**FINGERPRINT TEMPLATE PROTECTION USING PATTERN**

**TRANSFORMATION**

**A PROJECT REPORT**

*Submitted by*

**N LAKSHMI(2011503545)**

**S VAISHNAVI(2011503529)**

**S SOUNDARIYA(2011503561)**

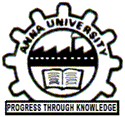
*In partial fulfillment for the award of the degree*

*of*

**BACHELOR OF ENGINEERING**

*in*

**COMPUTER SCIENCE AND ENGINEERING**

****

**DEPARTMENT OF COMPUTER TECHNOLOGY**

**MADRAS INSTITUTE OF TECHNOLOGY**

**ANNA UNIVERSITY, CHENNAI – 600 044**

**APRIL 2015**

**BONAFIDE CERTIFICATE**

Certified that this project report titled,**“FINGERPRINT TEMPLATE PROTECTION USING PATTERN TRANSFORMATION”**is a bonafide record of work done by **N LAKSHMI (2011503545), S VAISHNAVI (2011503529)** and **S SOUNDARIYA (2011503561),** who carried out the project work under my supervision, for the partial fulfillment of the requirements for the award of the degree of Bachelor of Engineering in Computer Science & Engineering. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

**Place :**Chennai

**Date** :

**(SIGNATURE)**

**Dr. P. ANANDHAKUMAR**

**HEAD OF THE DEPARTMENT**

Department of Computer Technology,

Anna University, MIT Campus,

Chennai – 600 044.

**(SIGNATURE)**

**Dr. P. ANANDHAKUMAR**

**PROJECT SUPERVISOR**

Department of Computer Technology,

Anna University, MIT Campus,

Chennai – 600 044.

**ABSTRACT**

Biometric templates are vastly used as a major means of authenticating a person in various industries. The need for fingerprint template protection has become increasingly important. The fingerprint template security using pattern transformation system provides fingerprint privacy by using a shuffling mechanism through intermixing of pixels followed by snake ladder approach (SNL), simulated key insertion and a tree based shuffling mechanism to generate a new virtual identity for fingerprint database security. During the enrollment phase, the left and right fingerprints of a person are combined and then subjected to the proposed algorithms. This work assures a triple layered security mechanism. A non-revocable fingerprint is generated and then stored in the database. During the authentication phase, a similar process is carried out on the input fingerprint. Using alignment and matching algorithms, by means of transformations, the similarity score is computed for each of the registered fingerprints. A threshold value is fixed and those templates that exceed the value are claimed to be identical. Experimental results show that our proposed method has a false matching rate of 0.5 %, false non matching rate of 0.3 % and equal error rate less than 0.1%.

ACKNOWLEDGEMENT

We are highly indebted to our respectable Dean, **Dr. A. RAJADURAI** for providing us with sufficient facilities that contributed to our success in this endeavor.

We are very much thankful and greatly indebted to our Head of the Department and project guide **Dr. P. ANANDHAKUMAR** for his continuous encouragement and exemplary guidance throughout the project. We thank him for his valuable suggestions without which it would have been impossible for us to complete the project in stipulated time.

We sincerely thank our Project Coordinators **Dr. P. JAYASHREE, Dr. R. K. PONSY SATHIA BAMA** and **Mr. P. RAMESH** for their kind support and suggestions to carry out the project work.

We extend our gratitude to the **DST-FIST** for rendering us technical support in accomplishing the project successfully.

We would be failing in our duty, if we forget to thank our parents, all the teaching and non-teaching staff of the department, for their constant support throughout the course of our project work.

**N LAKSHMI S VAISHNAVI S SOUNDARIYA**

**(2011503545) (2011503529) (2011503561)**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER**  **NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | **ii** |
|  | **LIST OF FIGURES** | **vii** |
|  | **LIST OF TABLES** | **ix** |
|  | **LIST OF ABBREVIATIONS** | **x** |
| **1** | **INTRODUCTION** | **1** |
|  | 1.1 OVERVIEW | 1 |
|  | 1.2 BIOMETRICS | 1 |
|  | 1.2.1 Biometrics Authentication Techniques | 2 |
|  | 1.2.2 Threshold Settings Based Matching | 3 |
|  | 1.3 PROBLEMS IN BIOMETRICS | 3 |
|  | 1.4 FINGERPRINT | 5 |
|  | 1.5 NEED FOR PROTECTION  1.6 ORGANIZATION OF THE THESIS  1.7 SUMMARY | 6  7  7 |
| **2** | **LITERATURE SURVEY** | **8** |
|  | 2.1 OVERVIEW  2.2 FINGERPRINT PROTECTION TECHNIQUES | 8  8 |
|  | 2.3 DRAWBACKS OF THE EXISTING SYSTEM | 13 |
|  | 2.4 SUMMARY | 14 |
| **3** | **PROPOSED SYSTEM** | **15** |
|  | 3.1 OVERVIEW | 15 |
|  | 3.2 ARCHITECTURE OF THE PROPOSED SYSTEM | 16 |
|  | 3.3 COMBINED MINUTIAE TEMPLATE | 17 |
|  | 3.3.1 Minutiae Point Alignment | 17 |
|  | 3.3.2 Minutiae Direction Assignment | 17 |
|  | 3.4 SNAKE LADDER APPROACH | 18 |
|  | 3.4.1 Intermixing | 18 |
|  | 3.4.2 Applying SNL  3.5 TREE BASED SHUFFLING MECHANISM  3.5.1 Working Of The Algorithm  3.6 ALIGNMENT PROCESS  3.7 MATCHING PROCESS | 19  19  21  23  24 |
|  | 3.8 SUMMARY | 27 |
| **4** | **EXPERIMENTAL RESULTS** | **29** |
|  | 4.1 MATLAB  4.2 ENROLLMENT PHASE  4.3 AUTHENTICATION PHASE  4.4 PERFORMANCE ANALYSIS  4.5 SUMMARY | 29  30  34  36  40 |
| **5** | **CONCLUSION AND FUTURE WORK** | **41** |
|  | 5.1 CONCLUSION  5.2 FUTURE WORK  **APPENDIX**  **REFERENCES** | 41  41 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
|  |  |  |
| 1.1  2.1 | Minutiae features  Architecture of the existing system | 6  13 |
| 3.1 | Architecture of the proposed system | 16 |
| 3.2 | Working of the SNL algorithm | 18 |
| 3.3 | Working of tree based shuffling  Algorithm | 22 |
| 4.1 | Combined minutiae template | 30 |
| 4.2 | Fingerprint after SNL algorithm | 31 |
| 4.3 | Fingerprint after artificial minutiae points | 31 |
|  | Insertion |  |
| 4.4 | Histogram variation | 32 |
| 4.5 | Tree based shuffling mechanism | 33 |
| 4.6 | Fingerprint database | 33 |

4.7 Minutiae feature extraction from query 34

fingerprint

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |

4.8 Similarity score calculation 35

4.9 Matching of fingerprints 36

4.10 FMR, FNMR and EER 38

4.11 Performance comparison 39

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| 2.1 | Summary of the literature survey | 11 |
| 4.1 | EER (%) of proposed method with other | 39 |
|  | Methods |  |
|  |  |  |
|  |  |  |
|  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **NOTATIONS** | **EXPANSION** |
| DNA | Deoxyribo Nucleic Acid |
| PIN | Personal Identification Number |
| ID  HMM  MCC | Identity Document  Hidden Markov Model  Minutiae Cylinder Code |
| SNL  FVC  DST  FIST | SNake Ladder  Fingerprint Verification Competition  Department of Science and Technology  Fund for Improvement of S&T |
| MATLAB  ROI  FMR  FNMR  FAR  FRR  EER | MATrixLABoratory  Region Of Interest  False Match Rate  False Non-Match Rate  False Acceptance Rate  False Recognition Rate  Equal Error Rate |

**CHAPTER 1**

**INTRODUCTION**

Humans like any other living organisms are characterized with the property of uniqueness for every individual. This unique property serves as an identity at various social circles, monetary accounts, educational certificates, security authentication systems.

**1. 1 OVERVIEW**

Some of the unique identities of an individual which can be used for identification are the finger print, retinal scan, personal signature, DNA fingerprinting, forensic odontology, facial recognition system, gait analysis, voice analysis, password, security questions and digital signatures. Identity verification are based on knowledge (passwords and PIN) or possession factors (ID cards and token) afford low level of security since passwords and PIN can be forgotten and acquired by covert observation. Biometrics-based verification systems confirm an individual’s identity based on the physiological and behavioral characteristics of the user. This chapter deals with biometrics and need for its protection.  
  
**1.2 BIOMETRICS**

Biometrics refers to the metrics related to human characteristics and traits which can be used as form of identification and access control. Biometric identifiers are the distinctive, measurable characteristics which can be either physiological or behavioral and they are used to label and describe individuals.  
Physiological characteristics are related to the shape of body and behavioral to the pattern of behavior of a person. Biometrics based methods provide direct link between the service and the actual user. A biometric verification system is a one-to-one match that determines whether the claim of an individual is true.

**1.2.1 Biometrics Authentication Techniques**

A biometric authentication is essentially a pattern-recognition that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.

An important issue is designing a practical approach to determine how an individual is identified. An authentication can be divided into two modules:

1. Enrollment module

2. Identification or Verification module

The enrolment module is responsible for enrolling individuals into the biometric system. During the enrolment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. In order to facilitate matching, the raw digital representation is usually further processed by feature extractor to generate a compact but expensive representation, called a template.

Depending on the application, the template may be stored in the central database. Depending on the application, biometrics can be used in one of two modes: verification or identification. Verification, also called authentication is used to verify a person’s identity, that is, to authenticate that individuals are who they say they are. Identification is used to establish a person’s identity, that is, to determine who a person is.

Although biometric technologies measure different characteristics in substantially different ways, all biometric systems start with an enrollment stage followed by a matching stage that can use either verification or identification.

**1.2.2 Threshold Settings Based Matching**

No match is ever perfect in either verification or identification system, because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no-match decision, based on a predefined number, referred to as a threshold, which establishes the acceptable degree of similarity between the trial template and the enrolled reference template.

After the comparison, a score representing the degree of similarity is generated, and this score is compared to the threshold to make a match or no-match decision. Depending on the setting of the threshold in identification systems, sometimes several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches.

**1.3 PROBLEMS IN BIOMETRICS**

While biometric technology provides various advantages, there exist some major problems.

1. Changeability:

Biometrics cannot be easily changed or reissued if compromised due to the limited number of biometric traits that human has. When the biometric template in one application is compromised, the biometric signal itself is not lost forever, and a new biometric template can be reissued.

2. Privacy:

Biometric data reflect the user’s physiological or behavioral characteristics. If the storage of the biometric templates is obtained by an adversary, the user’s privacy may be compromised. The biometric templates should be stored in a format such that the user’s privacy is preserved.

One simple method to address the changeability and privacy problems is to use user-specific encryption keys to encrypt the biometric data during the enrollment and decrypt at the time of authentication. However, this method provides limited privacy protection since the original biometric template will be exactly recovered if the key is stolen. To deal with this, a number of research works have been proposed in recent years. These techniques can be categorized into two main classes:

1. Biometric cryptosystems:

In a biometric cryptosystem, secure sketch is derived from the enrolled biometric template and stored in the system database instead of the original template. It must be computationally hard to reconstruct the template from the sketch.

2. Template transformation:

Template transformation techniques modify the biometric template with user specific key such that it is difficult to recover the original template from the transformed template.

Currently deployed systems typically employ classical cryptographic techniques to securely store data. However, even if the stored data are kept secure when not used, decryption has to be performed during authentication, thus leaving biometric system unprotected. Therefore a template protection scheme should satisfy the following properties:

1. Renewability:

For each user, it should be possible to revoke a compromised template and reissue a new one based on the same biometric data. This property is needed to ensure the user’s privacy.

2. Security:

It must be impossible or computationally hard to obtain the original biometric template from the stored and secured one.

3. Performance:

The recognition performance should not degrade significantly with the introduction scheme, with respect to the performance of unprotected system.

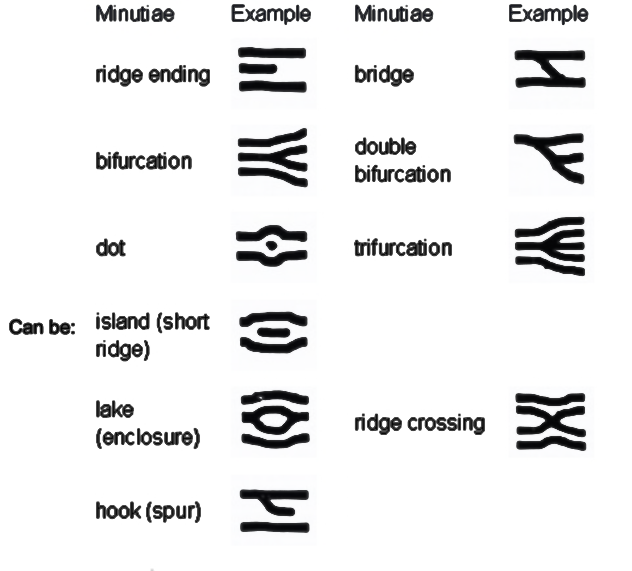
**1.4 FINGER PRINT**

Out of all biometric features, fingerprint templates are the most commonly used feature for identifying an individual. Fingerprints are the traces of impressions from the friction ridges of any part of a human hand.  
 Fingerprint identification (dactyloscopy) is the process of comparing two   
instances of friction skin impressions (Minutiae) from human fingers, toes, palm or sole of the foot.

The fingerprints can be either flat or rolled. A flat print captures only an impression of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger

During enhancement, “noise” caused by such things as dirt, cuts, scars, and creases or dry, wet or worn fingerprints is reduced, and the definition of the ridges is enhanced. Approximately 80 percent of vendors base their algorithms on the extraction of minutiae points relating to breaks in the ridges of the fingertips.

The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points as shown in the Fig 1.1



**Figure 1.1 Minutiae features**

Minutiae, in fingerprinting terms, are the points of interest in a fingerprint,   
Some of the notable minutiae used for the identification are,

1. ridge endings - a ridge that ends abruptly

2. ridge bifurcation - a single ridge that divides into two ridges

3. short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends

4. spur - a bifurcation with a short ridge branching off a longer ridge

5. crossover or bridge - a short ridge that runs between two parallel ridges

**1.5 NEED FOR PROTECTION**

With the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue.

Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint.

Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen.

**1.6 ORGANIZATION OF THE THESIS**

The thesis is organized as follows, Chapter 1 dealing with the introduction to authentication using an individual’s biometric traits. Chapter 2 deals with the survey of all the works related to feature extraction from biometric templates, authenticating a user and security aspects. Chapter 3 deals with the proposed work for providing security using pattern transformation mechanisms. Chapter 4 gives the implementation details of the proposed technique followed by conclusions and future work in Chapter 5.

**1.7 SUMMARY**

The fingerprint is one of the accepted biometric methods used to verify human being. It is tricky to design accurate algorithms capable of extracting relevant features and matching them in a robust way, especially with reduced quality fingerprint images. There are only a few schemes that are able to protect the privacy of the fingerprint. Hence, providing a better solution for protection of fingerprint templates is the main focus of this work.

**CHAPTER 2**

**LITERATURE SURVEY**

Fingerprint template protection can be obtained with the help of encryption as well as decryption; otherwise the confidentiality is removed and it is easy for the hacker to obtain the original fingerprint. In the recent years, new protection techniques are found in order to provide privacy to the fingerprints.

**2.1 OVERVIEW**

The main application of fingerprint techniques is the fingerprint authentication and validation systems and other applications include providing privacy for the fingerprint images. This chapter deals with the initiatives taken by various researchers to protect the fingerprint template of an individual.

**2.2 FINGERPRINT PROTECTION TECHNIQUES**

Alex C. Kot et al.[21] and [12], [11] proposed the fingerprint combination for privacy protection in which two different fingerprints were combined to produce a new virtual identity and finally stored in database. They have proposed [21] a fingerprint reconstruction algorithm. A fake fingerprint image is reconstructed from a stolen combined fingerprint template; there are possibilities that the hacker can crack traditional systems. Minutiae points are found based on amplitude and frequency and the reconstructed fingerprint is used by the attacker to rebuild. The spirals from the partial fingerprint image and the fingerprint can be reconstructed intuitively.

By reconstructing a fingerprint it might be faked, which causes enormous problems to the security systems.

JianjiangFeng et al.[5] proposed an orientation field estimation for latent fingerprint enhancement. It is a technique that retrieves the preliminary orientations from the fingerprint. After obtaining the clustered candidates, final direction is determined. The proposed algorithm is poor and inefficient in terms of latency and speed.

S. Li et al. [10] proposed an architecture that provides security to fingerprints, in which the fingerprint privacy is done in enrollment without using any key. This makes it a tough deal for the hacker to differentiate the original fingerprint template from the saved template. Even if the combined minutiae template is stolen, the hacker will not be able to obtain the properties of the complete fingerprint thus overcoming the existing fingerprint privacy protection techniques. The algorithm is still not up to the inferiority mark, thus resulting in slow speed and low quality latent.

A. Othman et al. [17] proposed a visual cryptography for biometric privacy that makes use of cryptography for imparting confidentiality of biometric information such as fingerprint images, face images, iris codes. The planned approach [17] stores the fingerprint in non-recoverable format. Without pixel expansion VCS is developed. Now there does not exist any such scheme where accidental noisy images are produced.

The algorithms proposed earlier are based on keys that ensure fingerprint security. However, if the keys are stolen, it makes the protection system insecure.

Teohet al. [22] proposed a bio-hashing approach in which pseudo random numbers and minutiae features extracted from the fingerprint are made use of. The key which is being made use of should not be revealed to increase the protection criteria[7].

Rathaet al. [16] suggested by generating a cancelable fingerprint template by employing transformations, on the features extracted, that are non- recoverable. The resulting transformed template is encrypted with a key and an irreversible template is obtained. If the key and the resultant template are hacked, [7] and [16] prove worthless.

Nandakumar et al. [14] suggested by executing fuzzy fault logic on the minutiae features in which the key-inversion attack was used [20]. The works in [9] hides the identity of the user who has a thinned fingerprint image by making use of keys. When the thinned fingerprint template and the key is revealed, the user identity can be easily hacked. Only few protection techniques are available without making use of keys.

In matching applications, two separate databases are required in order to perform computations or work in it. The works in [24] a new identity is obtained after combining the features [24] or images [18],[15] of left and right fingerprints. Minutiae features from two fingerprints are obtained and are combined in [24].

The new identity will be a mixture of existing minutiae features and new minutiae positions. The attacker can identify the new template because of the presence of a number of new minutiae features. After experimenting with the fingerprint database, EER is found to be 2.1%.

In [1], a new technique is proposed where artificial minutiae points are inserted into the fingerprint template by means of voice input. Thus a new template is generated after inserting these artificial minutiae points. After experimentation, EER is found to be less than 2%.

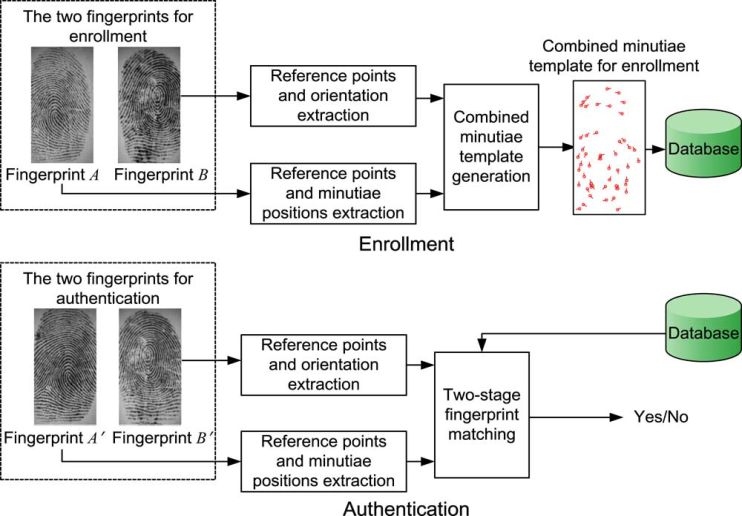
In [18], [15], image level combination of two fingerprints is proposed. Firstly, spiral and continuous components of each fingerprint is separated with respect to FM-AM model[8].

This proposed SNL makes use of techniques such as inter-mixing, swapping, simulated key insertion followed by tree based shuffling mechanism to provide new virtual identity. The matching algorithm combines transformations for alignment purposes and a threshold based mapping approach to calculate a similarity score. The implementation results show very low error rate with FMR of 0.5 % and FNMR of 0.3 % .

**Table 2.1 Summary of the literature survey**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SNo** | **Title & Author** | **Technique used** | **Problem Addressed** | **Limitations** |
| 1 | Fingerprint Combination for Privacy Protection by Sheng Li Sch. of Electr. & Electron. Eng., Nanyang Technol. Univ., Singapore, Singapore  Kot, AC | Fingerprint combination | New virtual identity  Low error rate | Limited privacy protection  Features of original template completely revealed in the new identity-information leakage |
| 2 | Privacy protection from fingerprint database by Sheng Li Sch. of Electr. & Electron. Eng., Nanyang Technol. Univ., Singapore, Singapore  Kot, AC | Data hiding | Better data hiding techniques by embedding user’s private information | Poor performance |
| 3 | Cancealable templates for sequence based biometrics with application to online signature recognition by [Maiorana,E.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Maiorana,%20E..QT.&searchWithin=p_Author_Ids:37392740300&newsearch=true) Dipt. di Elettron. Applicata [Campisi,P.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Campisi,%20P..QT.&searchWithin=p_Author_Ids:37269456300&newsearch=true) ; [Fierrez,J.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Fierrez,%20J..QT.&searchWithin=p_Author_Ids:37392738600&newsearch=true) ; [Ortega-Garcia, J.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Ortega-Garcia,%20J..QT.&searchWithin=p_Author_Ids:37281647300&newsearch=true) ; [Neri, A.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Neri,%20A..QT.&searchWithin=p_Author_Ids:37272753900&newsearch=true) | Bio convolving and HMM | Non invertible transforms | Security depends on hardness of transformations applied |
| 4 | Non invertible minutia cylinder code representation by [Ferrara, M.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Ferrara,%20M..QT.&searchWithin=p_Author_Ids:37408613100&newsearch=true) ; Dept. of Electron., Univ. of Bologna, Cesena, Italy ; [Maltoni, D.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Maltoni,%20D..QT.&searchWithin=p_Author_Ids:38513068700&newsearch=true) ; [Cappelli, R.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Cappelli,%20R..QT.&searchWithin=p_Author_Ids:38513413900&newsearch=true) | MCC representation | Accurate  Better privacy protection | Invertible |
| 5 | Blind authentication: a secure crypto biometric verification protocolby [Upmanyu, M.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Upmanyu,%20M..QT.&searchWithin=p_Author_Ids:37397740400&newsearch=true) ; Int. Inst. of Inf. Technol., Hyderabad, India ; [Namboodiri, A.M.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Namboodiri,%20A.M..QT.&searchWithin=p_Author_Ids:37268964700&newsearch=true) ; [Srinathan, K.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Srinathan,%20K..QT.&searchWithin=p_Author_Ids:37318346000&newsearch=true) ; [Jawahar, C.V.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Jawahar,%20C.V..QT.&searchWithin=p_Author_Ids:37270075200&newsearch=true) | Public key cryptography | Applicable to multiple biometrics | Involves more computations |
| 6 | Multi biometric cryptosystems based on feature level fusion by [Nagar, A.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Nagar,%20A..QT.&searchWithin=p_Author_Ids:38472081900&newsearch=true) ; Dept. of Comput. Sci. & Eng., Michigan State Univ., East Lansing, MI, USA ; [Nandakumar, K.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Nandakumar,%20K..QT.&searchWithin=p_Author_Ids:37400095000&newsearch=true) ; [Jain, A.K.](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Jain,%20A.K..QT.&searchWithin=p_Author_Ids:38200462600&newsearch=true) | Feature level fusion framework and fuzzy commitment | Higher security | Poor feature fusion  Multimodal database management |
| 7 | A Delaunay quadrangle based fingerprint authentication system with template protection using topology code for local registration and security enhancement by [Wencheng Yang](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Wencheng%20Yang.QT.&newsearch=true) ; Sch. of Eng. & Inf. Technol., Univ. of New South Wales, Canberra, ACT, Australia ; [Jiankun Hu](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Jiankun%20Hu.QT.&newsearch=true) ; [Song Wang](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=p_Authors:.QT.Song%20Wang.QT.&newsearch=true) | Delaunay quadrangle based structure | Improved security | Uncertainty due to rotation and translation |

**2.3 DRAWBACKS OF THE EXISTING SYSTEM**



**Figure 2.1 Architecture of the existing system**

Left and right fingerprints are obtained from the user, say fingerprint A and fingerprint B. Minutiae positions from fingerprint A and orientation from fingerprint B are extracted as shown in Fig 2.1. Reference points are extracted from both fingerprint A and fingerprint B. The minutiae points in fingerprint A are rotated to an angle specified by the orientations of minutiae points in fingerprint B. Thus a new virtual identity is generated and stored in the database. In the authentication phase, query fingerprint A’ and B’ are obtained from the user. A similar approach is carried out. The generated template is then compared with the template stored in the database. A matching score is calculated. If the matching score is above a fixed threshold value, the user is authenticated. If the attacker’s target is to recover the approximate version of the original minutiae template so that the attacker can launch a successful attack, the probability to recover fingerprint A and B from combined template is significantly high. Therefore the existing system does not ensure proper privacy and security to the fingerprint templates.

**2.4 SUMMARY**

In this chapter, the works related to fingerprint privacy protection and matching strategies have been discussed in detail. Research papers that discuss the methodologies adopted by various researchers have been reviewed and corresponding pros and cons of each work has been inferred. This chapter gives an insight into various challenges like alignment processes, efficient matching strategies and high protection to enrolled fingerprint templates for security purposes.

**CHAPTER 3**

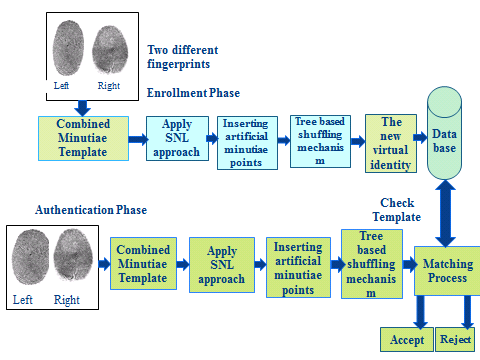
**PROPOSED SYSTEM**

The proposed work is a fingerprint recognition system for defending fingerprint privacy by combining two dissimilar fingerprints by applying the snake ladder approach to generate a new virtual identity and stored in the fingerprint database.

**3.1 OVERVIEW**

The system captures two fingerprints from two different fingers, Extract the minutiae position from one fingerprint, orientation from the other fingerprint, the reference point from both fingerprints. Based on coding strategies, combined minutiae template is generated. The combined minutiae template is then subjected to various shuffling algorithms like intermixing of pixels, SNL approach and insertion of artificial minutiae points followed by a tree based shuffling mechanism. Hence a new virtual identity is created for the user. Even if the attacker obtains the generated virtual identity, it would be difficult for him to get back the original fingerprint. Intermixing of pixels, SNL approach and insertion of artificial minutiae points serve as a three layered security mechanism. Instead of storing the combined minutiae template as such in the database, storing the template after these operations will ensure better security and non-invertible template generation.

**3.2 ARCHITECTURE OF THE PROPOSED SYSTEM**



**Alignment**

**Figure 3.1 Architecture of the proposed system**

Left and right fingerprints are combined to generate a combined template as shown in Fig 3.1. SNL algorithm is applied on the combined minutiae template. Artificial minutiae points are inserted at chosen locations and the resulting image is subjected to tree based shuffling mechanism. Hence a new virtual identity is created. This template is stored in the database. In the authentication phase, a similar procedure is carried out on the query fingerprints. The generated identity is matched with the stored template. If it matches reasonably, the user is authenticated.

**3.3 COMBINED MINUTIAE TEMPLATE**

The fingerprint minutiae matching algorithm is used to construct the combined minutiae template. The algorithm involves the following steps:

**3.3.1 Minutiae Position Alignment**

To find minutiae position (let’s assume is located at with the angle, and is located at with the angle .

) Calculate the position value.

(3.1)

H is the rotation matrix

H= (3.2)

**3.3.2 Minutiae Direction Assignment**

Minutiae direction assignment initializes the , direction.

(3.3)

Where, is the average direction of the nearest neighboring minutiae points of the location ) in fingerprint is the direction of the adjacent neighboring minutiae point of the location in fingerprint image, and the position value which is able to supply a good stability between the diversity and matching accuracy of the minutiae points.

**3.4 SNAKE LADDER APPROACH**

The proposed SNL algorithm makes use of techniques such as intermixing, swapping and simulated key insertion to provide new virtual identity. Finally created the new virtual identity and stored in the database. This approach is secured



**Figure 3.2 Working of the SNL algorithm**

**3.4.1 Intermixing**

All the pixel values of the image are shuffled to form a new virtual identity as shown in Fig 3.2. The resulting image is subjected to SNL algorithm.

**3.4.2 Applying SNL**

Snakes and ladders are inserted at desired locations. Based on the Snake and Ladder game the pixel values of the image are aligned. When a snake is encountered pixel value goes down, whereas pixel value moves up on seeing a ladder. For example, Snake(16,20) = LCM(16, 20) = 80. Hence 80 times the value of upper level pixel value comes downwards. Ladder(8,2) = bit. complement(8,2) = bit. complement(1000, 2) = 12 . Hence 12 times the value of lower level pixel will go up. Later on minutiae points are inserted to enhance the security.

**3.5 TREE BASED SHUFFLING MECHANISM**

The resultant image is subjected to a shuffling algorithm based on swapping of nodes in a tree. A tree is constructed using the matrix that represents the pixel values of the image.

**TREE BASED SHUFFLING ALGORITHM**

**INPUT: COMBINED MINUTIAE TEMPLATE AFTER APPLYING SNL**

**OUTPUT: ENCRYPTED IMAGE (New virtual identity)**

Obtain the value of the pixel in the first row-first column.

for each iteration

obtain the level of the node with 1st 2 MSB

if ( level= 0)

say x is the value of last 6 LSBs mod 8

if( x=0 )

leftleftleft swap

if( x=1 )

leftleft right swap

if( x=2 )

left right left swap

if( x= 3)

left right right swap

if( x=4 )

right left left swap

if( x=5 )

right left right swap

if( x=6 )

rightright left swap

if( x=7 )

rightrightright swap

if( level = 1 )

node to be swapped= last 6 LSBs mod 2

say x is the value of last 6 LSBs mod 4

if( x=0 )

leftleft swap

if( x=1 )

left right swap

if( x=2 )

rightright swap

if( x=3 )

right left swap

if( level =2 )

node to be swapped=last 6 LSBs mod 4

say x is the value of last 6 LSBs mod 2

if( x=0 )

left swap

if( x=1 )

right swap

if( level=3 )

node to be swapped=last 6LSBs mod 8

swap with its sibling

Remove first 2 MSBs

Say y is the pixel value mod 8

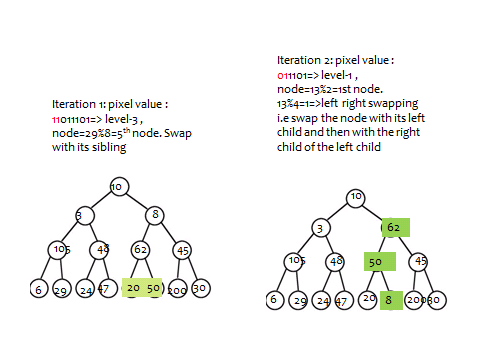
do the swapping operations for level 0; selecting one of the eight possibilities using y value end

**3.5.1 Working Of The Algorithm**

|  |  |  |  |
| --- | --- | --- | --- |
| 221 | 10 | 3 | 8 |
| 105 | 48 | 62 | 45 |
| 6 | 29 | 24 | 47 |
| 50 | 20 | 200 | 30 |

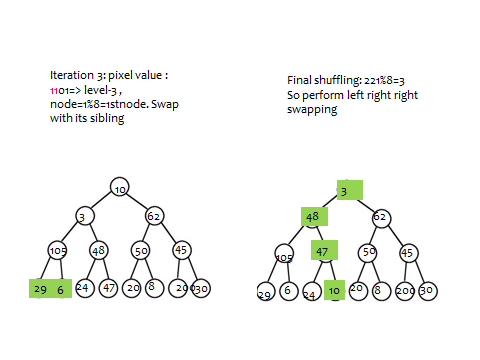
Let the below matrix represent the combined template generated after applying SNL algorithm.

The above matrix is converted into a binary tree by inserting the elements into the tree. Once the elements are inserted, the tree based shuffling algorithm is performed and the pixel values are shuffled to obtain a new virtual identity. The algorithm works as shown below in Fig 3.3.



(a)

(b)

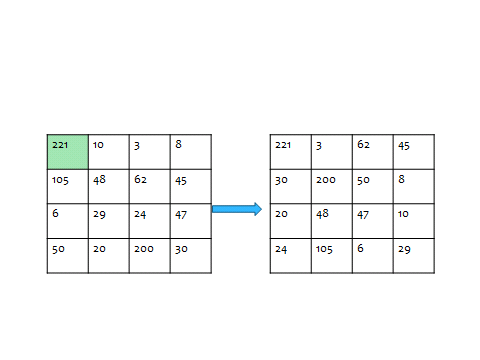


(d)

(c)

**Figure 3.3 Working of the tree based shuffling algorithm (a) Iteration 1 (b) Iteration 2 (c) Iteration 3 (4) Final shuffling**

The resultant tree is traversed in root-right-left fashion and the values are stored back in the matrix in row major order. The resulting template is now stored in the database. The following Fig 3.4 shows the transformation of the pixel vales after applying the tree based shuffling mechanism:



**Figure 3.4 Transformation of the pixel values**

**3.6 ALIGNMENT PROCESS**

Fingerprint matching is an important problem in fingerprint identification. A set of minutiae is usually used to represent a fingerprint. Most existing fingerprint identification systems match two fingerprints using minutiae-based method. Typically, they choose a reference minutia from the template fingerprint and the query fingerprint, respectively. When matching the two sets of minutiae, the template and the query, firstly reference minutiae pair is aligned coordinately and directionally, and secondly the matching score of the rest minutiae is evaluated.

**ALIGNMENT ALGORITHM 1**

**INPUT: ith PIXEL OF COMBINED MINUTIAE TEMPLATE AFTER APPLYING TREE BASED SHUFFLING MECHANISM**

**OUTPUT: IMAGE WITH NEW CO-ORDINATES**

Begin

Initialize number counter, count to the size of the image along x direction

Initialize x reference, y reference, theta reference to the current pixel’s corresponding values

For i=1 to count

B = [ M ( i , 1) – Xref ; M ( i , 2 ) – Yref ; M ( i , 4 ) – ThRef ] ;

/\* B is the transformation matrix \*/

T = B /\*where T is the image with new co-ordinates\*/

End

End

When a fingerprint A1 that is identical to fingerprint A has been input for authentication; no matter what the co-ordinate position variations are; has to be authenticated. The co-ordinate positions have to be aligned in order to obtain the accurate results. The above algorithm transforms the fingerprint A1 with reference to the co-ordinate values of the ith pixel that is sent from the matching function. This algorithm ensures that the fingerprints A1 and A are brought to a common base for easy comparison of minutiae positions. To determine if the minutiae at ith position are aligned along the same direction in both fingerprints A1 and A, a similar translation vector is made use of. A threshold degree is fixed and the minutiae feature of fingerprint A1 is rotated +/- the threshold to determine if it matches with the corresponding minutiae feature of fingerprint A. Instead of rotation, the following algorithm makes use of translation of theta value of minutiae feature to compute similarity score.

**ALIGNMENT ALGORITHM 2**

**INPUT: ith PIXEL OF COMBINED MINUTIAE TEMPLATE AFTER APPLYING TREE BASED SHUFFLING MECHANISM**

**OUTPUT: IMAGE WITH NEW CO-ORDINATES**

Begin

Initialize number counter, count to the size of the image along x direction

Alpha value ranges from -5 to 5 /\* 5 degree is taken as the threshold here \*/

For i=1 to count

B = T ( i , : ) - [ 0 0 alpha 0 ]

/\* B is the transformation matrix \*/

T = B /\*where T is the image with new theta value\*/

End

End

**3.7 MATCHING PROCESS**

The matching process is the authentication phase where a matching score is calculated with which the user is authenticated. This authentication process extracts minutiae position and orientation point from query minutiae by the recognition system. If the matching score is less than a predefined threshold, the input image is said to have successfully matched with the template. Matching Score Calculated using the following formula,

Total matched percentage= (matched data/total data) \* 100; (3.4)

The input fingerprint is compared with the rest of the fingerprints in the database and a similarity score is computed for each of the comparisons. Those fingerprints with which the similarity score exceeds the threshold are returned as the matching fingerprints. If no such fingerprint with the required similarity score is found, the fingerprint is not authenticated. The input image is subjected to alignment and comparison is made out. The following algorithm returns the best similarity score or the extent to which the input image matches with that in the database after transformations.

**MATCHING ALGORITHM**

**INPUT: INPUT IMAGE AND FINGERPRINT DATABASE**

**OUTPUT: BEST SIMILARITY SCORE**

Begin

Initialize count1 to the size of the registered image along x direction

Initialize count2 to the size of the input image along x direction

For i=1 to count1

T1 = alignment algorithm 1 ( registered image )

For j=1 to count 2

If minutiae feature of input image at jth position and that of registered image at ith position is same

T2 = alignment algorithm 1 ( input image )

For alpha = -5 to +5 /\*threshold for theta\*/

T3 = alignment algorithm 2 ( T2 )

similarity score = score calculation ( T3 , T1 )

Obtain the best similarity score out of all the transformations

End

End

End

Return similarity score

End

The similarity score value is computed by comparing the minutiae features of input fingerprint with that of the registered fingerprint. The minutiae positions of both the fingerprints are compared by means of Euclidean formula. A threshold for variation in distance is fixed. The distance variation between the two minutiae points are computed using,

\mathrm{d}(\mathbf{p},\mathbf{q})=\sqrt{(p_1-q_1)^2 + (p_2-q_2)^2}. (3.5)

Where p and q are minutiae points of input fingerprint and the registered fingerprint correspondingly and d is the distance between them. For minutiae direction, the theta values of both the minutiae features are compared and a threshold is used to determine if they match or not.

**SCORE CALCULATION ALGORITHM**

**INPUT: COMBINED MINUTIAE TEMPLATE AFTER APPLYING TREE BASED SHUFFLING MECHANISM AND REGISTERED TEMPLATE**

**OUTPUT: SIMILARITY SCORE**

Initialize number counter, count 1 to the size of the registered image along x direction

Initialize number counter, count 2 to the size of the input image along x direction

Initialise the threshold for distance as T

Initialise the threshold for theta as TT

Initialize the number of matched points, n=0

For i=1 to count 1

For j=1 to count 2

d = sqrt ( ( xi – xj )^2 + ( yi – yj )^2 )

If ( d < T )

ϴ = ϴi - ϴj

If ( ϴ < TT )

Increment n

End

End

Sm= sqrt( n \* n / count 1 \* count 2 )

Return Sm

If ‘n’ points match between the two fingerprints, the similarity score is computed using the formula,

Sm = sqrt ( n \* n / count 1 \* count 2 ) (3.6)

Where count 1 and count 2 are the size of the registered image and input image along x direction correspondingly.

For obtaining accurate results, threshold value is generally fixed as low as possible. By this way, our algorithm takes into account the alignment factor and matches the input image with that in the database with higher efficiency. The above algorithm returns similarity score with the x, y and theta value of the input and registered image that are being sent to the function. Once the input fingerprint is compared with the rest of the fingerprints in the database, similarity scores of each of the comparisons is considered for authentication. The best matching fingerprint is the one with the highest similarity score ( higher than the threshold fixed ). If such a fingerprint is found, the person is authenticated. Else the template is rejected and is claimed to be non-registered user.

Almost entire features of the original finger print are revealed in the existing approach; whereas in the proposed system, a triple layer security is provided to the templates thus hiding the original data and hence information leakage is minimal. The proposed protection system is non-invertible in nature. The hacker cannot obtain the original fingerprint from the new virtual identity.

**3.8 SUMMARY**

In this chapter, the proposed work for fingerprint template protection has been discussed in detail with an overall system architecture design. The modules in each phase have been listed and explained. Algorithms have been provided for triple layered security based encryption, alignment and matching processes. This chapter gives a detailed insight into our proposed work highlighting the uniqueness and the areas of innovation like template protection and alignment process.

**CHAPTER 4**

**EXPERIMENTAL RESULTS**

In this chapter, the results and the accuracy of fingerprint protection and authenticating system have been listed. The correctness of the proposed work has been tested with FVC2002 dataset for testing and with the **DST FIST Sponsored Fingerprint DB 2015** collected from the students of Department of Computer Technology, Madras Institute of Technology, Anna University as a part of the project work for training.

**4.1 MATLAB**

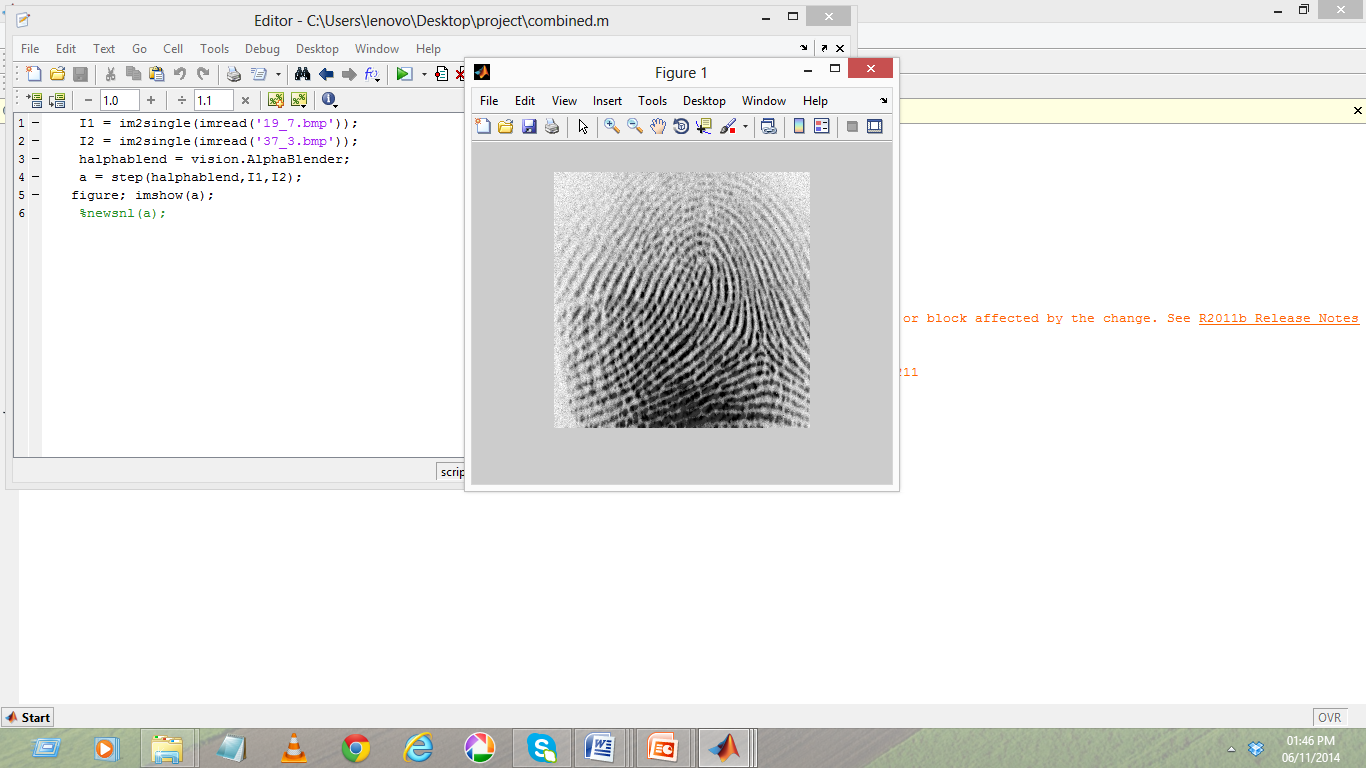
MATLAB version 2012 ( Windows 7) has been used for the implementation of the proposed work. It is known for its simplicity and ability to process huge amount of data. MATLAB (matrix laboratory) is a [multi-paradigm](http://en.wikipedia.org/wiki/Multi-paradigm_programming_language) [numerical computing](http://en.wikipedia.org/wiki/Numerical_analysis) environment and [fourth-generation programming language](http://en.wikipedia.org/wiki/Fourth-generation_programming_language). Developed by [MathWorks](http://en.wikipedia.org/wiki/MathWorks" \o "MathWorks), MATLAB allows [matrix](http://en.wikipedia.org/wiki/Matrix_(mathematics)) manipulations, plotting of [functions](http://en.wikipedia.org/wiki/Function_(mathematics)) and data, implementation of [algorithms](http://en.wikipedia.org/wiki/Algorithm), creation of [user interfaces](http://en.wikipedia.org/wiki/User_interface), and interfacing with programs written in languages, including [C](http://en.wikipedia.org/wiki/C_(programming_language)), [C++](http://en.wikipedia.org/wiki/C%2B%2B), [Java](http://en.wikipedia.org/wiki/Java_(programming_language)), [Fortran](http://en.wikipedia.org/wiki/Fortran) and [Python](http://en.wikipedia.org/wiki/Python_(programming_language)).

MATLAB was first adopted by researchers and practitioners in [control engineering](http://en.wikipedia.org/wiki/Control_engineering), Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of [linear algebra](http://en.wikipedia.org/wiki/Linear_algebra), [numerical analysis](http://en.wikipedia.org/wiki/Numerical_analysis), and is popular amongst scientists involved in [image processing](http://en.wikipedia.org/wiki/Image_processing)

The programs are written in a script file and saved with .m extension. MATLAB also provides us with a command prompt to get instant outcome, when we want to try a command. A help command can also be used to get a description about a particular command.

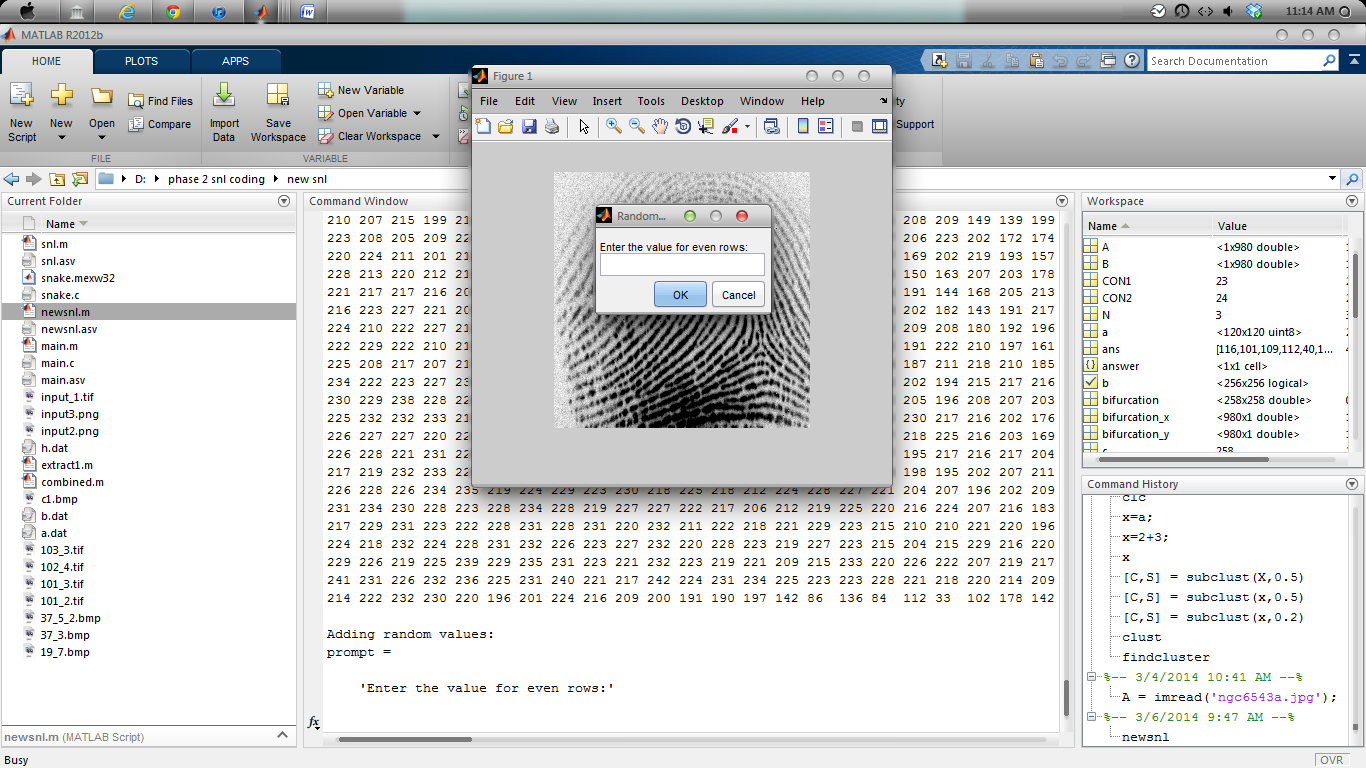
**4.2 ENROLLMENT PHASE**

Combined minutiae template is generated by combining the minutiae feature of the left fingerprint with the orientation of the right fingerprint using existing combined minutiae template generation algorithm as shown in the Fig 4.1



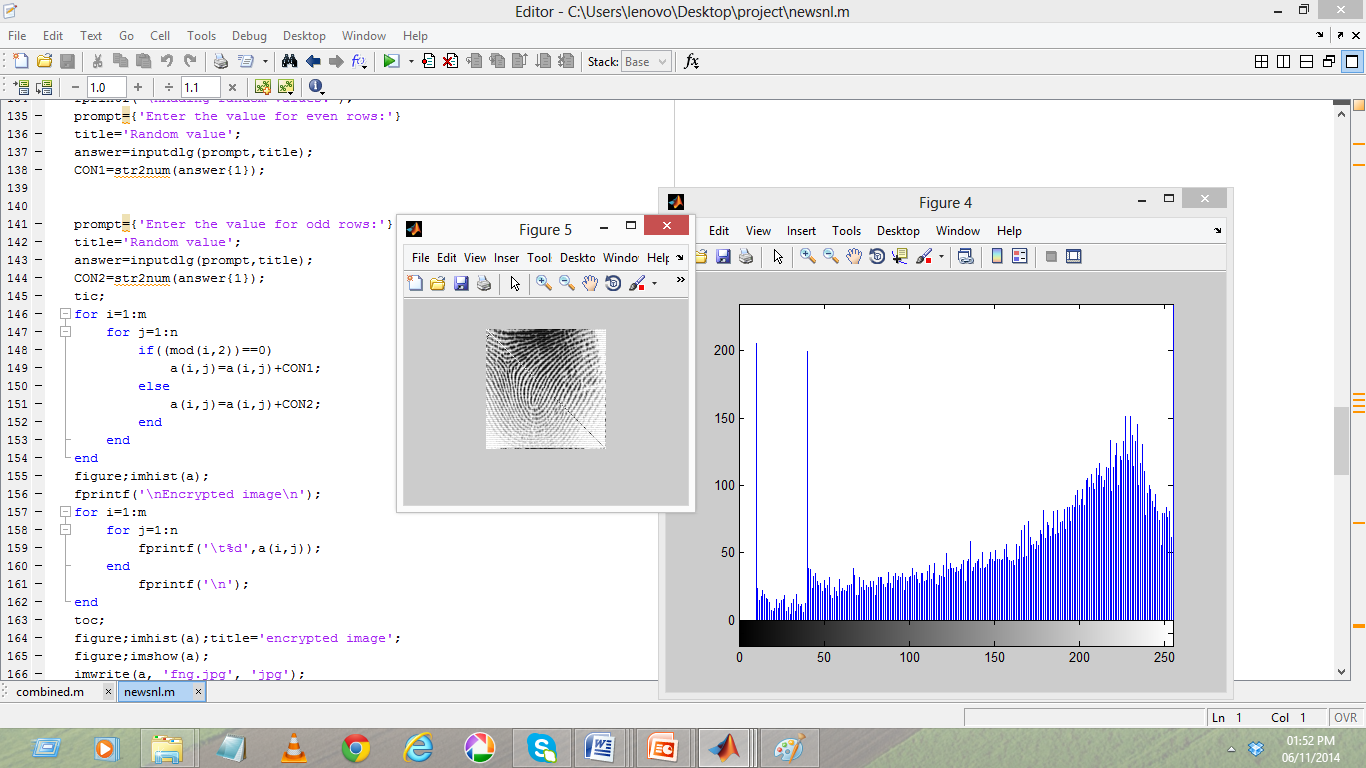
**Figure 4.1 Combined minutiae template**

The combined minutiae template is now subjected to a shuffling mechanism after which SNL algorithm is applied. The second layer of security; insertion of artificial minutiae points is then initiated through a prompt box asking the administrator for the keys to insert the minutiae points in chosen positions. Fig 4.2 shows the fingerprint image after the application of SNL algorithm and a prompt box asking for key value.

****

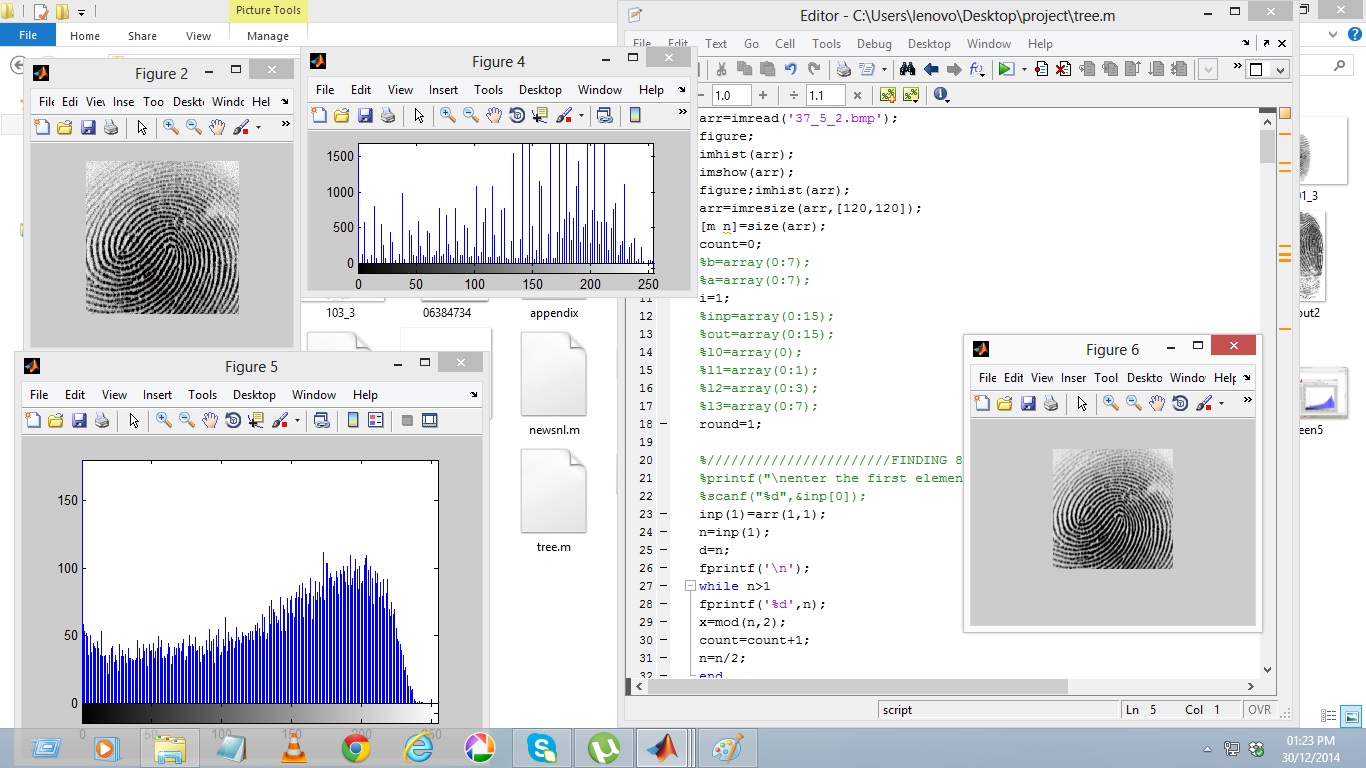
**Figure 4.2 Fingerprint after SNL algorithm**

After artificial minutiae points are inserted with the key values specified by the administrator, the pixel values are shuffled and modified as shown in Fig 4.3.



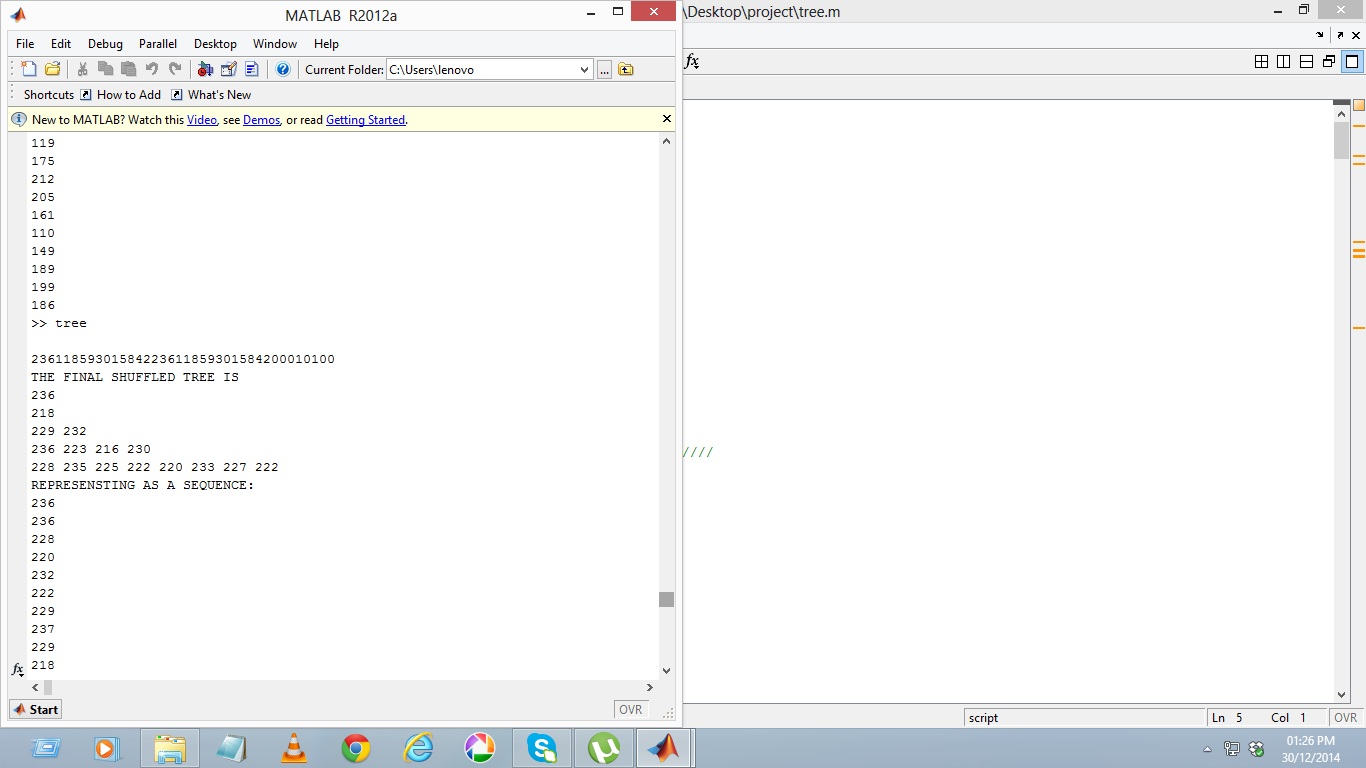
**Figure 4.3 Fingerprint after artificial minutiae points insertion**

The variations in the distribution of the pixel values in the original fingerprint and that after the application of double layered encryption mechanism are denoted in the following Fig 4.4



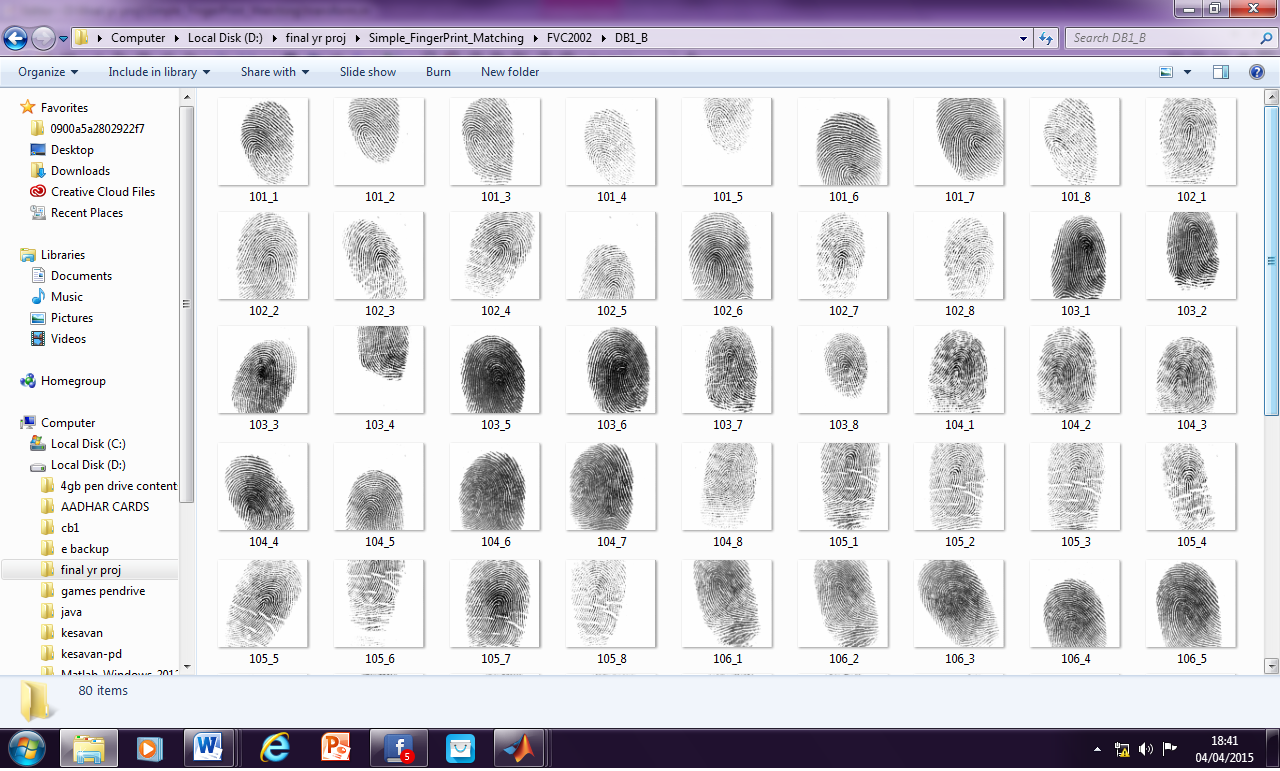
**Figure 4.4 Histogram variation**

A third layer security mechanism is carried out over the resultant template. A tree based shuffling mechanism is applied on the ROI as discussed and the redistribution of the pixel values after the implementation of the algorithm is shown in Fig 4.5. The resulting fingerprint template is then stored in the database. Hence it would be difficult for the hacker to track back the process to obtain the original template.



**Figure 4.5 Tree based shuffling mechanism**

Fingerprints of registered users are subjected to a similar process and stored in the database as shown below

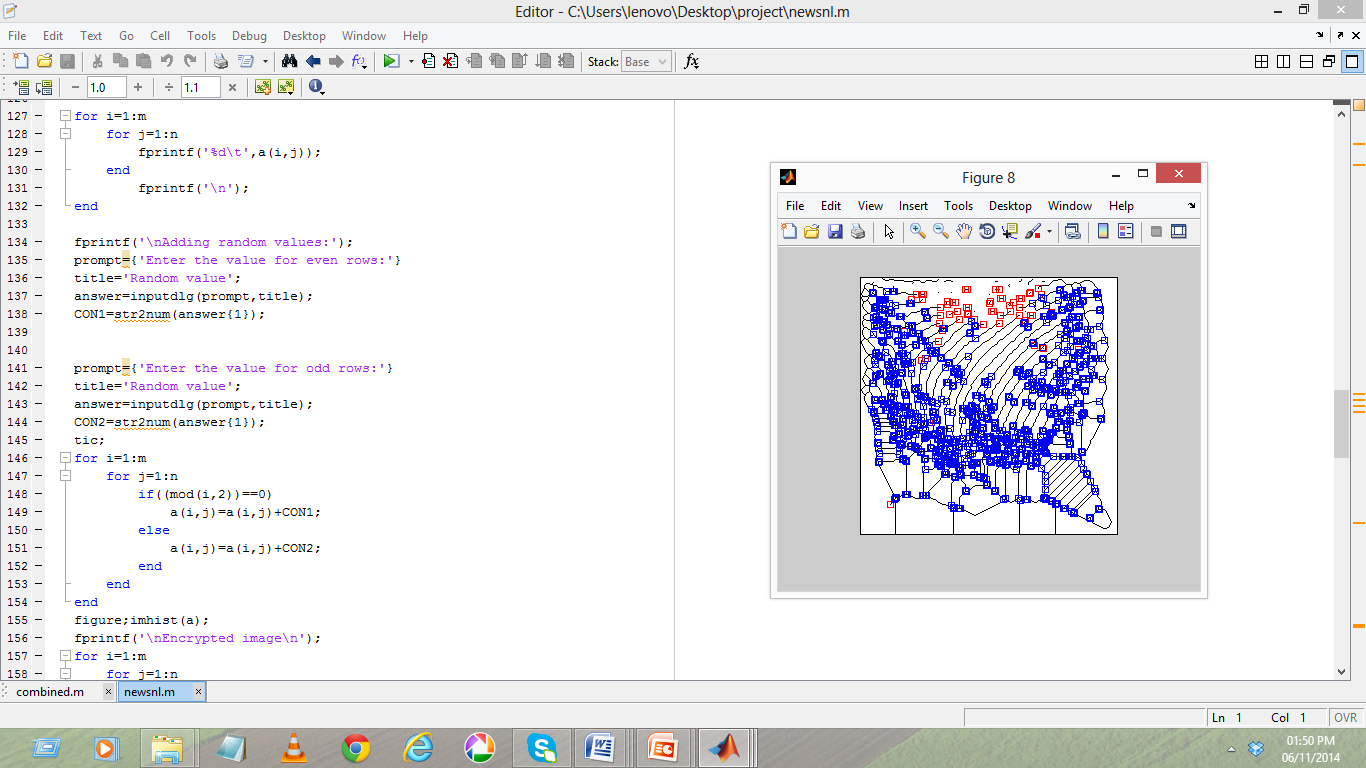


**Figure 4.6 Fingerprint database**

The collected database has about fingerprints of 545 users wherein for each user 8 differently aligned fingerprint of the same finger is captured to check the alignment and matching accuracy of the algorithm.

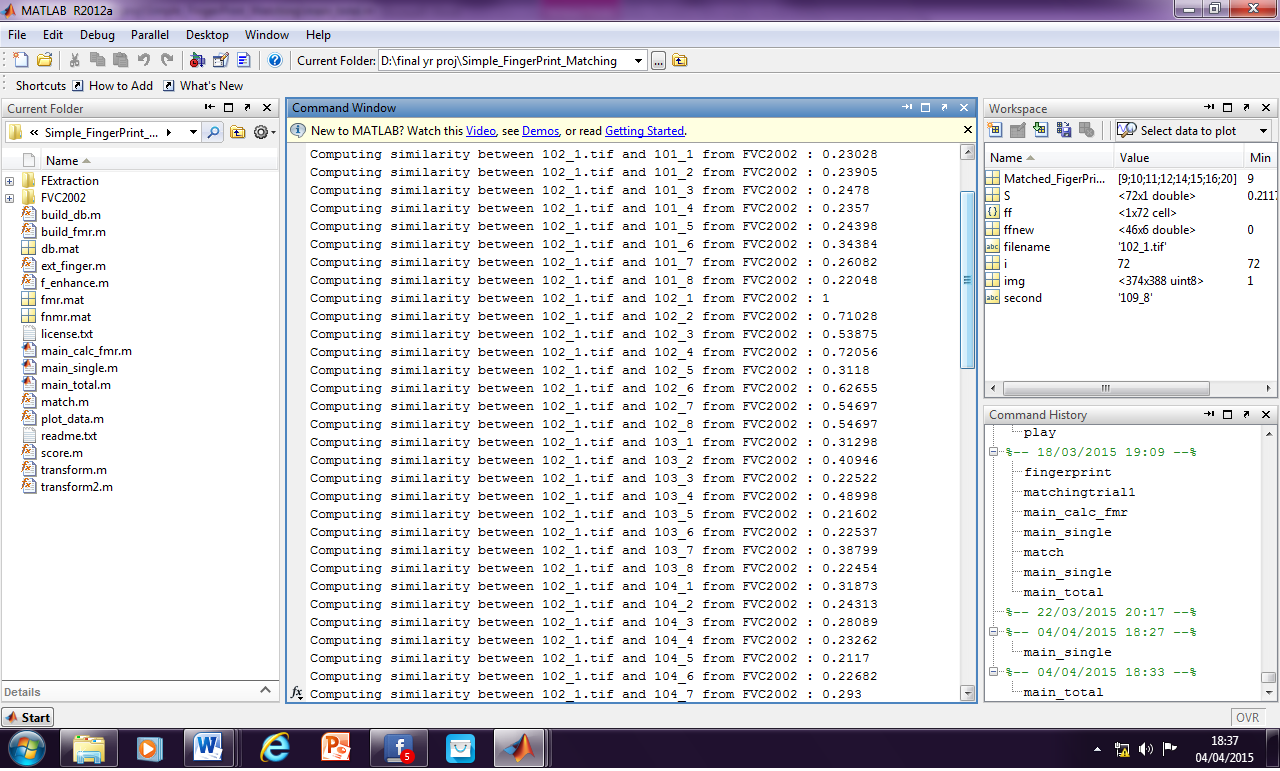
**4.3 AUTHENTICATION PHASE**

In the authentication phase, the query minutia is subjected to similar process and is compared with the stored template. A matching score is calculated and the user is authenticated only if the matching score crosses the threshold. The following Fig 4.7 shows the minutiae feature extraction from the query minutiae after applying the triple layered encryption mechanism.



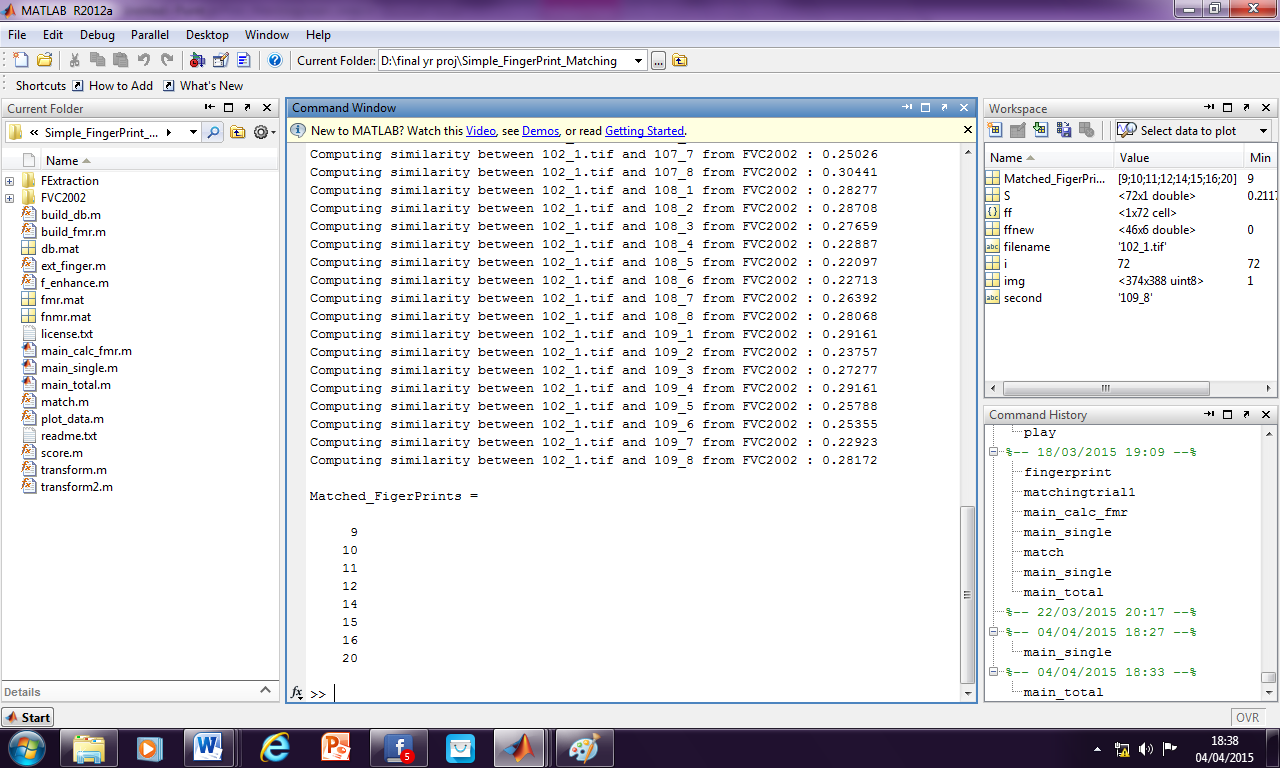
**Figure 4.7 Minutiae feature extraction from query fingerprint**

After subjecting the query fingerprint to alignment processes, it is compared with the rest of the templates to obtain the similarity score. The following Fig 4.8 shows the calculation of similarity score between the input fingerprint and the registered templates.



**Figure 4.8 Similarity score calculation**

Once the similarity scores are calculated, those fingerprints with which the similarity score exceeds a fixed threshold value are found to be the best matching templates. The Fig 4.9 gives the list of all templates that had matched with the input query fingerprint.



**Figure 4.9 Matching of fingerprints**

**4.4 PERFROMANCE ANALYSIS**

Different parameters have been analyzed for the system like the FMR and FNMR. EER is computed using the above values and the accuracy of the system is analysed. These areas discussed below.

A. False Reject Rate

Every fingerprint of one person is compared with fingerprints of other persons and this authentication method is known as False Reject Rate. The FRR is defined as follows,

FRR=x100% (4.1)

Each sample in the subset A is matched against the remaining samples of the same finger to compute the false non match rate (FNMR) (also referred as false rejection rate - FRR). FNMR value for score I is the number of genuine comparisons with score lower than I divided by the total number of genuine comparisons.

B. False Acceptance Rate

For calculating FAR, the imposter match was performed. For imposter match, each test fingerprint is compared with fingerprints belonging to other persons.

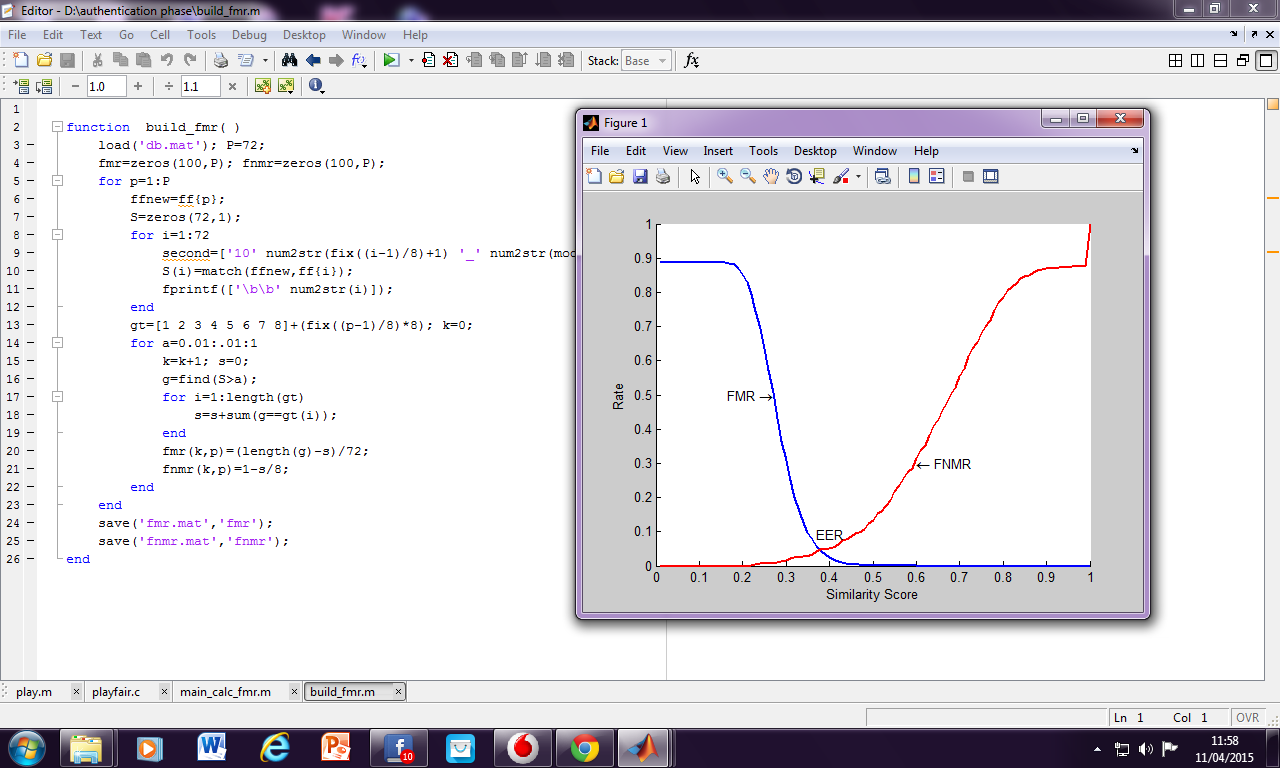
FAR= x100% (4.2)

The first sample of each finger in the subset A is matched against the first sample of the remaining fingers in A to compute the false match rate (FMR) (also referred as false acceptance rate - FAR. FMR value for the score I is the number of impostor comparisons with score higher than I divided by the total number of impostor comparisons. For every score value there is a pair of FMR and FNMR values and when the score increases the FNMR also increases and the FMR decreases and vice versa.

C. Equal Error Rate

Equal Error Rate is the point at which both FRR and FAR becomes equal. It is used as a performance pointer. i.e where FMR(i) = FMNR(i)

Figure 4.10 shows the FMR and FNMR for each similarity score. A graph is plotted with the results obtained. It is found that the system has a very low error rate of 0.5 % FMR and 0.3% FNMR. The point where FMR and FNMR is the EER which is way far less than 0.1%



**Figure 4.10 FMR, FNMR and EER**

##### The following Table 4.1 shows the EER comparisons of the proposed system with that of the existing systems.

**Table 4.1 EER (%) of proposed method with other methods**

|  |  |
| --- | --- |
| Methods | EER % |
| Minutiae based | 6.68 |
| Geometry moments based | 3.57 |
| Zernike moments based | 3.23 |
| Delaunay quadrangle based | 1.08 |
| Proposed method | <0.1 |

For the proposed method EER value is less than the other EER values so the recital of system is improved. The biometric template security is also checked under various security categories and is found to be highly secure. The following Fig 4.11 shows the comparison of the EER of proposed work with other works.

**Figure 4.11 Performance comparison**

**4.5 SUMMARY**

This chapter summarizes the experimental results of the proposed work. The various fingerprint templates that have been tested have been presented. The working of the proposed work has been supported with the screenshots of the implementation work. The accuracy of the proposed system is estimated. The system ensures high protection to the fingerprint templates using a triple layered security mechanism. The proposed technique is highly accurate with a very low EER % which is less than 0.1 %.

**CHAPTER 5**

**CONCLUSION AND FUTURE WORK**

**5.1 CONCLUSION**

The fingerprint template protection using pattern transformation technique has been proposed with keeping in mind the challenges prevailing in the field of biometric template security arena in preserving privacy. Analysis of user behavior or traits is important in the field of security systems. The better we do to secure systems, the more it helps in privacy protection. This project has been visualized in a holistic approach considering the critical issues that are daunting in the domain. The proposed framework for fingerprint template protection has been developed in such a way that it is as easy as possible to implement. The results are fairly consistent when tested with different datasets. Experimental results show that proposed work is highly accurate and secure with a very low EER % of 0.1%.

**5.2 FUTURE WORK**

In this project, a system that covers the major issues like security, privacy and recognition has been developed. In the future work, a better system may be developed that reduces the error rates and further strengthens security. The present system shall be enhanced such that it performs more efficiently and offers better results with greater accuracy, thus ensuring privacy and security.

##### **APPENDIX**

The **DST FIST Sponsored Fingerprint DB 2015** collected from the students of Department of Computer Technology, Madras Institute of Technology, Anna University as a part of the project work for training is done using U are U 4500 Reader. The hardware and software details and requirements of the kit are explained below.

**ONLINE BIOMETRICS KIT – FINGERPRINT**

The U are U 4500 reader is an elegant powerful fingerprint identity machine. With an executive class look and feel U are U 4500 reader is perfect for power users and shared environment. Its design is sleek and compact to conserve valuable desk space but it stays right where you put because of its nice heft and special undercoating as shown below



The U are U 4500 radiates an attractive blue glow that provides and unobtrusive presence in low light environments and also ensure that it does not compete with alarm colors in settings such as health care.

To use, you simple place your finger on the glowing window and the reader quickly scans your fingerprint. For superior user feedback, the red flash indicates that the fingerprint image has been captured. On board electronics calibrate the reader and encrypts the scanned data before sending it over the USB interface

**HARDWARE DETAILS**

* Digital persona U are U 4500 Reader specifications:
* Pixel resolution: 512 dpi ( average x, y over the scan area )
* Scan capture area: 14.6 mm ( nom width at centre ) 18.1 mm ( nom length )
* 8 bit gray scale ( 256 levels of gray )
* Reader size ( approximate : 65 mm x 36 mm x 15.56 mm )
* Compatible with USB 1.0, 1.1 and 2.0 ( full speed ) specifications
* Indoor, home and office use

**FEATURES**

* Blue LED
* Small form factor
* Excellent image quality
* Superior ESD resistance
* Encrypted fingerprint data
* Latent print rejection
* Counterfeit fingerprint rejection
* Rotation invariant
* Rugged
* Works well with dry, moist or rough fingerprints
* Compatible with Windows 7, Vista, XP Professional, 200 and Windows Server 2000, 2003, 2008

**SOFTWARE DETAILS**

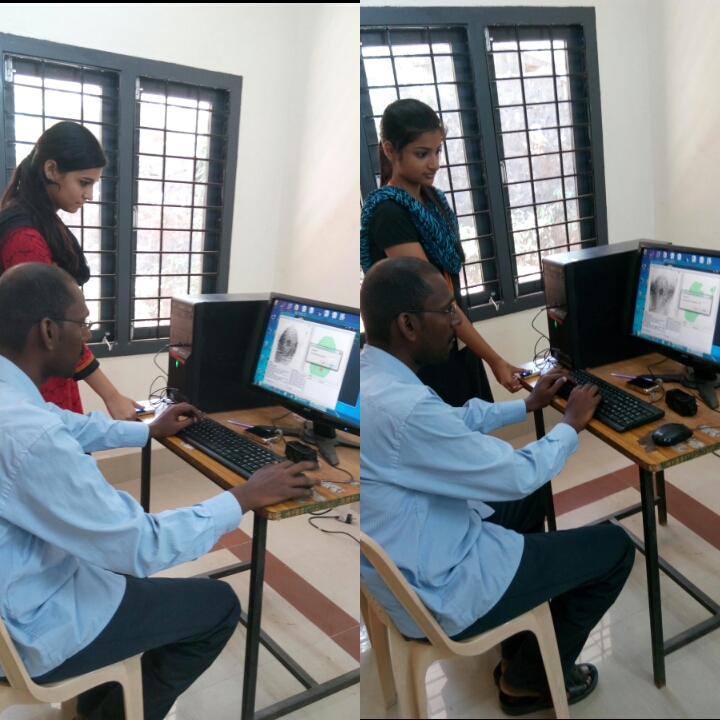
**SDK**

VeriFinger is a fingerprint identification technology intended for biometric systems developer and integrators. The technology assures system performance with fast, reliable fingerprint matching in one to one and one to many modes. VeriFinger is available as a software development kit that allows development of PC and Web based solutions on Microsoft Windows, Linux and Mac OS X platforms.

**SYSTEM REQUIREMENTS**

* System requirements for standard version of VeriFinger SDK
* PC with 500 mega hertz X86 compatible processors or better, or X86\_64 compatible processors, Mac with power PC or Intel core duo
* Mircosoft Windows 2000/2003/XP/Vista/7 or Linux or Mac OS X ( 10.3.9 or newer )
* Fingerprint scanner driver ( users can use the driver included in VeriFinger SDK or can update the driver from scanners manufacturers )

The following image shows the process of fingerprint database collection “DST FIST Sponsored fingerprint DB 2015” using the biometric kit sponsored to the department

.

##### **REFERENCES**

1. Camlikaya E., Kholmatov A. , and Yanikoglu B., “Multi-biometric templates using fingerprint and voice,” Proc. SPIE, Vol. 69440I, pp. 69440I-1– 69440I-9, 2008.
2. Cappelli R. , Erol A. , Maio D. , and Maltoni D., “Synthetic fingerprint image generation,” in Proc. 15th Int. Conf. Pattern Recognition, Sep. 3–7, 2000, Vol. 3, pp. 471–474.
3. Feng J. and Jain A. K. , “Fingerprint reconstruction: From minutiae to phase,” IEEE Trans. Pattern Anal. Mach. Intell., Vol. 33, no. 2, pp. 209–223, Feb. 2011.
4. Jain A. K. and Feng J., “Latent fingerprint matching,” IEEE Trans. Pattern Anal. Mach. Intel., Vol. 33, no. 1, pp. 88–100, Jan. 2011.
5. Jianjiang Feng, Jie Zhou, Proposed, “Orientation Field Estimation for Latent Fingerprint Enhancement” IEEE Trans, pattern anal, and machine intelligence, Vol. 35, no. 4, pp. 925-939, April 2013.
6. Josef Strom Bartunek, Mikael Nilsson, “Adaptive Fingerprint Image Enhancement with Emphasis on Preprocessing of Data”, IEEE transactions on image processing, Vol. 22, no. 2, pp. 644-656, February 2013.
7. Kong A. , Cheung K. -H. , Zhang D. , Kamel M. , and You J., “An analysis of biohashing and its variants,” Pattern Recognit., Vol. 39, no. 7, pp. 1359–1368, 2006.
8. Larkin K. G. and Fletcher P. A. , “A coherent framework for fingerprint analysis: Are fingerprints holograms?,” Opt. Express, Vol. 15, pp. 8667–8677, 2007.
9. Li S. and Kot A. C., “Privacy protection from fingerprint database,” IEEE Signal Process. Let., Vol. 18, no. 2, pp. 115–118, Feb. 2011.
10. Li. S and Alex C. Kot proposed, “A novel system for fingerprint privacy protection”, IEEE Signal Process. Let., Vol. 19, no. 3, pp. 101-112 Dec 2011.
11. Li. S and Alex C. Kot, “Attack uses reconstructed fingerprint,” Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
12. Li. S and Alex C. Kot, “Privacy protection from fingerprint database,” IEEE Signal Process. Let., Vol. 18, no. 2, pp. 115–118, Feb. 2011.
13. Nagar A. , Nandakumar K., and Jain A. K., “Biometric template transformation A security analysis,” in Proc. SPIE, Electron. Imaging,Media Forensics and Security, San Jose, Jan. 2010.
14. Nandakumar K. , Jain A. K. , and Pankanti S., “Fingerprint-based fuzzy vault: Implementation and performance,” IEEE Trans. Inf. ForensicsSecurity, Vol. 2, no. 4, pp. 744–57, Dec. 2007.
15. Othman A. and Ross A., “Mixing fingerprints for generating virtual identities,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
16. Ratha N. K. , Chikkerur S. , Connell J. H., and Bolle R. M. , “Generating cancelable fingerprint templates,” IEEE Trans. Pattern Anal. Mach.Intell., Vol. 29, no. 4, pp. 561–72, Apr. 2007.
17. Ross .A and Othman. A , “Visual cryptography for biometric privacy,” IEEE Transaction. Inf. Forensics, Security, Vol. 6, no. 1, pp. 70–81, Mar. 2011.
18. Ross A. and Othman A. , “Mixing fingerprints for template security and privacy,” Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.
19. Ross A. and for biometric Othman A., “Visual cryptography privacy,”IEEE Trans. Inf. Forensics, Security, Vol. 6, no. 1, pp. 70–81, Mar. 2011.
20. Scheirer W. J. and Boult T. E., “Cracking fuzzy vaults and biometric encryption,” Proc. Biometrics Symp., Sep. 2007, pp. 34–39.
21. Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, Fingerprint Combination for Privacy Protection IEEE Transactions on information forensics and security, Vol. 8, no. 2, pp. 350-360, February 2013.
22. Teoh B. J. A. , Ngo C. L. D. , and Goh A. , “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,”Pattern Recognit., Vol. 37, no. 11, pp. 2245–2255, 2004.
23. Ulugdag U. , “Secure Biometric Systems,” Ph.D. thesis, Michigan State Univ., East Lansing, MI, 2006.
24. Yanikoglu B. and Kholmatov A. , “Combining multiple biometrics to protect privacy,” Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.