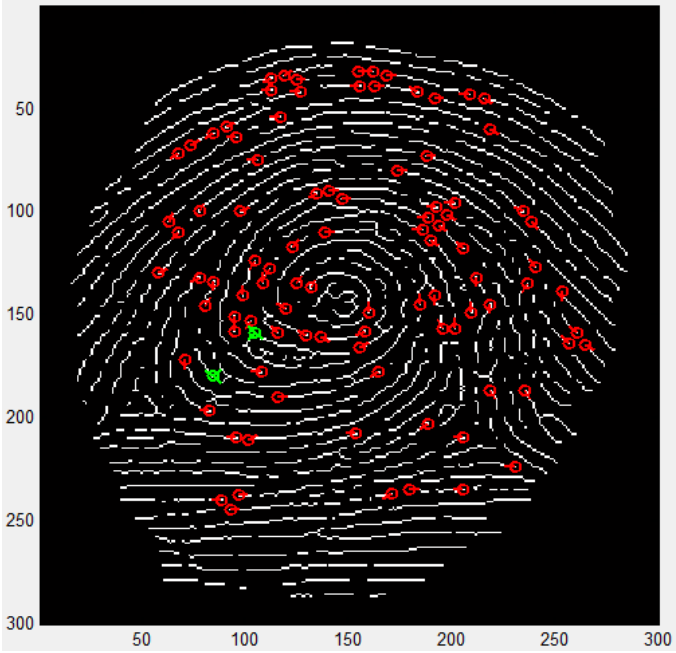

Figure 53: Specification of Terminations and Bifurcations

The white image specifies the exact location. As no one has the same minutiae point at the same location of the fingerprint so this brings uniqueness in the fingerprints of the individuals.

function ed_CreateFcn(hObject, eventdata, handles)

if ispc && isequal(get(hObject,'BkgroundColor'),
get(0,'defaultUicontrolBkgroundColor'))

set(hObject,'BkgroundColor','white');

end

.....

function WImage_Callback(hObject, eventdata, handles)

if get(hObject,'value')==1

set(handles.OImage,'value',0)

set(handles.Skel,'value',0)

end

.....

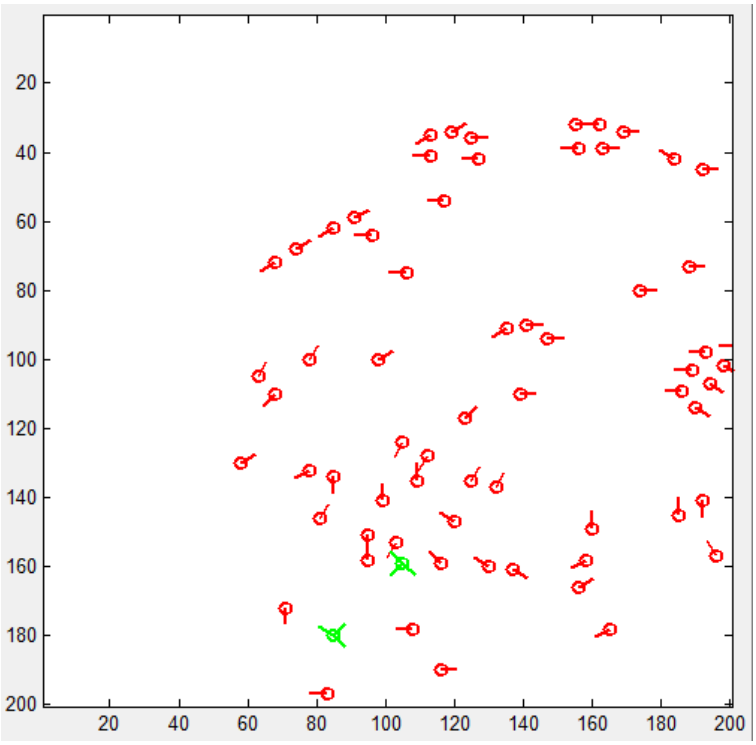

Figure 54: White Image of Terminations and Bifurcations

RNA-FINNT resulted in the augmentation of trust and privacy for legitimate user and enhancement of security over the public network.

The complete experiment results in reckoning of terminations and bifurcations. The minutiae points are extracted with RNA-FINNT and fingerprint matching is also done with RNA-FINNT. Performance evaluation and validation of RNA-FINNT is done in Chapter 6 of the thesis.

6

Performance Evaluation And Validation of RNA-FINNT

CHAPTER – 6

PERFORMANCE EVALUATION AND VALIDATION OF RNA-FINNT

Testing of RNA-FINNT is done on three different databases: real time database, existing database and noisy fingerprint database as mentioned in Section 5.4 Chapter 5. Performance Indicators False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage are set in this thesis and explained in Section 2.8 of Chapter 2. The computation of these performance indicators results in verification of the conditions to be fulfilled by RNA-FINNT. In order to validate the performance of RNA-FINNT computation of performance indicators, distortion tolerance and overall recognition accuracy of RNA-FINNT is required.

6.1 TESTING OF RNA-FINNT

The testing of RNA-FINNT is done on three different databases. The computed results for the databases results in either extraction of minutiae points but for few noisy fingerprints the extraction of minutiae points is not possible.

1. **Real Time Fingerprint Database Testing:** This database is prepared in the University with the help of the students and faculty of the University as the source. The database is concerned with the data protection and privacy issues associated with each participant so the database is not made available in public. This database is used only for the experimentation of RNA-FINNT. For the smooth testing of RNA-FINNT total 50 individuals participated. 2 impressions of each individual are considered for testing purpose. Total 100 fingerprints were used for the testing purpose. *Figure 55* represent the reckoning of terminations and bifurcations in one of the fingerprint of the real time database. The results of 10 fingerprints with extracted minutiae points are represented in *Table 10* and *Figure 56* in the form of Table and graph respectively. Testing done on real time fingerprint database represents that the fingerprints which do not have noise or distortion can be easily used for authentication purpose.

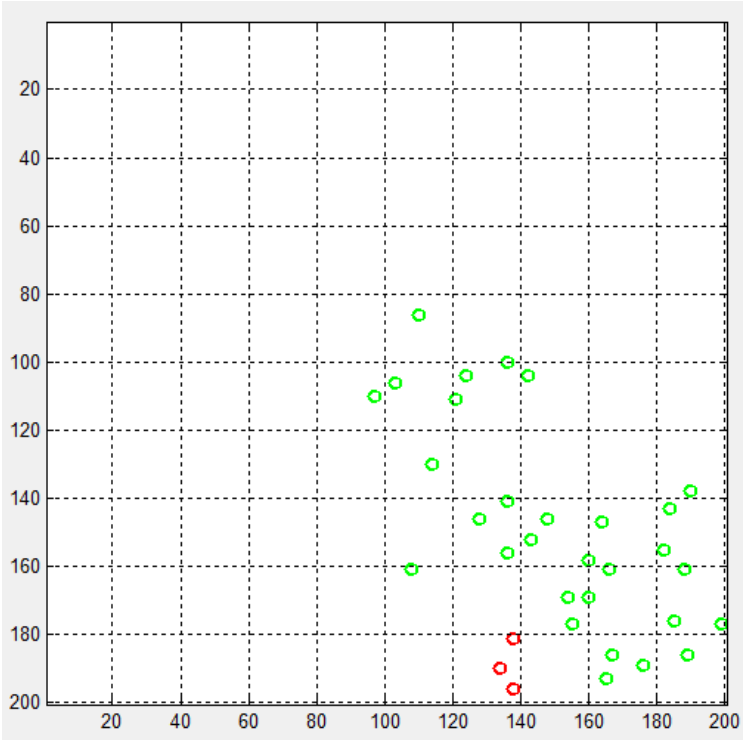

Figure 55: Extraction of Minutiae Points in Real Time Fingerprint Database

Table 10: Results of RNA-FINNT for Real Time Fingerprint Database

Real Time Fingerprint Database Results		
Fingerprint	**Reckoning of Terminations**	**Reckoning of Bifurcations**
501	15	92
502	102	4
503	30	23
504	30	24
505	76	31
506	46	5
507	39	42
508	50	35
509	75	47
510	5	32

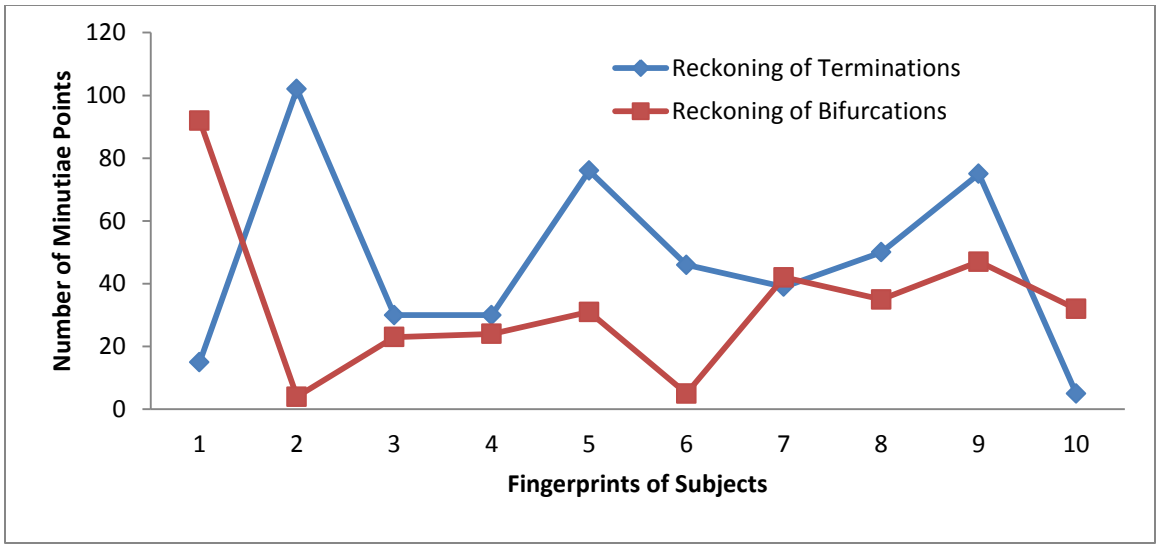

Figure 56: Graph of RNA-FINNT for Real Time Fingerprint Database

2. Existing Fingerprint Database Testing: The existing database used for testing of RNA-FINNT is FVC2000, FVC2002 and FVC2004. The databases have 80 fingerprint images in DB1_B, DB2_B, DB3_B and DB4_B respectively.

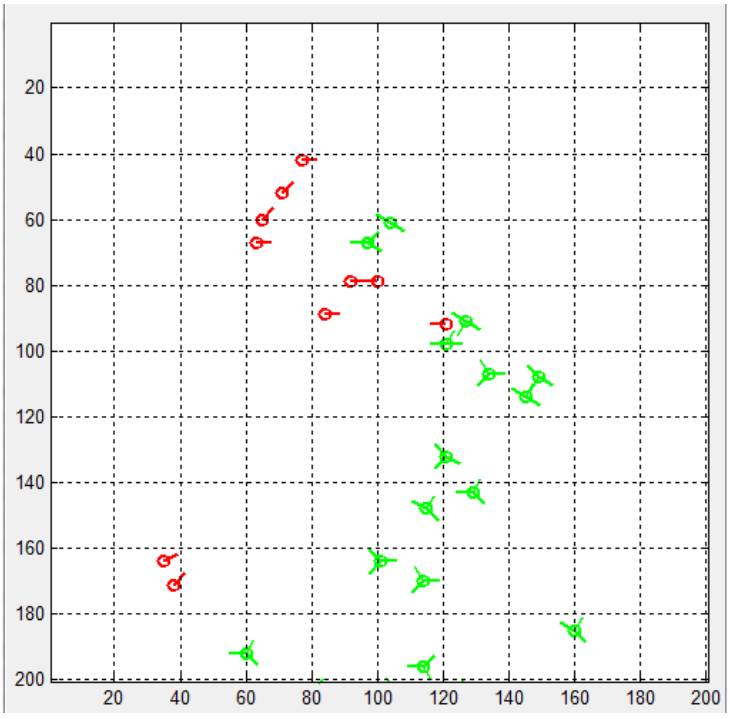

Figure 57: Extraction of Minutiae Points in Existing Fingerprint Database

While for the testing of RNA-FINNT 10 subjects are taken and 8 images per finger are considered so in total 80 fingerprint images are taken for testing. *Figure 57* represent the reckoning of terminations and bifurcations in one of the fingerprint of the existing fingerprint database. The results of 10 fingerprints with extracted minutiae points are represented in *Table 11* and *Figure 58* in the form of Table and graph respectively. Testing done on existing fingerprint database represents that the fingerprints which do not have noise or distortion can be easily used for authentication purpose.

Table 11: Results of RNA-FINNT for Existing Fingerprint Database

Existing Fingerprint Database Results		
Fingerprint	**Reckoning of Terminations**	**Reckoning of Bifurcations**
501E	5	32
502E	11	15
503E	15	25
504E	16	24
505E	30	23
506E	76	31
507E	46	5
508E	39	42
509E	75	47
510E	102	4

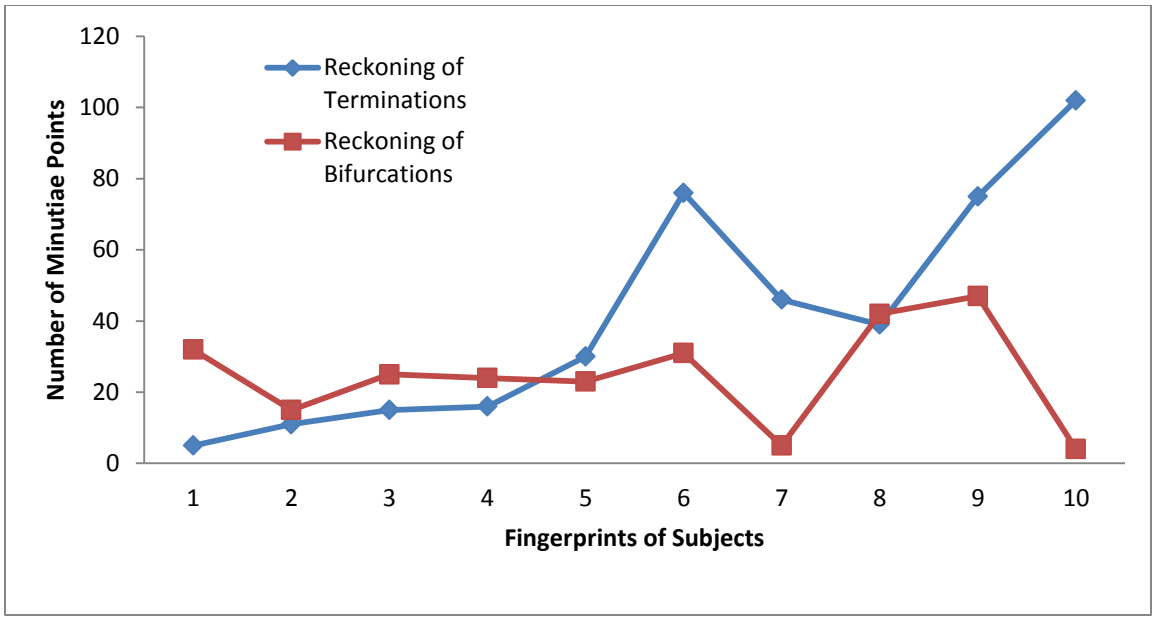

Figure 58: Graph of RNA-FINNT for Existing Fingerprint Database

3. **Noisy Fingerprint Database Testing:** The databases used for testing noisy fingerprint are FVC2000 and FVC2002 which has 80 fingerprint images in DB1_B, DB2_B, DB3_B and DB4_B respectively which has few fake or noisy fingerprint images. While for testing RNA-FINNT 10 subjects are taken 8 impressions of each fingerprint so in total 80 noisy fingerprints are tested. *Figure 59* and *Figure 60* represent the non extraction and extraction of terminations and bifurcations of one of the fingerprint of the noisy fingerprint database respectively. The results of 10 fingerprints with either extracted minutiae points or NULL values are represented in *Table 12* and *Figure 61* in the form of Table and graph respectively. Testing done on noisy fingerprint database represents that the fingerprints which do not have noise or distortion can be easily used for authentication purpose. But fingerprint which have 50% of noise ratio would give NULL value as execution.

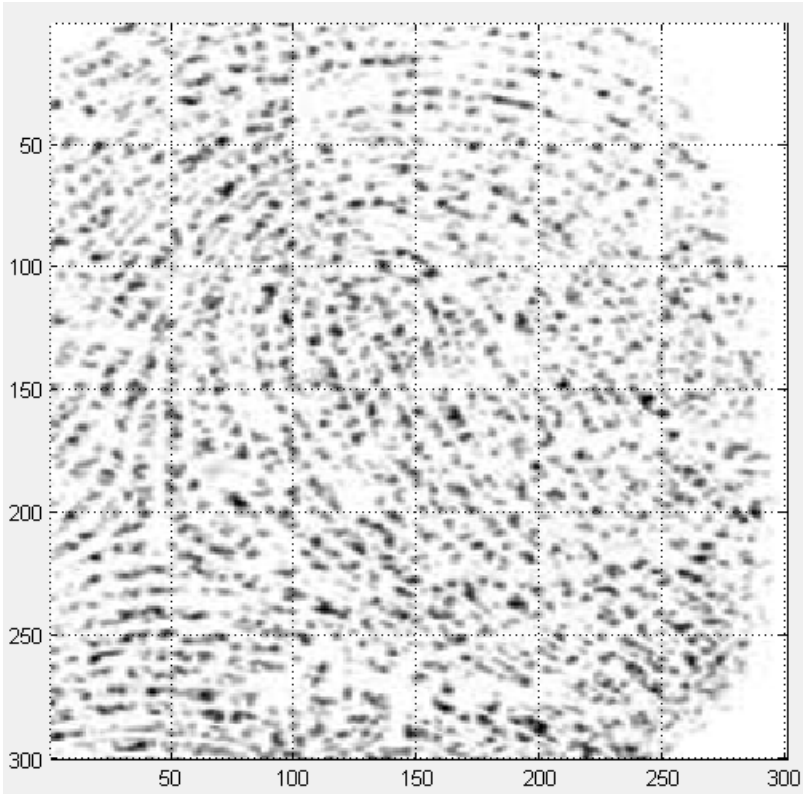

Figure 59: Non Extraction of Minutiae Points in Noisy Fingerprint Database

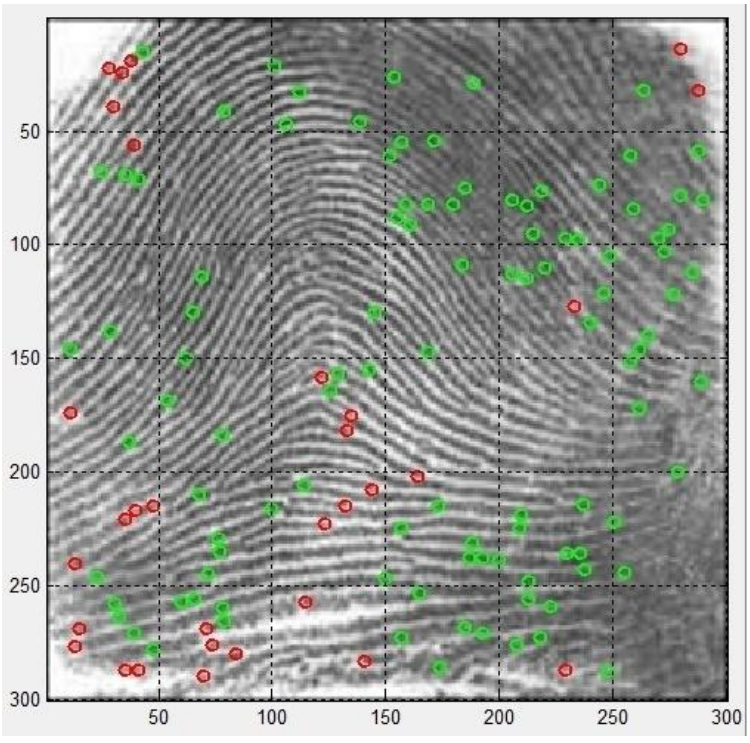

Figure 60: Extraction of Minutiae Points in Noisy Fingerprint Database

Table 12: Results of RNA-FINNT for Noisy Fingerprint Database

Noisy Fingerprint Database Results		
Fingerprint	**Reckoning of Terminations**	**Reckoning of Bifurcations**
501N	33	69
502N	32	24
503N	0	0
504N	8	49
505N	31	105
506N	0	0
507N	55	19
508N	33	46
509N	3	116
510N	0	0

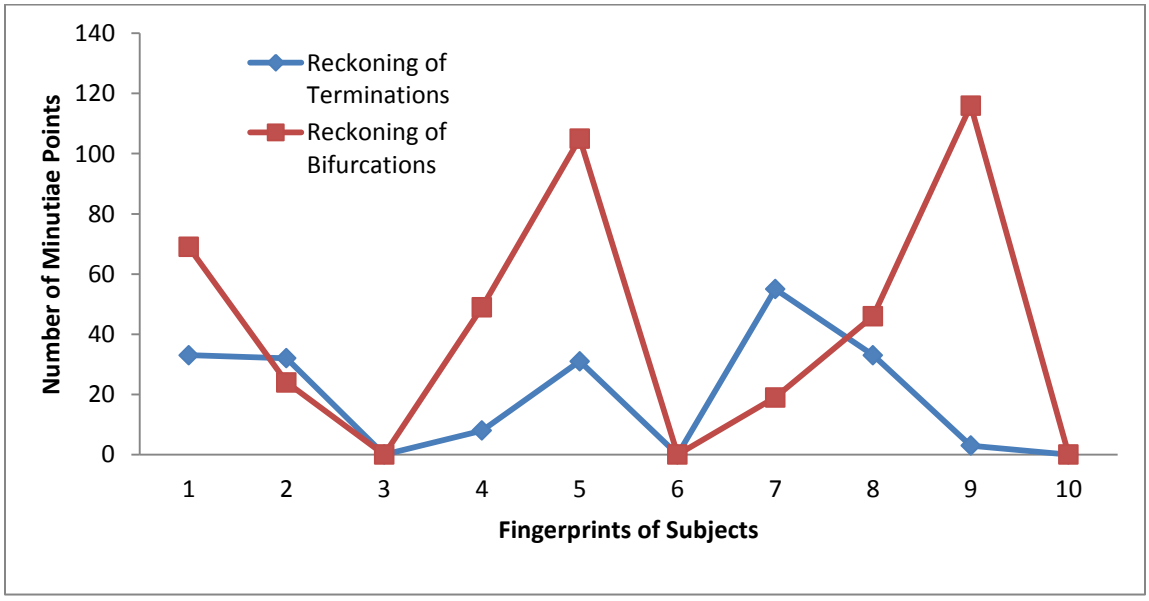

Figure 61: Graph of RNA-FINNT for Noisy Fingerprint Database

6.2 COMPUTATION OF PERFORMANCE INDICATORS

RNA-FINNT has resulted in reduction in error because it has very less angles; all grids are executed simultaneously. RNA-FINNT is evaluated on the basis of below mentioned performance indicators. The formula for computation of performance indicators are [109]:

Details of the Computation of Performance Indicators of RNA-FINNT [109]:

Total 50 subjects are taken, 2 impressions of each subject (index finger) are taken.

Number of Genuine Recognition Attempts (NGRA) = 50 X 2 = 100

Number of Imposter Recognition Attempts (NIRA) = (50 X 2) X (50 – 1) = 4900.

Table 13: Grid Wise details of Terminations and Bifurcations for first and second time extraction

First Time Extraction			Second Time Extraction		
Grid No	**501_1 Terminations**	**501_1 Bifurcations**	**Grid No**	**501_2 Terminations**	**501_2 Bifurcations**
1	2	2	1	2	1
2	2	2	2	2	1
3	0	2	3	1	1
4	1	0	4	1	0
5	0	1	5	2	0
6	2	0	6	0	1
7	0	2	7	0	1
8	1	0	8	2	1
9	2	2	9	1	2
SUM	10	11	SUM	11	8

$$Geometric\ Mean\ as\ per\ First\ Extraction = \sqrt[2]{10\ X\ 11} = 10.48$$

$$Geometric\ Mean\ as\ per\ Second\ Extraction = \sqrt[2]{11\ X\ 8} = 9.38$$

1. **False Matching Rate:** Number of successful false matches and divided by number of attempted false matches. Formula is:

$NIMS: Number\ of\ Imposter\ Matching\ Scores$

$NIRA: Number\ of\ Imposter\ Recognition\ Attempts$

$$FMR(t_1, t_2) = \frac{NIMS1 \leq t_1\ ^\wedge\ NIMS2\ \leq\ t_2}{NIRA}$$

$$FMR(t_1, t_2) = \frac{10.48\ ^\wedge 9.38}{4900} = 0.020$$

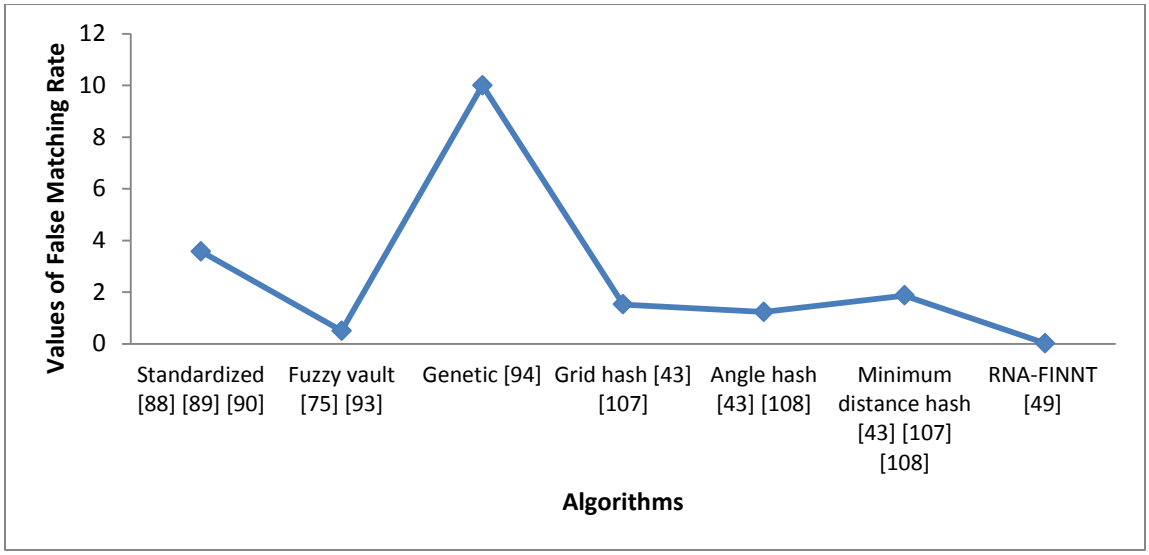

Figure 62: Comparison of False Matching Rate of RNA-FINNT

2. **Equal Error Rate:** It is the value where false match rate FMR(i) and false non match rate FNR(i) are equal.

$$EER\ Value = FMR(i) = FNR(i)$$

$$Example: FMR = 0.3638\ and\ FNR = 0.3638\ then\ EER = 0.01$$

$$EER = 0.0534\ when\ t_1 = 30\ and\ t_2 = 5$$

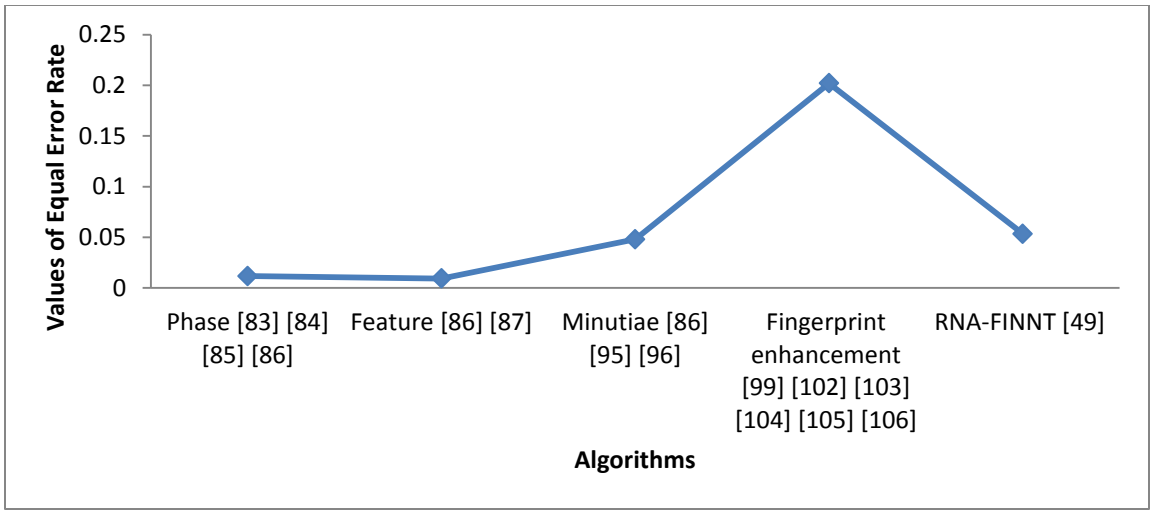

Figure 63: Comparison of Equal Error Rate of RNA-FINNT

3. **Threshold Value:** It is pre defined value and collected data is compared with this pre defined value. If conditions are met then performance is good.

$t_1 = 30$ *and* $t_2 = 5$ *at which EER is computed.*

$t_1 = 16$ *and* $t_2 = 7$ *at which Recognition Accuracy is calculated.*

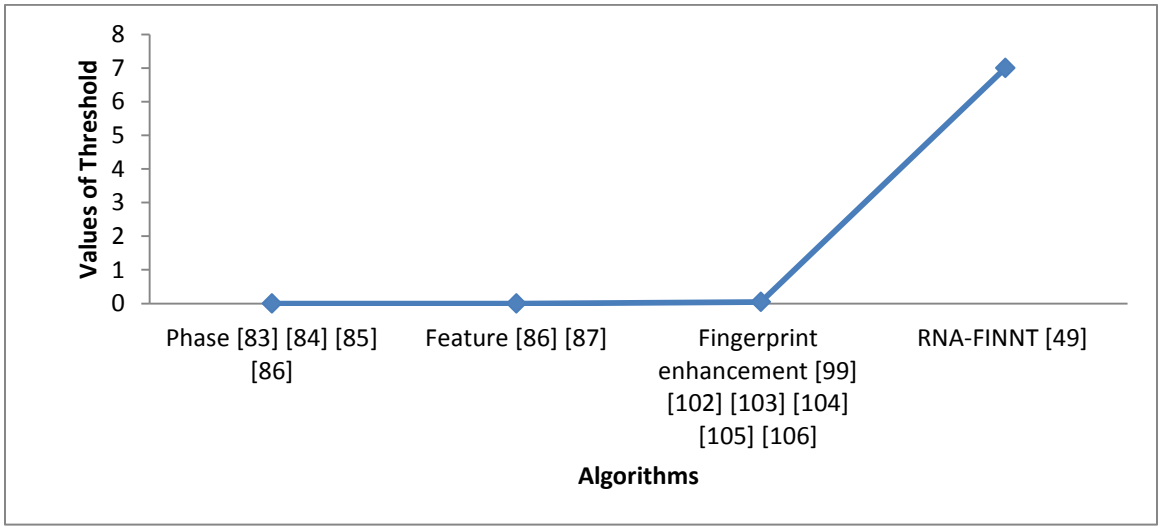

Figure 64: Comparison of Threshold Value of RNA-FINNT

4. **False Acceptance Rate:** Its computation is done on the basis of Failure to Acquire Rate (FTA gives frequency of failing to acquire a biometric feature), Failure to Capture

Rate (FTC gives the frequency of failing to capture a sample) and Failure to Extract Rate (FTX gives frequency of failing to extract a feature from sample).

$$FTA = FTC + FTX\ (1 - FTC)$$

$$NIMS: Number\ of\ Imposter\ Matching\ Scores$$

$$NIRA: Number\ of\ Imposter\ Recognition\ Attempts$$

$$FMR(t_1, t_2) = \frac{NIMS1 \leq t_1\ \hat{}\ NIMS2\ \leq\ t_2}{NIRA}$$

$$FMR(t_1, t_2) = \frac{10.48\ \hat{}\ 9.38}{4900} = 0.020$$

$$FAR = FMR\ (1 - FTA)$$

$$FAR = 0.020\ (1 - 0) =\ 0.020$$

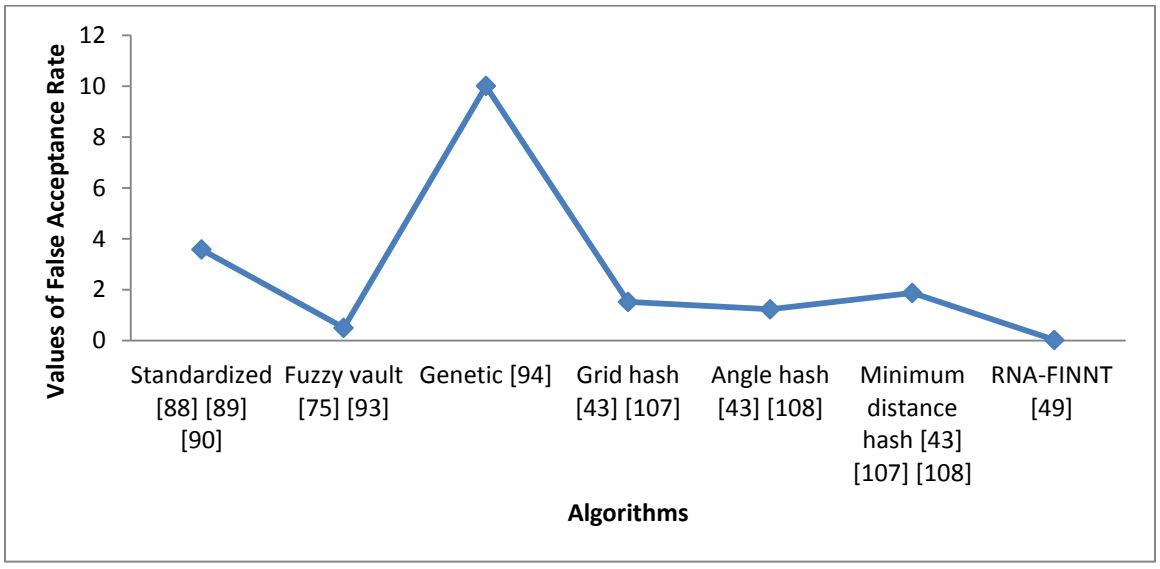

Figure 65: Comparison of False Acceptance Rate of RNA-FINNT

5. **False Reject Rate:** It is the probability of the system which fails to detect a match between matching templates of the database with input pattern.

$$FTA = FTC + FTX\ (1 - FTC)$$

$NGMS: Number\ of\ Genuine\ Matching\ Scores$

$NGRA: Number\ of\ Genuine\ Recognition\ Attempts$

$$FNR(t_1, t_2) = \frac{NGMS1 \geq t_1 v\ NGMS2\ \geq\ t_2}{NGRA}$$

$$FNR(t_1, t_2) = \frac{10.48\ v\ 9.38}{100} = 0.198$$

$$FRR = FTA + FNR\ (1 - FTA)$$

$$FRR = 0 + 0.198\ (1 - 0) =\ 0.198$$

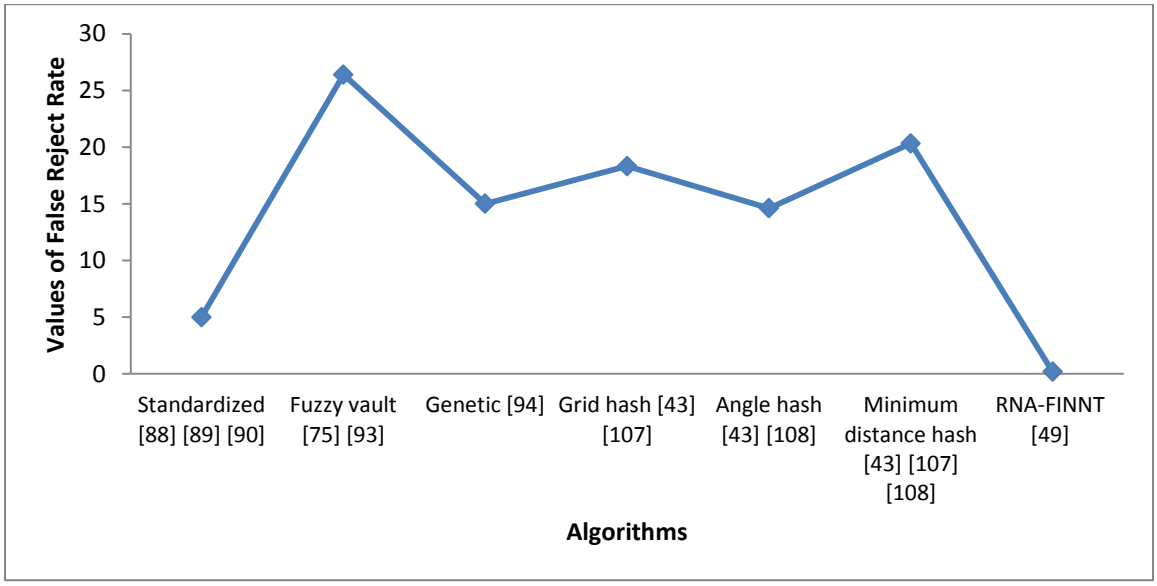

Figure 66: Comparison of False Reject Rate of RNA-FINNT

6. **False Non Match Rate:** It is the probability of the system which fails to detect a match between matching template of the database with input pattern.

$NGMS: Number\ of\ Genuine\ Matching\ Scores$

$NGRA: Number\ of\ Genuine\ Recognition\ Attempts$

$$FNR(t_1, t_2) = \frac{NGMS1 \geq t_1 v\ NGMS2\ \geq\ t_2}{NGRA}$$

$$FNR(t_1, t_2) = \frac{10.48\ v\ 9.38}{100} = 0.198$$

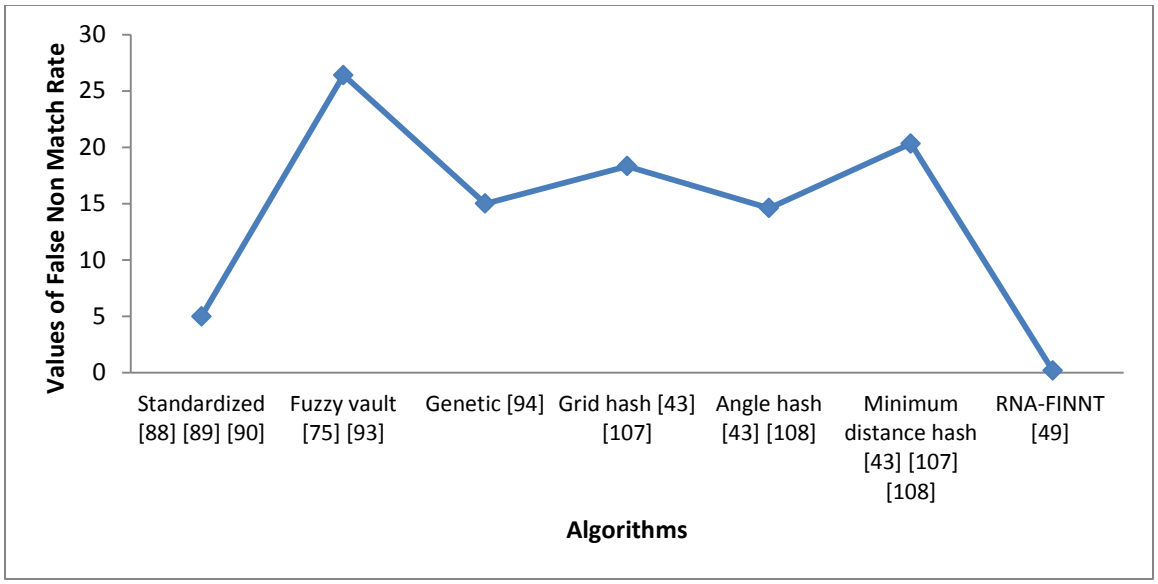

Figure 67: Comparison of False Non Match Rate of RNA-FINNT

7. **Error Percentage:** It is also called fractional difference. It is measured on the basis of experimental value as E in comparison to the true or accepted value as A.

$$Error\ \% = \frac{|E - A|}{A}$$

$$Error\ \% = \frac{|0.0534 - 0.1454|}{0.1454}$$

$$Error\ \% = 0.632$$

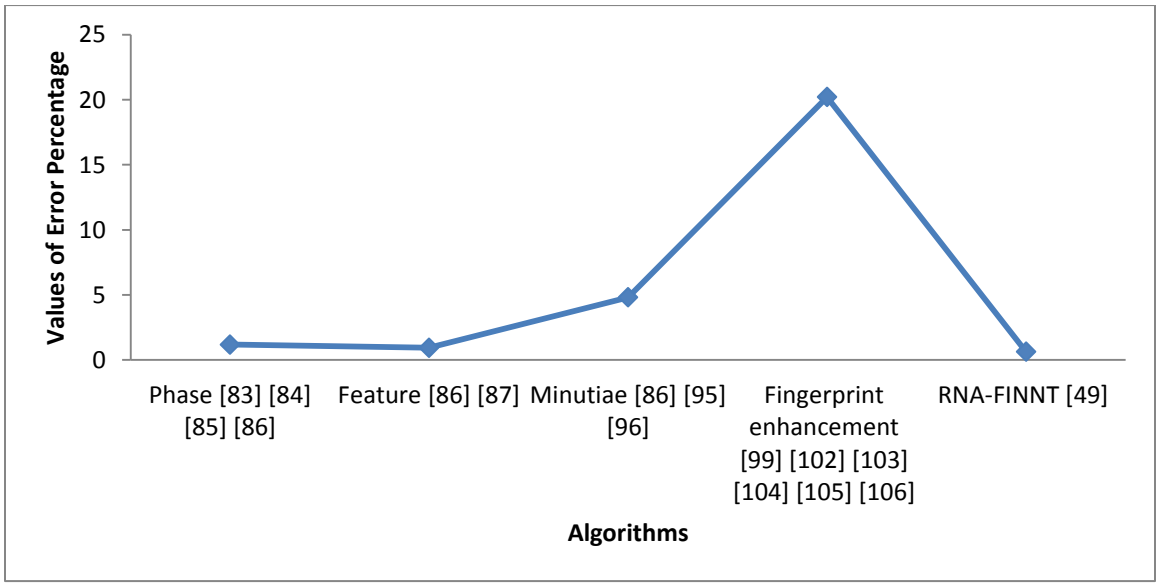

Figure 68: Comparison of Error Percentage of RNA-FINNT

Even the precision rate would result in calculating the error percentage. The average of two extracted values is taken. So the difference between error percentage is:

$$Difference\ \% = \frac{|E_1 - E_2|}{\left(\frac{E_1 + E_2}{2}\right)}$$

$$Difference\ \% = \frac{|0.0534 - 0.14541|}{\left(\frac{0.0534 - 0.14541}{2}\right)}$$

$$Difference\ \% = \frac{0.09201}{(0.046005)}$$

$$Difference\ \% = 2.0$$

The difference between the error percentages signifies that the stated algorithm performs better than the other taken in comparison. The difference of the error percentage for RNA-FINNT is 2.0.

The computed values of performance indicators would be used to verify the conditions set for RNA-FINNT. If RNA-FINNT meets those conditions then it has good performance and even overall accuracy of RNA-FINNT would also be computed. These conditions are same as Biometric Ideal Test. This test has taken 500 subjects, 5 images per finger and in total 8 fingers is considered and CASIA-FingerprintV5 is used [135]. Performance Indicators False Matching Rate, Equal Error Rate, Threshold Value, False Acceptance Rate, False Reject Rate, False Non Match Rate and Error Percentage are set in this thesis and conditions are set keeping the Biometric Ideal Test in consideration. RNA-FINNT could be ranked on the basis of these conditions. Below stated are the conditions which RNA-FINNT if fulfills then its validity is substantiated [131]:

- Error Percentage should be less than 10.
- Average Processing Time should be less than 10 seconds.
- Average Matching Time should be less than 0.1 second.

The computed values of performance indicators would help in evaluating the overall accuracy of RNA-FINNT. Above three stated conditions are verified in Section 6.4 of the thesis. If RNA-FINNT meets these conditions then the performance of it is comparable.

6.3 DISTORTION TOLERANCE OF RNA-FINNT

Distortion is to change the normal shape, form or appearance of the minutiae point. It gives unfaithful reproduction whenever any modification is done. Sometimes it refers to change or misrepresentation of data. In order to distort the fingerprint image either the minutiae points or locations and orientations could be randomly removed, replaced or disturbed [145]. Few existing algorithms use various other methods to compute the distortion tolerance of the algorithm like for deformed fingerprints local minutiae triangle based feature sets to measure similarity [146], ridge compatibility and fingerprint placement [147], Delaunay triangulation based template synthesis algorithm [148], geometric deformation is handled by using phase congruency-based information with image deformation correction algorithm [149], non linear deformations are done with elastic distortion model [150], distortion tolerance filters like summation or weighted or MINACE [151], mapping fingerprint image into a canonical representation [152], average deformation model [153][154], minutia matching algorithm [155], image mosaicking and feature mosaicking [156], average deformation model to pre-distort a template prior to matching [157], approach to unrolling and to solve the interoperability [158] and detecting fake fingerprint [159].

The computation of distortion tolerance for RNA-FINNT is done by randomly removing, replacing and disturbing the locations and orientations of the minutiae points over the fingerprints available in three databases real time fingerprint database, existing fingerprint database and noisy fingerprint database. The threshold for performing the matching with RNA-FINNT in case of distortion is pre defined as 30. It means if the number of terminations and bifurcations match for a fingerprint is greater than 30 then it gets matched otherwise no match. Three methods would be adopted to validate that RNA-FINNT has acceptable distortion tolerance which are randomly removing, replacing and disturbing the minutiae points [160].

For Fingerprint #105 in real time fingerprint database the self match rate varies from 3 to 7 in total 8 impressions of the fingerprint. Distortion tolerance of RTFD #105 is 76.56%. Table 14 demonstrates the results. Average distortion tolerance for real time fingerprint database is 70.83%.

Table 14: Distortion Tolerance of RNA-FINNT for Fingerprint RTFD #105

Distortion Tolerance of RNA-FINNT for Real Time Fingerprint Database RTFD #105												
Number of Minutiae Points	106	73	59	40	84	79	75	65	THV	SMR	DT	Distortion Tolerance of RNA-FINNT for Real Time Database Fingerprint #105 is: (49/64)*100 = 76.56%
Real Time Database Fingerprint #105	1	2	3	4	5	6	7	8				
1	50	65	19	35	47	68	54	25	30	6/8	75	
2	65	45	45	32	45	45	25	34	30	7/8	87.5	
3	78	65	35	21	67	67	46	56	30	7/8	87.5	
4	35	23	46	23	78	43	56	35	30	6/8	75	
5	43	45	56	22	46	35	67	45	30	7/8	87.5	
6	12	52	24	34	25	24	78	23	30	3/8	37.5	
7	67	14	43	35	47	65	54	43	30	7/8	87.5	
8	46	35	14	21	57	67	43	44	30	6/8	75	

1. Distortion tolerance of RNA-FINNT when minutiae are removed: Three fingerprint images are taken from real time fingerprint database #101, 102 and 103. The self match rate of these fingerprints varies from 1 to 8 and distortion tolerance is collective 54.16%. But by removing 10 minutiae points in the validation process the distortion tolerance remains 50%. Not much marginal difference is observed. Table 15 demonstrates the result and validates that RNA-FINNT is capable for acceptable distortion tolerance even when randomly few minutiae points are removed.

Table 15: Distortion Tolerance of RNA-FINNT when Minutiae are removed

Distortion Tolerance of RNA-FINNT for Real Time Database when Minutiae are removed												
Real Time Database Impressions	1	2	3	4	5	6	7	8	THV	SMR	DT	Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are removed is: (13/24)*100 = 54.16%
101	10	37	28	15	15	9	15	10	30	1/8	12.5	
102	76	72	43	72	55	55	57	71	30	8/8	100	
103	111	109	82	61	13	11	23	23	30	4/8	50	
Number of Minutiae Points Removed	10	10	10	10	10	10	10	10				Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are removed is: (12/24)*100 = 50%
101	0	27	18	5	5	0	5	0	30	0/8	0	
102	66	62	33	62	45	45	47	61	30	8/8	100	
103	91	99	72	51	3	1	13	13	30	4/8	50	

2. Distortion tolerance of RNA-FINNT when minutiae are replaced: Three fingerprint images are taken from real time fingerprint database #101, 102 and 103. The self match rate of these fingerprints varies from 1 to 8 and distortion tolerance is collective 54.16%. But by replacing 30 minutiae points in the validation process the distortion tolerance remains 33.3%. There is marginal difference in the initial value and the value obtained after replacing minutiae points. Table 16 demonstrates the result and validates that RNA-FINNT is capable for acceptable distortion tolerance even when randomly few minutiae points are replaced.

Table 16: Distortion Tolerance of RNA-FINNT when Minutiae are replaced

Distortion Tolerance of RNA-FINNT for Real Time Database when Minutiae are replaced												
Real Time Database Impressions	1	2	3	4	5	6	7	8	THV	SMR	DT	Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are replaced is: (13/24)*100 = 54.16%
101	10	37	28	15	15	9	15	10	30	1/8	12.5	
102	76	72	43	72	55	55	57	71	30	8/8	100	
103	111	109	82	61	13	11	23	23	30	4/8	50	
Number of Minutiae Points Replaced	30	30	30	30	30	30	30	30				Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are replaced is: (8/24)*100 = 33.3%
101	0	7	0	0	0	0	0	0	30	0/8	0	
102	46	42	13	42	25	25	27	41	30	4/8	50	
103	81	79	52	31	0	0	0	0	30	4/8	50	

3. Distortion tolerance of RNA-FINNT when minutiae are disturbed: Three fingerprint images are taken from real time fingerprint database #101, 102 and 103. The self match rate of these fingerprints varies from 1 to 8 and distortion tolerance is collective 54.16%.

Table 17: Distortion Tolerance of RNA-FINNT when Minutiae are disturbed

Distortion Tolerance of RNA-FINNT for Real Time Database when Minutiae are disturbed												
Real Time Database Impressions	1	2	3	4	5	6	7	8	THV	SMR	DT	Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are disturbed is: (13/24)*100 = 54.16%
101	10	37	28	15	15	9	15	10	30	1/8	12.5	
102	76	72	43	72	55	55	57	71	30	8/8	100	
103	111	109	82	61	13	11	23	23	30	4/8	50	
Number of Minutiae Points Disturbed	20	20	20	20	20	20	20	20				Distortion Tolerance of RNA-FINNT for Real Time Database when minutiae are disturbed is: (11/24)*100 = 45.8%
101	0	17	8	0	0	0	0	0	30	0/8	0	
102	56	52	23	52	35	35	37	51	30	7/8	87.5	
103	91	89	62	41	0	0	3	3	30	4/8	50	

But by disturbing 20 minutiae points in the validation process the distortion tolerance remains 45.8%. There is the marginal difference of approximately 10% after disturbing minutiae points. Table 17 demonstrates the result and validates that RNA-FINNT is capable for acceptable distortion tolerance even when randomly few minutiae points are disturbed.

Overall this validation process for distortion tolerance substantiates that RNA-FINNT has acceptable capability of distortion tolerance even when the minutiae points are removed, replaced or disturbed.

6.4 VALIDATION WITH ERROR PERCENTAGE, AVERAGE PROCESSING AND MATCHING TIME

In order to validate that RNA-FINNT is providing best accuracy following conditions are to be met by the algorithm. These conditions are taken from Biometric Ideal Test 2014 [135]. The conditions for substantiating the overall performance of RNA-FINNT are:

1. Error Percentage should be less than 10.

$$Error\ \% = \frac{|E - A|}{A}$$

$$Error\ \% = \frac{|0.0534 - 0.1454|}{0.1454}$$

$$Error\ \% = 0.632$$

The error percentage of RNA-FINNT is 0.632 which is less than 10 so RNA-FINNT has met the first condition. Even the precision rate would result in calculating the error percentage. The average of two extracted values is taken. So the difference between error percentage is:

$$Difference\ \% = \frac{|E_1 - E_2|}{\left(\frac{E_1 + E_2}{2}\right)}$$

$$Difference\ \% = \frac{|0.0534 - 0.14541|}{\left(\frac{0.0534 - 0.14541}{2}\right)}$$

$$Difference\ \% = \frac{0.092011}{(0.046005)}$$

$$Difference\ \% = 2.0$$

The difference between the error percentages signifies that the stated algorithm performs better than the other taken in comparison. The difference of the error percentage for RNA-FINNT is 2.0. The error percentage of RNA-FINNT is 0.632 which is less than 10 resulted in fulfillment of condition by RNA-FINNT and filling of the research gap 4.

2. Average Processing Time should be less than 10 seconds.

These results are implemented using matrix laboratory as program platform used in the University. Programs are tested on Intel(R) Core(TM) i3-2310M CPU @ 2.10 GHz computer with 4GB RAM in the laboratory.

Table 18: Average Processing Time of RNA-FINNT

S.No	Activity	Processing Time (Seconds)
1	Fingerprint Minutiae Points Extraction	2.98
2	Dividing Fingerprint into Grid of Squares	0.61
3	Minutiae Points thinning, orientation and validation	2.55
	Processing Time	6.14

The processing time for RNA-FINNT is 6.14 seconds which is less then 10 seconds so RNA-FINNT has met the second condition also. The average processing time of RNA-FINNT is 6.14 seconds which is less than 10 seconds resulted in fulfillment of the condition by RNA-FINNT and filling of the research gap 5.

3. Average Matching Time should be less than 0.1 seconds

Table 19: Average Matching Time of RNA-FINNT

S.No	Activity	Processing Time (Seconds)
1	Fingerprint Minutiae Points Extraction	0.0012
2	RNA-FINNT Fingerprint Match	0.0004
3	Overall Recognition Accuracy (Section 6.5)	0.00005
	Matching Time	0.00165

The matching time taken by RNA-FINNT is 0.00165 seconds which is less than 1 second. So RNA-FINNT has met the third condition also. The average matching time of RNA-FINNT is 0.00165 seconds which is less than 1 second resulted in fulfillment of the condition by RNA-FINNT and filling of the research gap 6.

6.5 OVERALL RECOGNITION ACCURACY OF RNA-FINNT

In order to compute the overall recognition accuracy all the combinations of threshold are to be evaluated. The threshold value which gives the minimum difference between False Acceptance Rate (*FAR*) and False Rejection Rate (*FRR*) should be considered for computing the overall recognition accuracy. From the all set combinations of threshold the combination of (16,7) gives the minimum difference between False Acceptance Rate (*FAR*) and False Rejection Rate (*FRR*) which is *FAR* = 0.2109 and *FRR* = 0.2105 at the threshold values as $t_1 = 16$, $t_2 = 7$.

$$True\ Acceptance\ Rate\ (TAR) = 1 - False\ Acceptance\ Rate\ (FAR)$$

$$TAR = 1 - FAR = 1 - 0.2109 = \ 0.7891$$

$$True\ Rejection\ Rate\ (TRR) = 1 - False\ Rejection\ Rate\ (FRR)$$

$$TRR = 1 - FRR = 1 - 0.2105 = 0.7895$$

$$Overall\ recognition\ accuracy\ is\ the\ average\ of\ TAR\ and\ TRR\ i.e \approx 78\%.$$

If the difference between *FAR* and *FRR* is higher then also the average has to be considered.

6.6 EMBEDDED RNA-FINNT IN BIOMETRIC MACHINES AUGMENTS SECURITY

Various identity authentication paramaters like smart cards, passwords and fingerprints etc are used by the biometric machines and the authenticatioon and verification of the human is possible through these patterns of input. Even sometimes feature extraction is helpful for authentication or verification process. Study for enhancement of security through biometrics with various algorithms and techniques resulted that they are not able to withstand the main security requirements and are vulnerable to attacks as mentioned in the thesis Section 2.1 of Chapter 2 [161]. But RNA-FINNT has resulted in comparable performance. The result stated are verified by an experiment performed on human beings for authentication and verification process in which extraction of the minutiae points is done through RNA-FINNT and the recognition match rate of the human being is better

[161]. So implementation of RNA-FINNT into the biometric machines will help in fortifying the security through biometrics.

This Chapter of the thesis substantiates the good performance of RNA-FINNT through the following ways:

1. Testing of RNA-FINNT with the help of real time, existing and noisy fingerprint database.
2. Computation of the performance indicators resulted that error percentage of RNA-FINNT is less than 10 which fulfills the research gap 4.
3. Computation of the distortion tolerance of RNA-FINNT resulted acceptable level.
4. Average processing and matching time of RNA-FINNT is 6.14 and 0.00165 respectively which fulfills the research gap 5 and 6.
5. Overall recognition accuracy of RNA-FINNT is above average.
6. Implementation of RNA-FINNT into the biometric machines will help in fortifying the security through biometrics.

Overall the above process and methodology resulted in substantiating the good performance of RNA-FINNT.

7

Conclusion And Future Work

CHAPTER – 7

CONCLUSION AND FUTURE WORK

When RNA-FINNT is implemented then it has resulted in Ideal Authentication Scheme which maintains confidentiality, authentication, traffic analysis and integrity. RNA-FINNT has resulted in reduction in error percentage, calculation of less number of angles, diminution in error approximation, and removal of dependency over the core points and fortification of security over the public network. RNA-FINNT has met all the set conditions for verification of its good performance. The computation of overall recognition accuracy is also done from the values of performance indicators evaluated. This thesis generated new algorithm for image processing. The process presented here is quiet advantageous because the computation of the fingerprint image is running in parallel with all grid of squares. This thesis has enhanced the knowledge and learning in the field of security and privacy and computing methodologies with main focus on authentication through biometrics [162] [163]. It is expected a user who desires more security and reduction in error percentage would surely prefer RNA-FINNT [164] [165]. But it has potential of further work and improvement also in the field of authentication through fingerprints instead of passwords [166] [167]. The thesis has achieved the objectives mentioned in Chapter 1.

1. The thesis has contributed in advancing science with respect to pattern recognition in the areas of security and privacy and computer methodologies by focusing on authentication process. Fingerprint is used for authentication of the user.

2. Thesis has resulted in deriving a new fingerprint hash algorithm that is Reduced Number of Angles Fingerprint Hash Algorithm (RNA-FINNT) as mentioned in Chapter 4. The algorithm resulted in diminution in the percentage or approximation of error resulting in Ideal Authentication Scheme as mentioned in Chapter 4.

3. Augmentation of trust and privacy of legitimate user by computing the values of RNA-FINNT on the basis of performance indicators and improving the overall recognition accuracy of the RNA-FINNT as mentioned in Chapter 6.

The thesis has accomplished all the research gaps as stated in the Chapter 3 Table 6.

Table 20: Accomplishments of the Research Gaps

S.No	*Analysis of Literature Review*	*Research Gap*	*Accomplishment of Research Gaps*
1	Table 1	Mutual authentication required when fingerprint is used as identity authentication parameter with new algorithm using hash based scheme	RNA-FINNT implemented for mutual authentication with virtualization in the multi server environment for enhanced security.
2	Table 2	Need to generate a new fingerprint hash algorithm with reduction in error percentage	Reduction in error percentage with RNA-FINNT is 4%.
3	Table 3	Need to derive a new fingerprint hash based algorithm by overcoming the drawbacks of the existing algorithms and diminution in error approximation	Error approximation when extraction of minutiae points is done with RNA-FINNT is 33%
4	Table 4	New fingerprint hash algorithm should have error percentage less than 10	The error percentage of RNA-FINNT is 0.632 which is less than 10.
5	Table 5	New fingerprint hash algorithm should have average processing time less than 10 seconds	The average processing time of RNA-FINNT is 6.14 seconds which is less than 10 seconds.
6	Table 5	New fingerprint hash algorithm should have average matching time as less than 0.1 seconds	The average matching time of RNA-FINNT is 0.00165 seconds which is less than 1 second.

Although all research gaps mentioned are accomplished in the thesis but this process has few drawbacks and there is the possibility of improvement of the thesis. Below mentioned are few drawbacks.

Drawbacks of the Process

1. Lengthy in computation.
2. The fingerprint having 50% of noise ratio then RNA-FINNT will give NULL value.
3. Many values are to be computed before finalizing the performance of the algorithm.

7.1 POSSIBLE IMPROVEMENT OF THE THESIS

The process used for RNA-FINNT could also be used in other identity authentication devices. It could be said that the real result of this thesis is not simply a new fingerprint algorithm but enhanced security level and fortified authentication process also.

The improvement or extension possible in RNA-FINNT is to:

1. Assimilation of fingerprint with password could be done to add one more tier of security.
2. Fingerprint with noise ratio more than 50% should be able to extract minutiae points.
3. Increase or improve the overall recognition accuracy of the algorithm.

In future the overall recognition accuracy of the algorithm could be improved and even assimilation of fingerprint with password could be done. The future of RNA-FINNT states that many applications could be executed with it with enhanced results. At present also there exist many applications which are being executed with fingerprints so RNA-FINNT could be used with all those applications for reduction in error percentage, diminution in error approximation and enhanced security.

7.2 FUTURE WORK

The future work of the thesis would be the extension of the work in the domain of hardware which states that in future the RNA-FINNT Chip could be prepared. Any complex digital system may be broken down into component gates and memory elements by successively subdividing the system in a hierarchical manner [168]. To do this, a

specific set of abstractions have been developed to describe integrated electronic systems. This divides the system in three distinct design domains [169] [170]:

- **Behavioral Domain** (This domain specifies what a particular system does)
- **Structural domain** (This domain specifies in order to achieve the prescribed behavior how entities are connected together)
- **Physical domain** (This domain specifies how to actually build a structure which has the required connectivity to implement that prescribed behavior)

Each design domain may have **variety of levels of abstraction.** Digital Integrated system is often partitioned into five interrelated tasks: architecture design, microarchitecture design, logic design, circuit design, and physical design [169] [170].

- **Architecture** describes the functions of the system. For example, the x86 microprocessor architecture specifies the instruction set, register set, and memory model
- **Microarchitecture** describes how the architecture is partitioned into registers and functional units. 80386, 80486, Pentium, Pentium II, Pentium III, Pentium 4, Celeron, Cyrix Mil, AMD K5, and Athlon are all microarchitectures offering different performance / transistor count tradeoffs for the x86 architecture
- **Logic** describes how functional units are constructed. Example: various logic designs for a 32-bit adder in the x86 integer unit include ripple carry, carry lookahead, and carry select
- **Circuit** design describes how transistors are used to implement the logic. Example, a carry lookahead adder can use static CMOS circuits, domino circuits, or pass transistors. The circuits can be tailored to emphasize high performance or low power
- **Physical** design describes the layout of the chip

These elements are inherently interdependent. To deal with these interdependencies, microarchitecture, logic, circuit, and physical design must occur, at least in part, in parallel.

An alternative way of viewing design partitioning is done with the **Y-chart**. The radial lines on the Y-chart represent three distinct design domains: behavioural, structural, and physical. These domains can be used to describe the design of almost any artefact and thus form a very general taxonomy for describing the design process. Within each domain there are a number of levels of design abstraction that start at a very high level and descend eventually to the individual elements that need to be aggregated to yield the top level function (i.e., in the case of chip design and transistors) [169] [170].

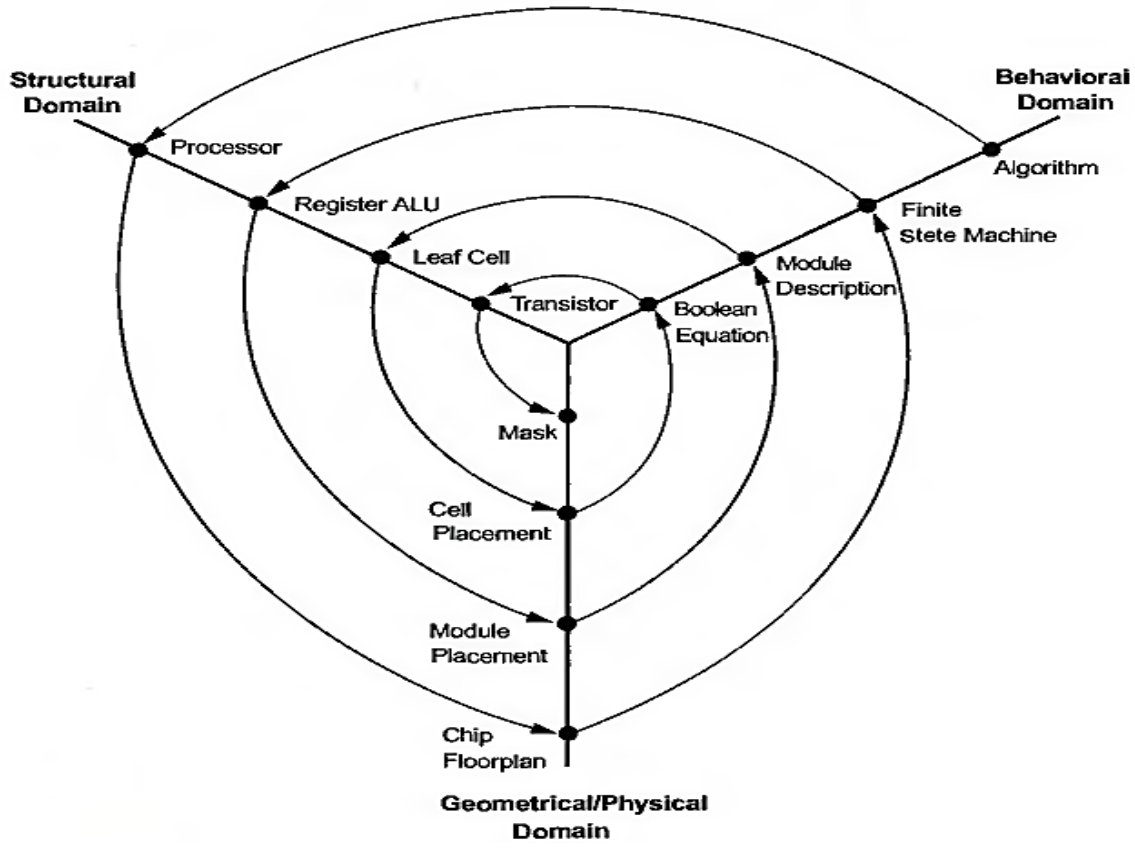

Figure 69: Y-Chart for preparing RNA-FINNT Chip

Steps required for preparing Chip of RNA-FINNT based upon the design partitioning with the help of Y-chart are as follows [169] [170]:

Step 1:

We have algorithm RNA-FINNT ready In Behavioral Domain.

Digital design of RNA-FINNT has to be prepared in Structural domain. Eg: Adder, Comparator etc.

Chip floor plan of digital design of RNA-FINNT has to be prepared in Physical domain.

Step 2:

Finite state machine of RNA-FINNT has to be prepared in Behavioral Domain.

Logic units of digital design of RNA-FINNT have to be prepared in Structural domain. eg: Gates, Registers etc.

Module placement of all the logic units has to be prepared in Physical domain.

Step 3:

Module description would be done in Behavioral Domain.

Leaf cell would be prepared in Structural domain eg: AND, OR gates etc.

Cell placement of each leaf cell has to be done in Physical domain.

Step 4:

Boolean equation of RNA-FINNT would be prepared in Behavioral Domain.

Transistor level circuit would be prepared in Structural domain.

Mask of the circuit would be prepared for projection in Physical domain.

Step 5:

Projection on Silicon wafer would be done using the Mask for further fabrication steps.

Step 6:

Fabrication of the Silicon chip would be done using different chip fabrication steps.

Step 7:

RNA-FINNT Chip is ready.

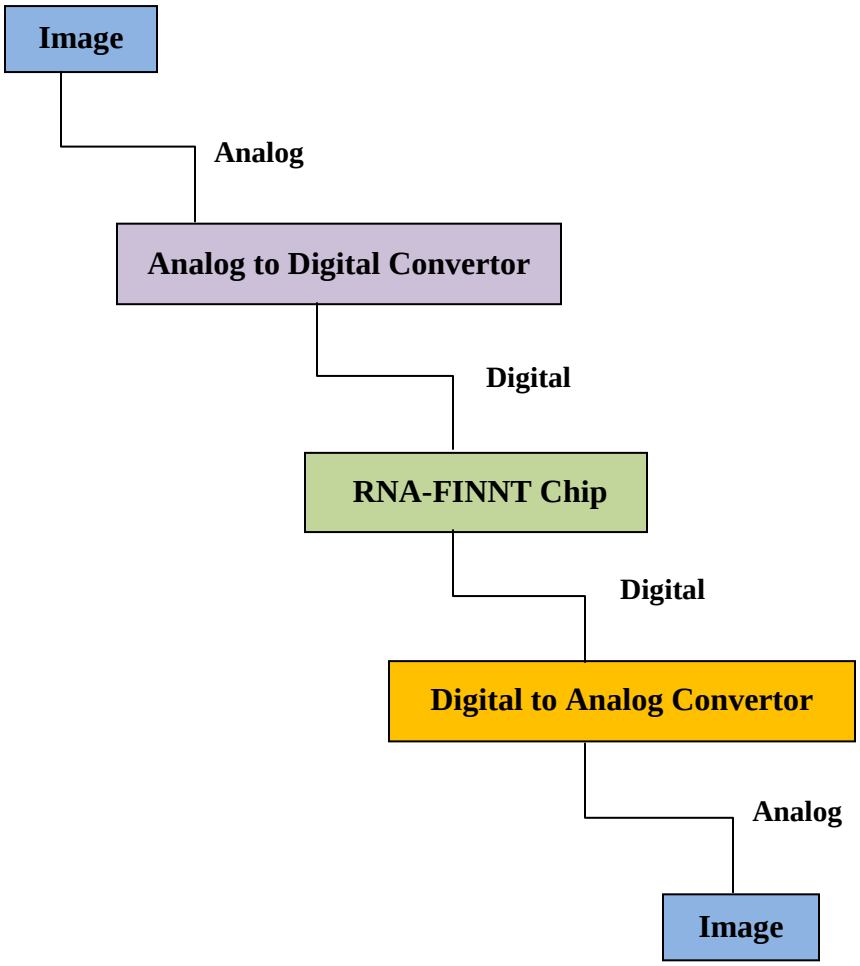

Figure 70: Process flow of RNA-FINNT

Figure 70 has shown the complete process flow for execution of RNA-FINNT algorithm with the hardware implementation of RNA-FINNT Chip.

Future extension of the thesis in the domain of hardware would be as follows:

1. Preparing the Boolean equation in the behavioral domain.
2. Transistor level circuit preparation in Structural domain.
3. Preparing Mask of the circuit of RNA-FINNT for projection in Physical domain.
4. Fabrication of the Silicon chip using different chip fabrication steps for making RNA-FINNT Chip.

Despite of this possible improvement or extension this thesis has resulted in success. The knowledge and experience gained from accomplishing this thesis will certainly be helpful for future enhancement in security and privacy and computer vision or authentication.

Bibliography

BIBLIOGRAPHY

1. Association for Computing Machinery. (2012). ACM [Online]. Available: http://www.acm.org/about/class/class/2012

2. Ratha, N.K.; Connell, J.H.; Bolle, R.M., "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal* , vol.40, no.3, pp.614,634, 2001 doi:10.1147/sj.403.0614, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5386935&isnumber=5386925

3. M. Bellare, D. Pointcheval, and P. Rogaway, 'Authenticated Key Exchange Secure Against Dictionary Attacks', In Eurocrypt '00, LNCS 1807, pp. 139-155, Springer-Verlag, Berlin, 2000.

4. M. Bellare and P. Rogaway, 'The AuthA Protocol for Password-Based Authenticated Key Exchange', Contributions to IEEE P1363, March 2000. URL: http://grouper.ieee.org/groups/1363/

5. M. Bellare and P. Rogaway, "Random Oracles Are Practical: a Paradigm for Designing Efficient Protocols," In Proc. of the 1st CCS, pp. 62-73, ACM Press, New York, 1993.

6. S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks," In Proc. of the Symposium on Security and Privacy, pp. 72-84, IEEE, 1992.

7. C. Boyd, P. Montague, and K. Nguyen, 'Elliptic Curve Based Password Authenticated Key Exchange Protocols', In ACISP '01, LNCS 2119, pp. 487-501, Springer-Verlag, Berlin, 2001.

8. T. Berners-Lee, R. T. Fielding, H. F. Nielsen, J. Gettys, and J. Mogul, 'Hypertext transfer protocol – HTTP/1.1.Internet Request for Comment RFC 2068', Jan. 1997.

9. W. Diffie and M. Hellman, ‘New directions in cryptography’, *IEEE Transactions on Information Theory*, IT-22(6):644–654, Nov. 1976.

10. D. P. Jablon, ‘Strong password-only authenticated key exchange’, *Computer Communication Review*, 26(5):5–26, Sep 1996.

11. T. Wu, ‘The secure remote password protocol’, In *Symposium on Network and Distributed Systems Security (NDSS ’98)*, pp. 97–111, San Diego, California, Mar.1998. Internet Society.

12. E. Bresson, O. Chevassut, and D. Pointcheval, “Security Proofs for an Efficient Password-Based Key Exchange,” in 10th ACM Conference on Computer and Communications Security, pp. 1-2,October 27, 2003, Washington, DC, USA.

13. Peter Buhler, Thomas Eirich, Michael Steiner and Michael Waidner, “Secure Password-Based Cipher Suite for TLS,” in Network and Distributed Systems Security Symposium (NDSS 2000), San Diego, California, February 2000.

14. Craig A. Huegen. (1998). Network-Based Denial of Service Attacks [Online]. Available: www.pentics.net/ denial-of-service/presentations/.../ 19980209_dos.pp...

15. Kim Davis. (2008,October). DNS Cache Poisoning Vulnerability Explanation and Remedies [Online]. Available: www.iana.org/about/.../davies-viareggio-entropyvuln-081002.pdf, Viareggio Italy.

16. David A. McGrew and Scott R. Fluhrer. (2005, May 31). Multiple forgery attacks against Message Authentication Codes [Online]. Available: eprint.iacr.org/2005/ 161.pdf, Cisco Systems, Inc.

17. Alberto Ornaghi, Marco Valleri, “Man In the Middle Attacks Demos,” in BlackHat Conference, USA 2003

18. Renaud Bidou. Ping Of Death [Online]. Available: www.iv2-technologies.com/DOSAttacks.pdf

19. IP Spoofing [Online]. Available: www.sans.org/reading.../introduction-ip-spoofing_959, United States, SANS

20. Christoph Hofer, Rafael Wampfler. IP Spoofing [Online]. Available: rvs.unibe.ch/teaching /cn%20applets/IP_Spoofing/IP%20Spoofing.pdf

21. Alec Yasinsac, Sachin Goregaoker, 'An Intrusion Detection System for Security Protocol Traffic', Department of Computer Science, Florida State University,p-12,1996

22. Ping Broadcast [Online]. Available: en.wikipedia.org/wiki/Broadcast_radiation

23. Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal. (2004). CompChall: Addressing Password Guessing Attacks [Online]. Available: http://eprint.iacr.org /2004/136.pdf

24. Larry Seltzer. (2009). Spoofing Server-Server Communication: How You Can Prevent It [Online]. Available: www.verisign.com/ssl/ssl.../ssl.../whitepaper-ev-prevent-spoofing.pdf

25. Shray Kapoor. Session Hijacking Exploiting TCP, UDP and HTTP Sessions [Online]. Available: infosecwriters.com/text_resources/.../SKapoor_Session Hijacking.pdf

26. Rajaram Ramasamy, Amutha Prabakar Muniyandi, 'New Remote Mutual Authentication Scheme using Smart Cards', Transactions on Data Privacy, Volume 2, p-141-152,2009

27. Smurf Attack [Online]. Available: http://en.wikipedia.org/wiki/Smurf_attack

28. Minho Kim and Cetin Kaya Koc, 'A Simple Attack on a Recently Introduced Hash-Based Strong-Password Authentication Scheme', International Journal of Network Security, Vol.1, No.2, PP.77–80, Sep. 2005

29. Teardrop Attack Detection [Online]. Available: https://www.daxnetworks.com/Dax/Products/Switch/DTS_T5C_24G_24GT.htm

30. DongGook Park, Colin Boyd and Sang-Jae Moon. Forward Secrecy and Its application to Future Mobile Communications Security [Online]. Available: www.dgpark6.com/ Down/pkc2000_FwdSec.pdf

31. Mutual Authentication. [Online]. Available: en.wikipedia.org/wiki/ Mutual_authentication

32. Network Security [Online]. Available: http://ftp.utcluj.ro/pub/users/dadarlat/ retele_master/prez3-sec.pdf

33. Roots of Trusted Interfaces and the User Experience [Online]. Available: crypto.stanford.edu/TIPPI/first/slides/inskeep.ppt

34. Tom Davis, 'RSA Encryption', http://www.geometer.org/mathcircles,October 10, 2003

35. Brent Waters, Allison Bishop, 'El Gamal Encryption CS395T Advanced Cryptography', Lecture 3,27th January 2009

36. ElGamal Encryption Example [Online]. Available: www.informatics.indiana.edu/ markus/i400/ lecture7.ppt

37. Kumar Mangipudi and Rajendra Katti, 'A Hash-based Strong Password Authentication Protocol with User Anonymity', International Journal of Network Security, Vol.2, No.3, PP.205–209, May 2006 (http://isrc.nchu.edu.tw/ijns/)

38. Hanjae Jeong, Dongho Won and Seungjoo Kim, 'Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol', Information Security Group, Journal Of Information Science and Engineering 26, 1845-1858 (2010)

39. Gartner Research Association [Online]. Available: https://www.gartner.com/doc/ 363557/research-collection-worldwide-chip-card

40. K.Kaur and G. Geetha, 'Survey for Generating an Ideal Password Authentication Scheme Which Results In Fortification of Transport Layer Security Protocol',

International Journal of Computer Science and Information Technologies, Vol.3, Issue.2, PP.3608–3614, March-April 2012 (http://www.ijcsit.com/ijcsit-v3issue2.php)

41. Revival of Biometrics in Banking: Heralding a New Era in mPayments [Online]. Available: http://www.tcs.com/SiteCollectionDocuments/White-Papers/ Biometrics-Banking-0614-1.pdf

42. Basic Types of fingerprints [Online]. Available: http://www.odec.ca/ projects/2004/fren4j0/public_html/ fingerprint_patterns.htm

43. Sahil Goyal and Mayank Goyal, 'Generation of hash functions from fingerprint scans', October 2011

44. Secured Shell Protocol and Public Key Infrastructure [Online]. Available: http://www.ietf.org/rfc/rfc4716.txt

45. SSL Essentials: Technology, Applications, Advantages, Disadvantages [Online]. Available: http://apps1.eere.energy.gov/buildings/publications/pdfs/ssl/dowling_ssl_essentials_07-16-07.pdf

46. SSL VPN Security [Online]. Available: http://www.cisco.com/web/about/ security/intelligence/05_08_SSL-VPN- Security.html

47. Basic Types of fingerprints [Online]. Available: http://www.odec.ca/projects/ 2004/ren4j0/public_html/fingerprint_patterns.htm

48. Fingerprint Matching [Online]. Available: http://members.fortunecity.com/ julzjerg/finger.htm

49. Kuljeet Kaur and G.Geetha.Article, 'Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter', International Journal of Computer Science Issues, Vol.9, Issue.2, No.2, pp.188-193,March 2012.

50. Kuljeet Kaur and G.Geetha. Article, ‘Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters’, International Journal of Computer Applications, 42(6):36-42, March 2012. Published by FCS, NY, USA.

51. T. Chang, “Texture analysis of digitized fingerprints for singularity detection,” in Proc. 5th Int. Conf. Pattern Recognition, 1980, pp. 478–480.

52. J. Canny, ‘A computational approach to edge detection’, IEEE Trans. Pattern Anal. Machine Intell., vol. PAMI-8, no. 6, pp. 679–698, 1986.

53. D. K. Isenor and S. G. Zaky, ‘Fingerprint identification using graph matching’, Pattern Recognit., vol. 19, no. 2, 1986.

54. Q. Xiao and Z. Bian, “An approach to fingerprint identification by using the attributes of feature lines of fingerprint,” in Proc. 7th ICPR, Paris, France, 1986, pp. 663–665.

55. B. M. Mehtre, N. N. Murthy, and S. Kapoor, ‘Segmentation of fingerprint images using the directional image’, Pattern Recognit., vol. 20, no. 4, pp. 429–435, 1987.

56. L. O’Gorman and J. V. Nickerson, ‘An approach to fingerprint filter design’, Pattern Recognit., vol. 22, no. 1, pp. 29–38, 1989.

57. A. K. Hrechak and J. A. McHugh, ‘Automated fingerprint recognition using structural matching’, Pattern Recognit., vol. 23, no. 8, 1990.

58. A. C. Bovik, M. Clark, and W. S. Geisler, ‘Multichannel texture analysis using localized spatial filters’, IEEE Trans. Pattern Anal. Machine Intell., vol. 12, pp. 55–73, Jan. 1990.

59. J. Bigun, G. H. Granlund, and J.Wiklund, ‘Multidimensional orientation estimation with applications to texture analysis and optical flow’, IEEE Trans. Pattern Anal. Machine Intell., vol. 13, pp. 775–790, Aug. 1991.

60. A. K. Jain and F. Farrokhnia, ‘Unsupervised texture segmentation using gabor filters’, Pattern Recognit., vol. 24, no. 12, pp. 1167–1186, 1991.

61. N. Ansari, M. H. Chen, and E. S. H. Hou, ‘A genetic algorithm for point pattern matching’, in Dynamic, Genetic, and Chaotic Programming, B. Souˆcek and the IRIS Group, Eds. New York: Wiley, 1992, ch. 13.

62. D. B. G. Sherlock, D. M. Monro, and K. Millard, “Fingerprint enhancement by directional Fourier filtering,” Proc. Inst. Elect. Eng. Visual Image Signal Processing, vol. 141, no. 2, pp. 87–94, 1994

63. A. Sherstinsky and R. W. Picard, “Restoration and enhancement of fingerprint images using -lattice a novel nonlinear dynamical system,” in Proc. 12th ICPR-B, Jerusalem, Israel, 1994, pp. 195–200.

64. G. T. Candela, P. J. Grother, C. I. Watson, R. A. Wilkinson, and C. L. Wilson, ‘PCASYS: A pattern-level classification automation system for fingerprints’, National Institute of Standards and Technology, Gaithersburg, MD, NIST Tech. Rep. NISTIR 5647, Aug. 1995.

65. N. Ratha, S. Chen, and A. K. Jain, ‘Adaptive flow orientation based feature extraction in fingerprint images’, Pattern Recognit., vol. 28, no. 11, pp. 1657–1672, 1995.

66. R. Bahuguna, “Fingerprint verification using hologram matched filterings,” in Proc. Biometric Consortium Eighth Meeting, San Jose, CA, June 1996.

67. M. Hartman, “Compact fingerprint scanner techniques,” in Proc. Biometric Consortium 8th Meeting, San Jose, CA, June 1996.

68. D. Maio and D. Maltoni, ‘Direct gray-scale minutiae detection in fingerprints’, IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 27–40, Jan. 1997.

69. A. K. Jain, L. Hong, and Y. Kulkarni, “A multimodal biometric system using fingerprint, face, and speech,” in Proc. Int. Conf. Audio- Video-Based Biometric Person Authentication, Washington, DC, Mar. 22–24,1999, pp. 182–187.

70. Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharat Pankanti, ‘Filterbank-based fingerprint matching’, IEEE Transactions on Image Processing, vol. 9, no. 5,pp. 846–859, May 2000.

71. J. K. Lee, S. R. Ryu, and K. Y. Yoo, ‘Fingerprint-based remote user authentication scheme using smart cards’, Electronics Letters, vol. 38, no. 12, pp. 554–555, 2002.

72. H. S. Kim, S. W. Lee, and K. Y. Yoo, ‘ID-based password authentication scheme using smart cards and fingerprints’, ACM Operating Systems Review, vol. 37, no. 4, pp. 32–41, 2003.

73. M. K. Khan and J. Zhang, ‘An efficient and practical fingerprint-based remote user authentication scheme with smart cards’, in Information Security Practice and Experience, vol. 3903 of Lecture Notes in Computer Science, pp. 260–268, 2006.

74. Y. J. Chang, W. Zhang, and T. Chen, ‘Biometrics-based cryptographic key generation’, in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '04), pp. 2203–2206, June 2004.

75. Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,” in Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '04), Interlaken, Switzerland, May 2004.

76. H. Khazaei and A. Mohades, “Fingerprint matching and classification using an onion layer algorithm of computational geometry,” in Proceedings of the 13th International CSI Computer Conference, 2008.

77. A. Panchenko, L. Niessen, A. Zinnen, and T. Engel, “Website fingerprinting in onion routing based anonymization networks,” in Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, pp. 103–114, ACM, 2011.

78. S. Mazaheri, B. S. Bigham, and R. M. Tayebi, ‘Fingerprint matching using an onion layer algorithm of computational geometry based on level 3 features’, Communications in Computer and Information Science, vol. 166, no. 1, pp. 302–314, 2011.

79. A. Baig, A. Bouridane, F. Kurugollu, and G. Qu, ‘Fingerprint-Iris fusion based identification system using a single hamming distance matcher’, International Journal of Bio-Science and Bio-Technology, vol. 1, no. 1, pp. 47–58, 2009.

80. G. Cao, Y. Mei, Z. Mao, and Q. S. Sun, ‘Fingerprint matching using local alignment based on multiple pairs of reference minutiae’, Journal of Electronic Imaging, vol. 18, no. 4, Article ID 043002, 2009.

81. Q. Wang, G. Liu, Z. Guo, J. Guo, and X. Chen, “Structural fingerprint based hierarchical filtering in song identification,” in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '11), pp. 1–4, IEEE, 2011.

82. R.Josphineleela and M.Ramakrishnan , ‘A New approach of altered fingerprints detection on the altered and normal fingerprint Database’, Indian Journal of Computer Science and Engineering , Vol. 3, No.6, pp. 818-821, 2013.

83. K. Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima, and Koji Kobayashi, ‘A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints’, IEEE, vol. II, pp. 33–36, 2005.

84. K. Ito, Ayumi Morita, Takafumi Aoki, Hiroshi Nakajima, Koji Kobayashi, and Tatsuo Higuchi, ‘A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching’, Springer LNCS 3832, pp. 316–325, 2006.

85. Ito, Izumi, and Hitoshi Kiya, ‘DCT sign-only correlation with application to image matching and the relationship with phase-only correlation’, Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on. Vol. 1. IEEE, 2007.

86. Koichi Ito, Ayumi Morita, Takafumi Aoki, Hiroshi Nakajima,Koji Kobayashi, and Tatsuo Higuchi, "A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching," Conference: Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, DOI: 10.1007/11608288_43

87. W. Forstner, 'A Feature Based Correspondence Algorithm for Image Matching', Int. Arch. of Photogrammetry, pp.26-3/3, 1986.

88. Ren Qun, Tian Jie, He Yuliang and Cheng Jiangang, 'Automatic Fingerprint Identification Using Cluster Algorithm', IEEE, 1051-4651/02, 2002

89. Feng. Jianjiang, Anil K. Jain, "FM Model Based Fingerprint Reconstruction from Minutiae Template," Proceedings of the Third International Conference on Advances in Biometrics, Springer-Verlag Berlin, Heidelberg, pp. 544-553, 2011

90. Le Hoang Thai, Ha Nhat Tam, 'Fingerprint Recognition using Standardized Fingerprint Model', International Journal of Computer Science Issues, Vol.7, Issue 3, No.7, May 2010.

91. Lee, Dongjae, et al., 'Fingerprint fusion based on minutiae and ridge for enrollment', Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2003.

92. Manhua Liu, Xudong Jiang, Alex Chichung Kot, 'Efficient fingerprint search based on database clustering', Pattern Recognition 40 (2007) 1793–1803

93. Nandakumar, Karthik, Anil K. Jain, and Sharath Pankanti, 'Fingerprint-based fuzzy vault: Implementation and performance', Information Forensics and Security, IEEE Transactions on 2.4 pp 744-757, 2007.

94. Xuejun Tan, Bir Bhanu, 'Fingerprint matching by genetic algorithms', Pattern Recognition 39 (Elsevier), pp. 465 – 477, 2006.

95. Sudha S. Ponnarasi,M. Rajaram, 'Impact of Algorithms for the Extraction of Minutiae Points in Fingerprint Biometrics', Journal of Computer Science 8(9), pp.1467-1472, 2012.

96. Davide Maltoni, Dario Maio,Anil K Jain, Salil Prabhakar, The Handbook of Fingerprint Recognition. Springer, 2003.

97. Jinwei Gu, Jie Zhou, 'Analysis of Singular Points in Fingerprints based on Topological Structure and Orientation Field', Springer-Verlag Berlin Heidelberg, pp. 1 – 8, 2007.

98. Limin Liu and Tian-Shyr Dai, 'A Reliable Fingerprint Orientation Estimation Algorithm', Journal of Information Science and Engineering, Vol. 27,pp. 353-368, 2011.

99. H B Kekre and V A Bharadi, 'Fingerprint Core Point Detection Algorithm Using Orientation Field Based Multiple Features', International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15

100. Jie Zhou, Jinwei Gu, and David Zhang, 'Singular Points Analysis in Fingerprints Based on Topological Structure and Orientation Field', Springer-Verlag Berlin Heidelberg , LNCS 4642, pp. 261–270, 2007.

101. Ali Ismail Awad and Kensuke Baba, 'Singular Point Detection for Efficient Fingerprint Classification', International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1):1-7.2012

102. Hong, Lin, Yifei Wan, and Anil Jain, 'Fingerprint image enhancement: algorithm and performance evaluation', Pattern Analysis and Machine Intelligence, IEEE Transactions on 20.8 (1998): 777-789.

103. Jain, Anil, and Sharath Pankanti, Fingerprint classification and matching, Handbook for Image and Video Processing, 2000.

104. Greenberg, Shlomo, et al., "Fingerprint image enhancement using filtering techniques," Pattern Recognition, 2000. Proceedings. 15th International Conference on. Vol. 3. IEEE, 2000.

105. Kumar, Ajay, et al., 'Personal verification using palmprint and hand geometry biometric', Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2003.

106. Shaikh Mohammedsayeemuddin, Sima K Gonsai, Dharmesh Vandra, ‘Efficient Fingerprint Image Enhancement Algorithm Based on Gabor Filter’, International Journal of Research in Engineering and Technology, Volume: 03 Issue: 04, 809-813, 2014

107. Jin, Zhe, et al., "Generating revocable fingerprint template using polar grid based 3-tuple quantization technique," Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on. IEEE.

108. Chama, Nimitha, "Fingerprint Image Enhancement and Minutiae Extraction," University of Clemson, 2003.

109. Amira Saleh, Ayman Bahaa and A. Wahdan, Fingerprint Recognition, Advanced Biometric Technologies, http://cdn.intechopen.com/pdfs-wm/17747.pdf, 2011

110. Virtualization in SQL Server (2008) [Online]. Available: www.microsoft.com/en-us/server-cloud/...server/hyper-v.aspx

111. Setting Connections in SQL Server [Online]. Available: www.connectionstrings.com/sql-server-2008

112. How to connect SQL Server Instances using SQL Server Management Studio [Online]. Available: kb.discountasp.net/.../how-to-connect-to-sql-server-2008-using-sql-s...

113. Active Connections in SQL Server [Online]. Available: www.jasonholden.com/blog/.../SQL-Server-2008-Active-Connection

114. Linked Server Components [Online]. Available: http://msdn.microsoft.com/en-us/library/ms188279.aspx

115. Configuration of Linked Servers [Online]. Available: http://msdn.microsoft.com/en-us/library/ms188279.aspx

116. Adding SQL Server Instances [Online]. Available: stackoverflow.com/.../how-do-i-add-a-sql-server-2008-service-instan...

117. Windows Server Virtualization [Online]. Available: www.windowsnetworking.com/.../Understanding-Windows-Server-2...

118. Linked Servers in SQL Servers in 2008 [Online]. Available: www.execsql.com/ post/linked-servers-in-sql-server-2005

119. Multiple Instances in SQL Server [Online]. Available: itknowledgeexchange.techtarget.com/sql-server//single-instance-vs-m...

120. Kaur, K, Dr.G.Geetha, 'Virtualization of Multi Server Environment results in Enhanced Communication and Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.3: 4101-4108, May-June 2012.

121. Moler, Cleve (2004). The origins of Matlab. Matlab News & Notes. Cleve's Corner [Online]. Available: www-format: URL:www.mathworks.se/ company/newsletters/news_notes/clevescorner/dec04.html?s_cid=wiki_matlab_3.

122. Vector Graphic (2012). The Tech Terms Computer Dictionary [Online]. Available: www-format: URL:http://www.techterms.com/definition/ vectorgraphic.

123. Cube of RGB color model (2010). Wikimedia Commons [Online]. Available: www-format: URL:www.mathworks.se/company/newsletters/news_notes/clevescorner /dec04.html ?scid=wiki_matlab_3.

124. Bitmap (2010). WiseGEEK clear answers for common questions [Online]. Available: www-format: URL:http://www.wisegeek.com/what-is-a-bitmap-image.htm.

125. Comparison of RGB and CMYK color systems (2010). Wikimedia Commons [Online]. Available: URL:http://commons.wikimedia.org/wiki/File:RGB_and_ CMYK_comparison.png.

126. Ready-built colormaps from Matlab's Image Processing Toolbox (2012). Math-Works Documentation [Online]. Available: URL:http://www.mathworks.se/help /techdoc/ref/colormap.html.

127. Kaur, K. and G.Geetha, "Reckoning Minutiae Points with RNA-FINNT Augments Trust and Privacy of Legitimate User and Ensures Network Security in the Public Network," Fifth International Conference on Networks and Communications (NETCOM - 2013), Chennai (Tamil Nadu, India), December, 2013.

128. K. Kaur, G.Geetha, 'Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to enhance Network Security', Journal of Information Security - JIS, ISSN 2153-1242 Volume 4, Number 4: 197-202, 2013.

129. Symmetric hash functions for fingerprint minutiae [Online]. Available: http://www.biometrics.org/ bc2004/Presentations/Conference/.../Sergey.pdf

130. Kareem Kamal A.Ghany, Mahmood A.Moneim,Neveen I.Ghali, Aboul Ella Hassanien, Hesham A. Hefny, 'A Symmetric Bio Hash function based on Fingerprint Minutiae and Principal curves approach', ICMET- 2011. http://ebooks.asmedigitalcollection.asme.org/content.aspx?bookid=481&sectionid =38789895

131. K. Kaur and G. Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," Proc. of the International Conference on Advances in Computer Science and Electronics Engineering — CSEE 2013 at New Delhi, India, ISBN: 978-981-07-5461-7 doi: 10.3850/ 978-981-07-5461-7_12, (p.55-59), 24th Feb, 2013. New Delhi, India

132. Banerjee, N., et. Al., "MATCH: A MATLAB Compiler for Configurable Computing Systems," Technical Report, Center for Parallel and Distributed Computing, Northwestern University, August 1999.

133. J. Davis II, M. Goel, C. Hylands, B. Kienhuis, E. A. Lee, J. Liu, X. Liu, L. Muliadi, S. Neuendorffer, J. Reekie, N. Smyth, J. Tsay and Y. Xiong, "Overview of the Ptolemy Project," Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA 94720, July 1999. (ERL Technical Memorandum UCB/ ERL No. M99/37

134. Mathworks, Inc.: MATLAB 5.3 Fact Sheet Natick, MA, (1999) [Online]. Available: http://www.coursehero.com/file/p361706/6-Mathworks-Inc-MATLAB-53-Fact-Sheet-Natick-MA-1999-7-Research-Systems-Inc/

135. Biometric Ideal Test[Online]. Available: http://biometrics.idealtest.org/2014/CCFP2014.jsp

136. FVC2000. (2009). [Online]. Available: http://bias.csr.unibo.it/fvc2000/download.asp

137. FVC2002. (2009). [Online]. Available: http://bias.csr.unibo.it/fvc2002/download.asp

138. FVC2004. (2009). [Online]. Available: http://bias.csr.unibo.it/fvc2004/download.asp

139. Atsushi Sugiura, Yoshiyuki Koseki, 'A User Interface Using Fingerprint Recognition- Holding commands and Data Objects on Fingers', C & C Media Research Laboratories, NEC Corporation, Japan 1998.

140. Raffaele Cappelli, Dario Maio,Davide Maltoni, James L. Wayman, Anil K. Jain, 'Performance Evaluation of Fingerprint Verification Systems', IEEE Transactions on Pattern Analysis and Machine Learning, Vol.28,No.1,January 2006.

141. Qijun Zhao, Lei Zhang, David Zhang, Nan Luo, 'Direct Pore Matching for Fingerprint Recognition', Biometrics Research Center, Hong Kong 2009.

142. Jianjiang Feng, Jie Zhou, 'A Performance Evaluation of Fingerprint Minutiae Descriptors', IEEE 2011.

143. Anil K. Jain, Jianjiang Feng, 'Latent Fingerprint Maching', IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.33, No.1, January 2011.

144. Chin-Chen Chang, Chih-Chiang Tsou, Yung- Chen-Chou, "A remediable image authentication scheme based on feature extraction and clustered VQ," PCM'07 Proceedings of the multimedia 8th Pacific Rim conference on Advances in multimedia information processing, 2007(http://dl.acm.org/citation.cfm?id=1779525)

145. Qinghai Gao, Xiaowen Zhang, ‘A Study of Distortion Effects on Fingerprint Matching’, Computer Science and Engineering, 2(3): 37-42,doi:10.5923/ j.computer.20120203.06, 2012

146. X. Chen, J. Tian, X. Yang, and Y. Zhang, ‘An algorithm for distorted fingerprint matching based on local triangle feature set’, IEEE Transactions on Information Forensics and Security, vol.1, pp.169-177, 2006.

147. K. Cao, X. Yang, X. Tao, P. Li, Y. Zang, and J. Tian, ‘Combining features for distorted fingerprint matching’, Journal of Network and Computer Applications, vol.33, pp.258–267, 2010.

148. T. Uz, G. Bebis, A. Erol, and S. Prabhakar, ‘Minutiae-based template synthesis and matching for fingerprint authentication’, Computer Vision and Image Understanding, pp. 979-992, 2009.

149. R. Singh, M. Vatsa, and A. Noore, ‘Improving verification accuracy by synthesis of locally enhanced biometric images and deformable model’, Signal Processing, vol.87, pp.2746–2764, 2007.

150. R. Cappelli, D. Maio, and D. Maltoni, “Modelling plastic distortion in fingerprint images,” Proc. Second International Conference on Advances in Pattern Recognition, pp. 369-376, March 2001.

151. C. Watson, P. Grother, D. Cassasent, “Distortion-tolerant filter for elastic-distorted fingerprint matching,” Proc. SPIE Optical Pattern Recognition, pp.166–174, 2000.

152. A. Senior and R. Bolle, ‘Improved Fingerprint Matching by Distortion Removal’, IEICE Transaction on Information and Systems, vol.84, no.7, pp.825-831, July 2001.

153. A. Ross, S. Dass, A. Jain, ‘A deformable model for fingerprint matching,’ Pattern Recognition, vol. 38, pp.95-103, 2005.

154. A. Ross, S. Dass, and A. Jain, 'Fingerprint warping using ridge curve correspondences', IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.28, no.1, pp.19-30, January 2006.

155. A. Bazen and S. Gerez, 'Fingerprint matching by thin-plate spline modelling of elastic deformations', Pattern Recognition, vol. 36, pp.1859-1867, 2003.

156. A. Ross, S. Shah, and J. Shah, "Image versus feature mosaicking: a case study in fingerprints," Proc. SPIE, 620208-1 – 620208-12, 2006.

157. Y. Chen, D. Dass, A. Ross, and A. Jain, "Fingerprint deformation models using minutiae locations and orientations," Proc. IEEE Workshop on Applications of Computer Vision, pp.150–155, 2005.

158. Q. Zhao, A. Jain, G. Abramovich, "3D to 2D fingerprints: Unrolling and distortion correction," International Joint Conference on Biometrics, pp. 1-8, October 2011.

159. A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, 'Fake finger detection by skin distortion analysis', IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006.

160. Qinghai Gao, Xiaowen Zhang, 'A study of Distortion effects on Fingerprint Matching', Computer Science and Engineering 2012, 2(3): 37-42 February 2012, DOI: 10.5923/j.computer.20120203.06

161. K. Kaur, G. Geetha, 'Pattern recognition by embedded reduced number of angles fingerprint algorithm in biometric machines augments security', Inderscience International Journal of Computer Applications in Technology Special Issue on Advances in Networking and Signal Processing for Social Security, Vol.51, No.2, pp.131 – 144, April 2015, DOI: 10.1504/IJCAT.2015.068924

162. L. Hong, A. K. Jain, S. Pankanti, and R. Bolle, "Fingerprint enhancement," in Proc. IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 202–207, 1996.

163. A. K. Jain, S. Prabhakar, and S. Chen, 'Combining multiple matchers for a high security fingerprint verification system', Pattern Recognit. Lett.,vol. 20, no. 11–13, pp. 1371–1379, 1999.

164. F. Hao, R. Anderson, and J. Daugman, 'Combining cryptography with biometrics effectively', Tech. Rep. UCAMCL-TR-640, University of Cambridge, Computer Laboratory, Cambridge, UK, 2005.

165. K. Kaur, G. Geetha, 'Implementing RNA-FINNT in Ideal Password Authentication Scheme results in Fortification of Transport Layer Security Protocol', International Journal of Advances in Computer Science and its Application, ISSN 2250-3765, Vol. 2, Issue 3, pp. 201-205, 2012.

166. Kaur, K, 'Fortification of Transport Layer Security Protocol', International Journal of Computer Applications, IJCA Special Issue on Network Security and Cryptography NSC (2):11-14, December 2011.doi:10.5120/4328-020

167. Computer Security book [Online]. Available: http://books.google.co.in/books?id=KTYxTfyjiOQC&dq=how+to+computer+EER+when+FMR+and+FNMR+is+given&source=gbs_navlinks_s

168. T. Dillinger, VLSI Engineering. Prentice Hall ISBN-13: 978-0139427312

169. Jayaram Bhaskar, A VHDL Synthesis Primer (3rd Edition). Pearson Education. P.113. ISBN 0-9650391-5-3, 1998.

170. Grout, Ian, Digital Systems Design with FPGAs and Cplds. Butterworth Heinemann. p. 724. ISBN 075068397X, 2008.

Index

INDEX

V

W

Y

Appendices

APPENDIX A – QUESTIONNAIRE OF THE SURVEY

Name: **Gender:** **Age:** **Qualification:** **Occupation:** **Place:** **Organization:**
Contact No: **Address:** **Email:** **Date:** **Signature:**

1. Which among the following is the most common and accepted authentication method for online transactions which you generally use?
   a) Password b) Smart Card c) Fingerprint d) Pass Phrase
2. What do you face as the most concerning challenges in online transactions?
   a) Authentication b) Security c) Usability d) None
3. How secure do you think passwords and tokens are during online transactions?
   a) High b) Medium c) Low d) Not Secure
4. How do you perceive usability of passwords and tokens are during online transactions?
   a) High b) Medium c) Low d) Not Decided
5. Which of these authentication types would you use for online transactions in future?
   a) Fingerprint b) Iris c) Location Based d) Voice Recognition
6. How do you evaluate security and privacy in online transactions if fingerprint is used as an authentication type?
   a) High b) Medium c) Low d) Not Secure
7. What are your expectations to secure your transactions while using online mode (either for e-purchasing, e-banking or e-communication etc)?
   a) User Authentication b) Server Authentication
   c) Security from Intruders d) All of the above
8. Generally you are using password for e-purchasing, e-banking or e-communication etc, but if one more tier of security is added with the use of fingerprint for these transactions to be completely secure than what is the possibility of acceptance for the user?
   a) High b) Medium c) Low d) Not Sure
9. Adding one more tier for enhancing security may result in some additional cost to few users, what is the possibility of acceptance that for enhancing security user can bear the nominal cost?
   a) High b) Medium c) Low d) Not Sure
10. If any prototype could result in complete security for e-purchasing, e-banking or e-communication etc then what is the possibility of user's willingness to purchase that?
    a) High b) Medium c) Low d) Not Sure

APPENDIX B – REAL TIME FINGERPRINT DATABASE RESULTS

RTFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#101	0	40	2	35	1	27	2	13	2	13	4	5	7	8	5	5	80	720	0.00	8.37	0.00	0.10	0.00	0.10	1.00	0.90	94.77	30	5	2	25.00
#102	8	68	9	63	7	36	6	66	41	14	41	14	17	40	24	47	80	720	23.32	23.81	0.77	0.59	0.77	0.59	0.23	0.41	31.97	30	5	8	100.00
#103	8	103	7	102	6	76	1	60	4	9	1	10	3	20	0	23	80	720	28.71	26.72	1.07	0.69	1.07	0.69	-0.07	0.31	12.09	30	5	4	50.00
#104	5	47	4	4	18	22	5	3	5	3	15	26	17	39	9	59	80	720	15.33	4.00	0.09	0.24	0.09	0.24	0.91	0.76	83.66	30	5	5	62.50
#105	3	103	5	68	11	48	8	32	15	69	12	67	7	68	11	54	80	720	17.58	18.44	0.45	0.45	0.45	0.45	0.55	0.55	54.98	30	5	8	100.00
#106	11	80	4	33	4	35	3	18	3	70	4	67	19	61	7	32	80	720	29.66	11.49	0.47	0.51	0.47	0.51	0.53	0.49	50.61	30	5	7	87.50

APPENDIX C – EXISTING FINGERPRINT DATABASE RESULTS

EFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#101	11	109	10	99	22	100	14	96	14	94	14	108	24	75	13	97	80	720	34.63	31.46	1.51	0.83	1.51	0.83	-0.51	0.17	17.39	30	5	8	100.00
#102	57	59	34	47	33	44	29	21	22	89	32	78	22	92	16	91	80	720	57.99	39.97	3.22	1.22	3.22	1.22	-2.22	-0.22	-22.46	30	5	8	100.00
#103	37	38	34	24	54	54	32	58	28	83	24	66	13	69	16	87	80	720	37.50	28.57	1.49	0.83	1.49	0.83	-0.49	0.17	17.42	30	5	8	100.00
#104	6	115	5	131	6	188	2	126	5	70	2	78	10	116	6	132	80	720	26.27	25.59	0.93	0.65	0.93	0.65	0.07	0.35	35.17	30	5	8	100.00
#105	36	80	63	58	52	54	48	76	19	97	30	83	32	67	33	57	80	720	53.67	60.45	4.51	1.43	4.51	1.43	-3.51	-0.43	-42.64	30	5	8	100.00
#106	10	6	18	6	18	12	20	20	12	16	19	14	21	19	23	16	80	720	7.75	10.39	0.11	0.23	0.11	0.23	0.89	0.77	88.82	30	5	4	50.00
#107	12	84	4	99	5	130	9	105	16	50	27	37	30	100	9	102	80	720	31.75	19.90	0.88	0.65	0.88	0.65	0.12	0.35	35.44	30	5	8	100.00
#108	9	73	18	78	27	76	22	71	10	80	5	78	9	59	27	46	80	720	25.63	37.47	1.33	0.79	1.33	0.79	-0.33	0.21	21.12	30	5	8	100.00
#109	5	65	10	71	17	57	16	53	14	47	17	38	7	86	3	81	80	720	18.03	26.65	0.67	0.56	0.67	0.56	0.33	0.44	44.16	30	5	8	100.00
#110	38	85	11	68	16	75	8	67	13	76	9	46	10	61	3	74	80	720	56.83	27.35	2.16	1.05	2.16	1.05	-1.16	-0.05	-5.23	30	5	8	100.00
#113	4	102	10	81	5	96	1	118	7	100	4	105	1	116	12	63	80	720	20.20	28.46	0.80	0.61	0.80	0.61	0.20	0.39	39.18	30	5	8	100.00
#114	6	106	6	74	11	101	4	120	16	82	4	103	3	69	3	87	80	720	25.22	21.07	0.74	0.58	0.74	0.58	0.26	0.42	42.14	30	5	8	100.00
#115	9	125	7	100	10	117	17	126	8	126	18	100	4	110	34	59	80	720	33.54	26.46	1.23	0.75	1.23	0.75	-0.23	0.25	25.00	30	5	8	100.00
#116	6	100	5	79	2	100	9	109	14	52	11	95	1	133	5	121	80	720	24.49	19.87	0.68	0.55	0.68	0.55	0.32	0.45	44.54	30	5	8	100.00
#117	43	64	45	80	10	104	16	91	17	82	15	89	37	86	25	57	80	720	52.46	60.00	4.37	1.41	4.37	1.41	-3.37	-0.41	-40.57	30	5	8	100.00
#118	12	73	21	70	9	79	11	77	5	70	21	76	23	67	8	81	80	720	29.60	38.34	1.58	0.85	1.58	0.85	-0.58	0.15	15.08	30	5	8	100.00
#119	27	0	27	0	3	0	38	0	51	0	19	0	31	0	43	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	4	50.00

EFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#120	90	1	113	2	112	9	67	4	72	0	58	1	82	5	104	7	80	720	9.49	15.03	0.20	0.31	0.20	0.31	0.80	0.69	80.19	30	5	8	100.00
#201	61	3	29	9	45	5	29	7	9	2	22	23	22	2	14	0	80	720	13.53	16.16	0.30	0.37	0.30	0.37	0.70	0.63	69.65	30	5	5	62.50
#202	5	56	8	18	17	23	18	16	2	81	3	64	36	6	28	7	80	720	16.73	12.00	0.28	0.36	0.28	0.36	0.72	0.64	72.11	30	5	7	87.50
#208	32	52	9	98	20	42	10	63	0	121	0	127	120	5	39	34	80	720	40.79	29.70	1.68	0.88	1.68	0.88	-0.68	0.12	11.89	30	5	8	100.00
#209	10	80	2	124	21	98	39	120	28	106	13	94	3	107	62	80	80	720	28.28	15.75	0.62	0.55	0.62	0.55	0.38	0.45	44.96	30	5	8	100.00
#210	6	88	39	39	15	60	39	93	2	28	12	66	18	51	31	35	80	720	22.98	39.00	1.24	0.77	1.24	0.77	-0.24	0.23	22.53	30	5	7	87.50
#211	8	68	5	80	6	95	1	86	58	80	0	98	4	83	34	19	80	720	23.32	20.00	0.65	0.54	0.65	0.54	0.35	0.46	45.85	30	5	8	100.00
#212	0	66	14	84	10	98	31	89	12	21	0	115	20	67	32	84	80	720	0.00	34.29	0.00	0.43	0.00	0.43	1.00	0.57	100.00	30	5	8	100.00
#213	38	19	20	40	37	27	29	42	9	27	27	43	12	61	36	35	80	720	26.87	28.28	1.06	0.69	1.06	0.69	-0.06	0.31	31.06	30	5	8	100.00
#214	41	100	27	99	23	92	40	86	58	46	16	39	14	76	11	111	80	720	64.03	51.70	4.60	1.45	4.60	1.45	-3.60	-0.45	-44.67	30	5	8	100.00
#215	29	62	45	58	120	43	16	64	33	53	8	50	19	59	118	37	80	720	42.40	51.09	3.01	1.17	3.01	1.17	-2.01	-0.17	-16.86	30	5	8	100.00
#216	4	77	1	71	2	64	1	47	80	22	10	63	7	58	33	15	80	720	17.55	8.43	0.21	0.32	0.21	0.32	0.79	0.68	79.46	30	5	8	100.00
#217	4	77	10	62	7	71	18	69	18	31	5	42	9	76	22	45	80	720	17.55	24.90	0.61	0.53	0.61	0.53	0.39	0.47	46.94	30	5	8	100.00
#223	27	31	45	28	52	52	73	11	78	50	54	13	53	27	75	8	80	720	28.93	35.50	1.43	0.81	1.43	0.81	-0.43	0.19	19.47	30	5	8	100.00
#224	67	30	67	16	81	18	80	16	87	32	64	19	60	36	73	31	80	720	44.83	32.74	2.04	0.97	2.04	0.97	-1.04	0.03	3.03	30	5	8	100.00
#225	39	40	8	49	15	52	29	39	10	63	12	37	15	41	12	51	80	720	39.50	19.80	1.09	0.74	1.09	0.74	-0.09	0.26	25.88	30	5	8	100.00
#226	31	38	25	47	20	26	3	37	23	37	9	43	2	44	8	35	80	720	34.32	34.28	1.63	0.86	1.63	0.86	-0.63	0.14	14.25	30	5	8	100.00
#227	4	45	18	43	11	38	8	34	26	47	10	31	38	20	25	54	80	720	13.42	27.82	0.52	0.52	0.52	0.52	0.48	0.48	48.45	30	5	8	100.00
#301	4	0	3	22	4	2	6	6	3	0	4	3	10	6	0	12	80	720	0.00	8.12	0.00	0.10	0.00	0.10	1.00	0.90	100.00	30	5	0	0.00

EFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#302	2	5	6	26	5	18	3	14	5	12	6	3	17	10	3	16	80	720	3.16	12.49	0.05	0.20	0.05	0.20	0.95	0.80	94.51	30	5	1	12.50
#303	5	11	3	1	2	31	5	20	4	21	3	1	5	18	7	12	80	720	7.42	1.73	0.02	0.11	0.02	0.11	0.98	0.89	98.22	30	5	1	12.50
#304	4	15	1	2	2	28	6	15	4	10	9	9	1	12	1	26	80	720	7.75	1.41	0.02	0.11	0.02	0.11	0.98	0.89	98.48	30	5	0	0.00
#305	1	0	4	18	9	7	9	4	4	1	6	0	8	25	3	28	80	720	0.00	8.49	0.00	0.11	0.00	0.11	1.00	0.89	100.00	30	5	2	25.00
#311	23	79	7	2	15	72	11	57	23	18	14	13	2	2	11	55	80	720	42.63	3.74	0.22	0.58	0.22	0.58	0.78	0.42	77.85	30	5	5	62.50
#312	10	73	30	42	5	100	7	35	11	0	13	39	18	10	3	133	80	720	27.02	35.50	1.33	0.78	1.33	0.78	-0.33	0.22	21.86	30	5	6	75.00
#313	18	84	3	2	8	121	13	3	42	22	25	22	31	65	9	129	80	720	38.88	2.45	0.13	0.52	0.13	0.52	0.87	0.48	86.77	30	5	6	75.00
#314	20	38	28	23	1	89	18	25	42	22	42	29	45	16	5	124	80	720	27.57	25.38	0.97	0.66	0.97	0.66	0.03	0.34	33.82	30	5	8	100.00
#315	38	4	15	0	0	148	1	64	46	38	29	8	0	0	26	35	80	720	12.33	0.00	0.00	0.15	0.00	0.15	1.00	0.85	100.00	30	5	6	75.00
#316	18	4	43	2	7	128	13	16	7	73	43	14	0	0	32	25	80	720	8.49	9.27	0.11	0.22	0.11	0.22	0.89	0.78	89.07	30	5	5	62.50
#317	12	14	11	93	41	15	21	21	13	6	10	3	7	5	11	58	80	720	12.96	31.98	0.58	0.56	0.58	0.56	0.42	0.44	43.82	30	5	4	50.00
#318	12	34	3	108	8	64	5	50	49	41	0	0	45	1	45	26	80	720	20.20	18.00	0.50	0.48	0.50	0.48	0.50	0.52	52.25	30	5	7	87.50
#319	49	29	7	7	2	117	3	120	42	55	21	13	1	106	7	113	80	720	37.70	7.00	0.37	0.56	0.37	0.56	0.63	0.44	63.35	30	5	7	87.50
#320	14	42	1	61	7	60	1	110	36	26	11	12	5	109	11	110	80	720	24.25	7.81	0.26	0.40	0.26	0.40	0.74	0.60	73.70	30	5	7	87.50
#326	6	106	6	74	11	101	4	120	16	82	4	103	3	69	3	87	80	720	25.22	21.07	0.74	0.58	0.74	0.58	0.26	0.42	42.14	30	5	8	100.00
#327	9	125	7	100	10	117	17	126	8	126	18	100	4	110	34	59	80	720	33.54	26.46	1.23	0.75	1.23	0.75	-0.23	0.25	25.00	30	5	8	100.00
#328	6	100	5	79	2	100	9	109	14	52	11	95	1	133	5	121	80	720	24.49	19.87	0.68	0.55	0.68	0.55	0.32	0.45	44.54	30	5	8	100.00
#329	43	64	45	80	10	104	16	91	17	82	15	89	37	86	25	57	80	720	52.46	60.00	4.37	1.41	4.37	1.41	-3.37	-0.41	-40.57	30	5	8	100.00
#330	12	73	21	70	9	79	11	77	5	70	21	76	23	67	8	81	80	720	29.60	38.34	1.58	0.85	1.58	0.85	-0.58	0.15	15.08	30	5	8	100.00

EFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#331	62	53	16	60	15	46	4	84	13	116	57	53	22	66	15	33	80	720	57.32	30.98	2.47	1.10	2.47	1.10	-1.47	-0.10	-10.38	30	5	8	100.00
#332	8	46	3	65	2	60	16	42	17	64	3	70	15	39	0	75	80	720	19.18	13.96	0.37	0.41	0.37	0.41	0.63	0.59	62.79	30	5	8	100.00
#333	12	36	15	33	10	30	4	21	13	32	14	46	17	45	22	32	80	720	20.78	22.25	0.64	0.54	0.64	0.54	0.36	0.46	46.21	30	5	7	87.50
#334	11	71	37	96	72	42	26	81	12	12	18	41	58	59	51	32	80	720	27.95	59.60	2.31	1.09	2.31	1.09	-1.31	-0.09	-9.43	30	5	7	87.50
#335	48	58	76	19	52	32	32	42	59	27	19	69	31	32	16	43	80	720	52.76	38.00	2.78	1.13	2.78	1.13	-1.78	-0.13	-13.45	30	5	8	100.00
#336	3	78	30	62	35	102	26	27	42	63	39	94	32	78	7	87	80	720	15.30	43.13	0.92	0.73	0.92	0.73	0.08	0.27	26.97	30	5	8	100.00
#337	85	20	60	39	107	27	95	12	40	9	157	10	21	11	34	44	80	720	41.23	48.37	2.77	1.12	2.77	1.12	-1.77	-0.12	-12.01	30	5	8	100.00
#338	85	53	56	14	88	15	73	48	32	37	120	14	76	41	33	49	80	720	67.12	28.00	2.61	1.19	2.61	1.19	-1.61	-0.19	-18.90	30	5	8	100.00
#339	120	15	68	17	88	33	28	32	99	32	43	5	48	55	71	51	80	720	42.43	34.00	2.00	0.96	2.00	0.96	-1.00	0.04	4.47	30	5	8	100.00
#340	86	13	60	20	82	11	70	27	57	8	45	36	35	27	56	10	80	720	33.44	34.64	1.61	0.85	1.61	0.85	-0.61	0.15	14.90	30	5	8	100.00

APPENDIX D – NOISY FINGERPRINT DATABASE RESULTS

NFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#101	5	1	9	13	3	0	0	0	8	2	1	0	0	0	1	0	80	720	2.24	10.82	0.03	0.16	0.03	0.16	0.97	0.84	90.16	30	5	0	0.00
#102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#103	11	2	32	2	35	2	0	0	0	0	0	0	0	0	0	0	80	720	4.69	8.00	0.05	0.16	0.05	0.16	0.95	0.84	89.46	30	5	2	25.00
#104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#106	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#107	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#108	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#109	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#113	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#114	59	0	30	0	11	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	1	12.50
#201	31	6	25	0	22	3	3	0	3	0	23	7	30	6	1	0	80	720	13.64	0.00	0.00	0.17	0.00	0.17	1.00	0.83	91.48	30	5	2	25.00
#202	28	1	17	1	5	0	7	0	16	0	0	0	14	3	4	0	80	720	5.29	4.12	0.03	0.12	0.03	0.12	0.97	0.88	92.60	30	5	0	0.00

NFD	1		2		3		4		5		6		7		8		NGRA	NIRA	GM1	GM2	FMR	FNR	FAR	FRR	TAR	TRR	RA	t1	t2	SMR	DT
	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B															
#203	4	0	20	0	20	0	17	0	25	0	17	0	47	19	8	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	1	12.50
#204	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#206	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#207	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#208	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#209	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#210	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#211	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#212	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00
#213	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	720	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1.00	100.00	30	5	0	0.00

APPENDIX E – DETAILS OF PUBLICATIONS

1. Kuljeet Kaur and Dr.G.Geetha, 'Fortification of Transport Layer Security Protocol with Hashed Fingerprint Identity Parameter', International Journal of Computer Science and Issues, ISSN: 1694-0814, Vol. 9, Issue 2, No 2: 188-193, March 2012

2. Kuljeet Kaur and Dr.G.Geetha, 'Fortification of Transport Layer Security Protocol by using Password and Fingerprint as Identity Authentication Parameters', International Journal of Computer Applications, ISSN 0975-8887, Vol. 42 No.6: 36-42, March 2012, doi: 10.5120/5700-7751

3. Kuljeet Kaur and Dr.G.Geetha, 'Virtualization of Multi Server Environment results in Enhanced Communication and Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.3: 4101-4108, May-June 2012

4. Kuljeet Kaur and Dr.G.Geetha, "Validation of RNA-FINNT for Reduction in Error Percentage," Proc. of the International Conference on Advances in Computer Science and Electronics Engineering — CSEE 2013 at New Delhi, India, ISBN: 978-981-07-5461-7 doi: 10.3850/ 978-981-07-5461-7_12, (p.55-59), 24th Feb, 2013. New Delhi, India

5. Kuljeet Kaur and Dr.G.Geetha, 'Diminution in Error Approximation by Identity Authentication with IPAS for FTLSP to enhance Network Security', Journal of Information Security - JIS, ISSN 2153-1242 Volume 4, Number 4: 197-202, October 2013, http://dx.doi.org/10.4236/jis.2013.44022

6. Kuljeet Kaur and Dr.G.Geetha, 'Survey for Generating an Ideal Password Authentication Scheme which results in Fortification of Transport Layer Security Protocol', International Journal of Computer Science and Information Technologies, ISSN 0975 – 9646, Vol. 3 Issue No.2: 3608-3614, March-April 2012

7. Kuljeet Kaur and Dr.G.Geetha, "Reckoning Minutiae Points with RNA-FINNT Augments Trust and Privacy of Legitimate User and Ensures Network Security in the Public Network," Fifth International Conference on Networks and Communications (NETCOM - 2013), Chennai (Tamil Nadu, India) dated 27th – 29th Dec, 2013, doi: 10.1007/978-3-319-03692-2_17

8. Kuljeet Kaur and Dr.G.Geetha, "Implementing RNA-FINNT in Ideal Password Authentication Scheme results in Fortification of Transport Layer Security Protocol," International Conference on Advances in Information Technology at Bangkok, Thailand, ISBN: 978-981-07-2683-6 doi:10.3850/978-981-07-2683-6 AIT-104 (p.14-18),23rd June,2012.Bangkok, Thailand

9. Kuljeet Kaur and Dr.G.Geetha, "Generating Multi Server Environment for implementation of Ideal Password Authentication Scheme," International Conference on Advances in Electronics, Electrical and Computer Science Engineering - EEC 2012 at Dehradun, India, ISBN: 978-981-07-2950-9 doi:10.3850/ 978-981-07-2950-9 EEC-376, (p.55-59),7th - 9th July, 2012.Dehradun (Himachal Pradesh, India)

10. Kuljeet Kaur and Dr.G.Geetha, 'Pattern Recognition by Embedded Reduced Number of angles Fingerprint Algorithm in Biometric Machines augments Security', Inderscience International Journal of Computer Applications in Technology, Special Issue on Advances in Networking and Signal Processing for Social Security, ISSN 1741-5047 Volume 51, Number 2: 131-144, April 2015, doi: 10.1504/IJCAT.2015.068924

IN COMMUNICATION

1. Kuljeet Kaur and Dr.G.Geetha, 'Performance and Recognition Accuracy Analysis of Reduced Number of Angles Fingerprint Hash Algorithm', EURASIP Journal on Image and Video Processing. Springer Open Journal **(Under Review)**.