**Biometric Pattern Analysis Using Spatio-Frequency Approach for Database Security**

N.sudha ,R.Ashoka Rajan,Dr.P.Anandha Kumar,

Madras Institute of Technology,AnnaUniversity,Chennai.

sudhacse2012@gmail.com,2ashok.tiruchendur@gmail.com,3anandh@annauniv.edu

*Abstract*—The proposed fingerprint recognition system provides fingerprint privacy by using a parallel processing mechanism, row major order based shuffling, snake ladder approach (SNL) and a tree based shuffling mechanism to generate a new virtual identity for fingerprint database security. An existing distinct fingerprint reconstruction approach is used to convert the combined minutiae template into an original fingerprint, which can be matched using minutiae-based fingerprint matching algorithms. During the enrollment, proposed algorithms are used to protect the fingerprint database efficiently. This SNL makes use of techniques such as intermixing, swapping and simulated key insertion to provide new virtual identity and the encrypted image is then subjected to a tree based shuffling mechanism which provides another level of security. The authentication process is a major challenge in database security. Thus the implementation results of the combined and encrypted fingerprint image show very lower error rate with EER = 0.7% than the existing approach. It is tricky to design accurate algorithms capable of extracting features and matching them. Therefore, proposed fingerprint recognition provides dependable and better recital in poor quality images than the existing technique.

Keywords—Fingerprint images, SNL (Snake Ladder Approach), Virtual identity.

1. INTRODUCTION

Biometrics refers to the detection of humans by their uniqueness or traits. It is described as the skill of recognizing an entity based on his or her physical or behavioral attributes. Biometric system generally provides the three functions such as verification, detection and screening.

The difficulty of manipulative a biometric system is based on three main factors viz., accuracy, scale or size of the database, and usability.

The fingerprint is one of the accepted biometric methods used to verify human being**.** Fingerprint recognition system is the most significant biometric technique. It affords consistent means of biometric verification due to features Universality, Distinctiveness, Permanence and Accuracy. It is the technique of identifying an individual and it can be used different applications, such as, medical records, criminal investigation, detection, verification, and cloud computing, communication.

Fingerprint detection involves the location and resolution of the unique characteristics of the fingerprint. The fingerprint is collected of various ‘ridges’ and ‘bifurcation’, which forms the basis of the loops, arches and swirls on the fingertip. The ridges and bifurcation contain different kinds of breaks and discontinuities known as ‘minutiae’. It is from these minutiae that the unique features are located and resolute. There are two types of minutiae points: ridge and valley points.

This paper proposed fingerprint recognition system provides fingerprint privacy by using a snake ladder approach (SNL) to generate a new virtual identity for fingerprint database security.

II. RELATED WORK

The extensive applications of fingerprint techniques in validation systems, shielding the privacy of the fingerprint become an important concern. The conventional encryption is not sufficient for fingerprint confidentiality protection for the reason that decryption is necessary before the fingerprint matching, which exposes the fingerprint to the mugger. Consequently, in recent years, important efforts have been put into mounting specificprotection techniques for fingerprint.

Alex C. Kot et al.[1] And [5], [4] proposed Fingerprint Combination for Privacy Protectiondefensive fingerprint privacy by combining two dissimilar fingerprints provide new identity and stored .They have proposed [1] a fingerprint reconstruction algorithm. Reconstruct a fingerprint image from a stolen united minutiae template and make a fake finger; the attacker may be able to break into other traditional system.[4] Proposed Attack uses Reconstructed Fingerprintrebuilds the fingerprint from minutiae points based on the amplitude and frequency modulated (AM-FM) fingerprint model to trick a system that requires a full print. By removing the spirals in the partial image of the enhanced ridge pattern, the incessant phase can be reconstructed intuitively.

They require reconstructing fingerprint can be used to assemble a fake finger or Directly injected into a communication channel to take in the fingerprint recognition system, which will cause grave security problems.

JianjiangFeng et al.[2] Proposedan orientation Field Estimation for Latent Fingerprint Enhancement. A simple local evaluation approach is used to obtain a primary orientation field of the latent fingerprint. The final direction field for the latent is obtained by finding the grouping of candidates that minimize an energy function. However, the proposed algorithm is still poorer to manually marking, in particular on low-quality latent, and its speed is slow.

S. Li et al. [6] proposed a Novel System for Fingerprint Privacy Protectionthe fingerprint privacy without using a token or key in the enrollment [6]. If it is difficult for attacker to distinguish our template from the minutiae of an original fingerprint. If the combined minutia template is stolen, the complete minutia feature of each fingerprint is not compromised these properties contribute the advantage of our system over the existing fingerprint privacy protection techniques. The algorithm is still inferior to manuallymark, especially inthe low - quality latent, and its speed is slow.

A. Othman at El [7], [15]proposed aVisual Cryptography for Biometric Privacy the image cryptography for imparting confidentiality of biometric information such as fingerprint images, face images, iris codes. The planned approach [7] for de-identifying and storing a fingerprint image. To developed VCS without pixel expansion. But no such scheme presently exists for generating sheets that are not accidental noisy images.

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

Teohet al. [8] Propose a biohashing approach by computing the private products between the user’s fingerprint features and a pseudorandom number. The precision of this approach mainly depends on the key, which is unspecified to be never stolen or shared [9].

Rathaet al. [10] Suggest generating cancelable fingerprint template, applying noninvertible transform on the minutiae. The noninvertible transform is guided by a key, which will frequently lead to a decrease in matching precision. The work in [9] and [10] are shown to be susceptible to intrusion and linkage attacks when both the key and the transformed pattern are stolen [11]. Nandakumaret al. [12] suggest executing fuzzy fault on the minutiae, which is susceptible to the key-inversion attack [13]. Our works in [14] invisibly hide the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the protected thinned fingerprint are stolen. There are only a few schemes [15] –[19] that are able to shield the privacy of the fingerprint without using a key.

However, it requires two separate databases to work together, which is not practical in matching applications. The works in [16] –[18] combine two different fingerprints into a particular new identity either in the feature level [16] or in the image level [17], [18]. In [16], the concept of combining two dissimilar fingerprints into a new identity is first proposed, where the new identity is shaped by combining the minutiae positions extract from the two fingerprints.

The unique minutiae positions of each fingerprint can be secluded in the new identity. However, it is easy for the mugger to classify such a new identity because it contains many more minutiae positions than that of a new fingerprint. The experiment shows that the EER of matching the new identities is 2.1% when the unique minutiae positions are marked physically from the original fingerprints.

A alike scheme is proposed in [19], where the minutiae positions extract from a fingerprint and the artificial points create from the voice are combined to produce a new identity. In this work, the EER are shown to be less than 2%, according to the experimental results.

In [17], [18], the authors first suggest to combine two dissimilar fingerprints in the image level. First of all, each fingerprint is decaying into the continuous component and the spiral component based on the fingerprint FM-AM model [20].

This proposed SNL makes use of techniques such as intermixing, swapping and simulated key insertion to provide new virtual identity. The authentication process is a major challenge in database security. Thus the implementation results of the combined and encrypted fingerprint image show very low error rate with EER performance rate 2.1% than the existing approach.

III. PROPOSED WORK

The proposed work is a fingerprint recognition system for defending fingerprint privacy protection by combining two different fingerprints by applying the snake ladder approach to generate a new virtual identity and applying tree based shuffling technique and after that

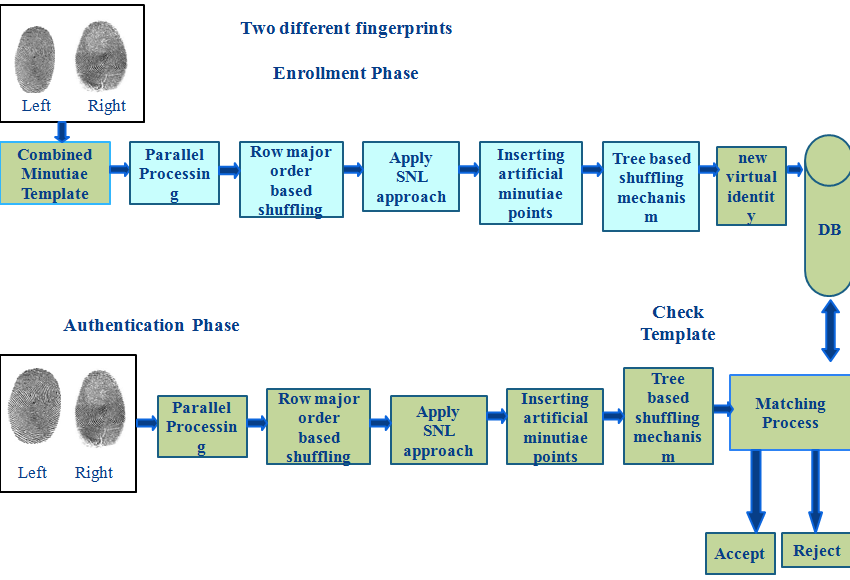


Fig.1.Architecture

it is stored in the fingerprint database.

Thus the new virtual identity is created from two dissimilar fingerprints, encrypting the new virtual identity using snake ladder approach and performing the shuffling operation then store in the database. The matching process [23] is done to increase the recognition a person for security. The fingerprint is one of the accepted biometric methods used to verify human being.

1. COMBINED MINUTIAE TEMPLATE:

Among the obtainable fingerprint reconstruction approaches, our preceding work achieves exceptional performance. In this approach, a combined fingerprint is obtained from a combined minutiae template. However, the work in [21] does not integrate a noising and interpretation step to build the reconstructed fingerprint image real-look alike. Combined minutiae template is generated by extracting minutiae features, orientation of the fingerprints and reference points from both the fingerprints. It is stored as an encrypted image and later on it is followed by the Snake ladder (SNL) approach.

The fingerprint minutiae matching algorithm is to construct the combined minutiae template and stored. [22], [25] this algorithm is defined as the feature level and image level. Feature level is creating the new identity. The analysis provides that it is not easy for the hacker to recover the original minutiae template from a combined minutiae template or a combined fingerprint since it is non-invertible.

1. PARALLEL PROCESSING:

Here a 16x16 pixel values is used where the first 16x16 is divided into a set of 4x4 matrices and each 4x4 is assigned a processor. Then another 12 pixel values are taken where each of the pixels of 9x9 is assigned with a processor. In the next stage,8 pixels are taken where each of the pixels of 4x4 is assigned with a processor. Parallel processing is done here in such a way to implement it efficiently and faster since each pixel matrices are assigned with unique processor for faster computation.



Fig.2.Parallel processing mechanism

1. ROW MAJOR ORDER BASED SHUFFLING:

Assume that the sequence S={x1,x2,….xn} of distinct integers is to be sorted on a mesh-connected parallel computer and then n processors P1,P2,…..Pn are available. The purpose of sorting is to permute the elements.

Here P1 is placed in row j and column k of processor array. When this indexing rule is used the sorted sequence is said to be in row-major order.

0 1 2 3

|  |  |  |  |
| --- | --- | --- | --- |
| P1 | P2 | P3 | P4 |
| P5 | P6 | P7 | P8 |
| P9 | P10 | P11 | P12 |
| P13 | P14 | P15 | P16 |

In the first stage, a 16 pixel values are shuffled by either moving upwards or downwards done by row major order shuffling.

In second phase, 9 pixel values of the matrix are shuffled accordingly and the shuffling mechanism is depicted in Fig.3.It varies for different matrix values.

|  |  |  |
| --- | --- | --- |
| P1 | P2 | P3 |
| P4 | P5 | P6 |
| P7 | P8 | P9 |

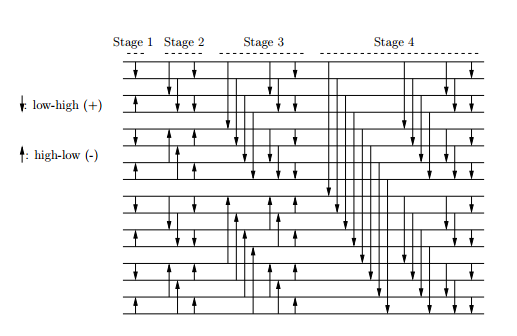


Fig.3. Row major order shuffling

The Fig.3. shown above is row major order based shuffling and the pixel values are either swapped upwards or downwards. In each stage, as shown above the pixel values varies.

D. SNAKE LADDER APPROACH

This proposed Fig (4) SNL makes use of the 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 and make confession to attackers when they hack the fingerprint database.

SNL FLOW DIAGRAM

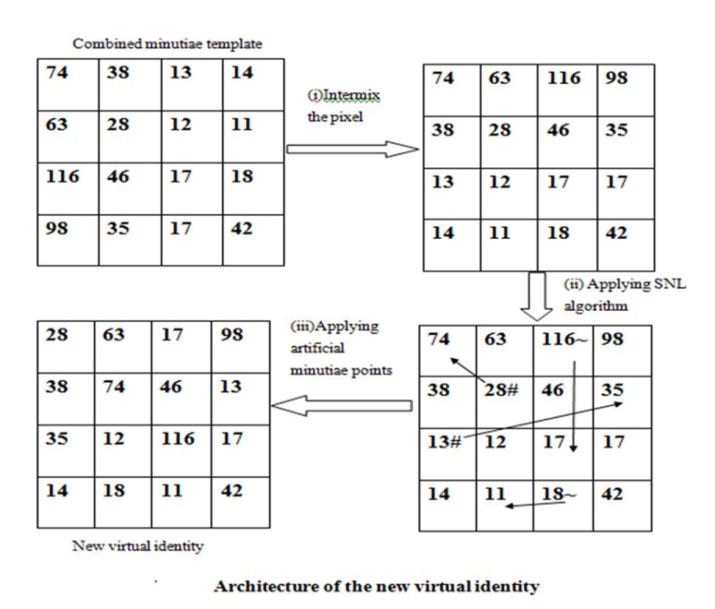
****

Fig.4. Proposed snake ladder approach

The Snake and Ladder game, the pixel values of the image are aligned accordingly. When a snake is encountered, the pixel value goes down, whereas pixel value moves up on seeing a ladder.

Snake(16,20) = LCM(16, 20) = 80

Hence 80 times the value of upper level pixel value comes downwards. The generated gap will be filled by the other pixels.

Ladder(8,2) = BIT. COMPLEMENT(8,2)

= BIT. COMPLEMENT(1000, 2)

= 12

Hence 12 times the value of lower level pixel will go up. The generated gap will be filled by the other pixels.

Different number of snakes and ladders will be inserted in each level to increase the template protection.

**1.Intermixing**

All the pixel values of the image are shuffled to form a new virtual identity. This is done by taking the whole 4\*4 pixel matrix and performing permutations on the pixels and finally a different set of shuffled pixel matrix is obtained which is unique from the original.Thus thereby the hacker does not know what compuataion is done in order to find the original pixel values. This is carried further by adding another level of security which is the (SNL)Snake ladder approach.

Where,

(m,n) is the image size or the total size of matrix.

(i,j) is the pixel value

‘a’ is fingerprint image

Intermixing technique shuffle the pixel locations of the matrix depending on computations.An encrypted image is obtained as a result of intermixing.

**2.Applying SNL**

Based on the Snake and Ladder game the pixel values of the image are aligned. In this SNL method, the technique is performed on the intermixed pixels of the matrix. This adds to another layer of security since again the pixels positions are interchanged in the matrix. When a snake is encountered pixel value goes down, whereas pixel value moves upon seeing a ladder .This depends on the number of times the pixel value goes up or down.

Where,

(x,y) is given values for swapping SNL game technique.

**3.Artificial minutiae points**

Later on minutiae points are inserted to enhance the security. This is done by getting input from the user based on even rows and odd rows.

Prompt box gets value from the user and based on it the pixels are again rearranged in the 4x4 matrix. A new virtual identity is obtained finally and the main advantage of artificial minutiae point is that the hacker does not know what input is taken to shuffle the pixel values. This adds to another layer of security and hence an encrypted image different from that of original image is obtained.

1. **SNL ALGORITHM**

**INPUT: FINGERPRINT IMAGE**

**OUTPUT: ENCRYPTED IMAGE**

Read fingerprint image.

Generate the Combined image used to following eq(1),(2)&(3).

Applying the encryption technique.

Read image[a] // Display pixel value

for i ϵ {1...m-1} do //Performing Permutation. Read img[i]

for j ϵ {1:n-1} do

Read img[j]

k=a(i,j);

a(i,j)=a(m-i,n-j);

a(m-i,n-j)=k;

if (i==j)

end,end

display(a)

for i ϵ{1:m} do //Snake and Ladder

for j ϵ{1:n} do

if(i==x)

if(j==y)

a(x,y)=a(x,y)+a(i,j);

a(i,j)=0

end

end

for j ϵ{1:m} do //Artificial value added

for j ϵ{1:n} do

if((mod(i,2))==0)

a(i,j)=a(i,j)+CON1;

else

a(i,j)=a(i,j)+CON2;

end

end

display(a) //Display encrypted image

If count at aij> aij+1// Binary operation

then

aij=1Elseaij=0

aij = aij-1 ^ aij+1// Performing XOR operation

//Generate the Graph and stored in database Fig(3).

end

**INPUT: ENCRYPTED IMAGE**

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

Read encrypted image.

Applying the encryption technique.

Read image[a] // Display pixel value

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

(here 221=11011101=> level 3)

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 fisrt 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 )

E. TREE BASED SHUFFLING MECHANISM

F. MATCHING PROCESS

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**

Initialize count to the size of the image along x

Alpha value ranges from -5 to 5

For i=1 to count

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

T = B /

End

End

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;

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}.

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 )

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.

IV. IMPLEMENTATION

The SNL approach has the following three techniques.

Permuted image shows the intermixing the pixel values within the combined fingerprint image.

Fig.3. shows the permuted image after intermix of the pixel values and then a prompt box to enter the artificial minutiae points at various locations to again shuffle the values. It asks for input values of even and odd rows and corresponding input values are added to the intermixed pixel values and thus a new virtual identity is obtainned.

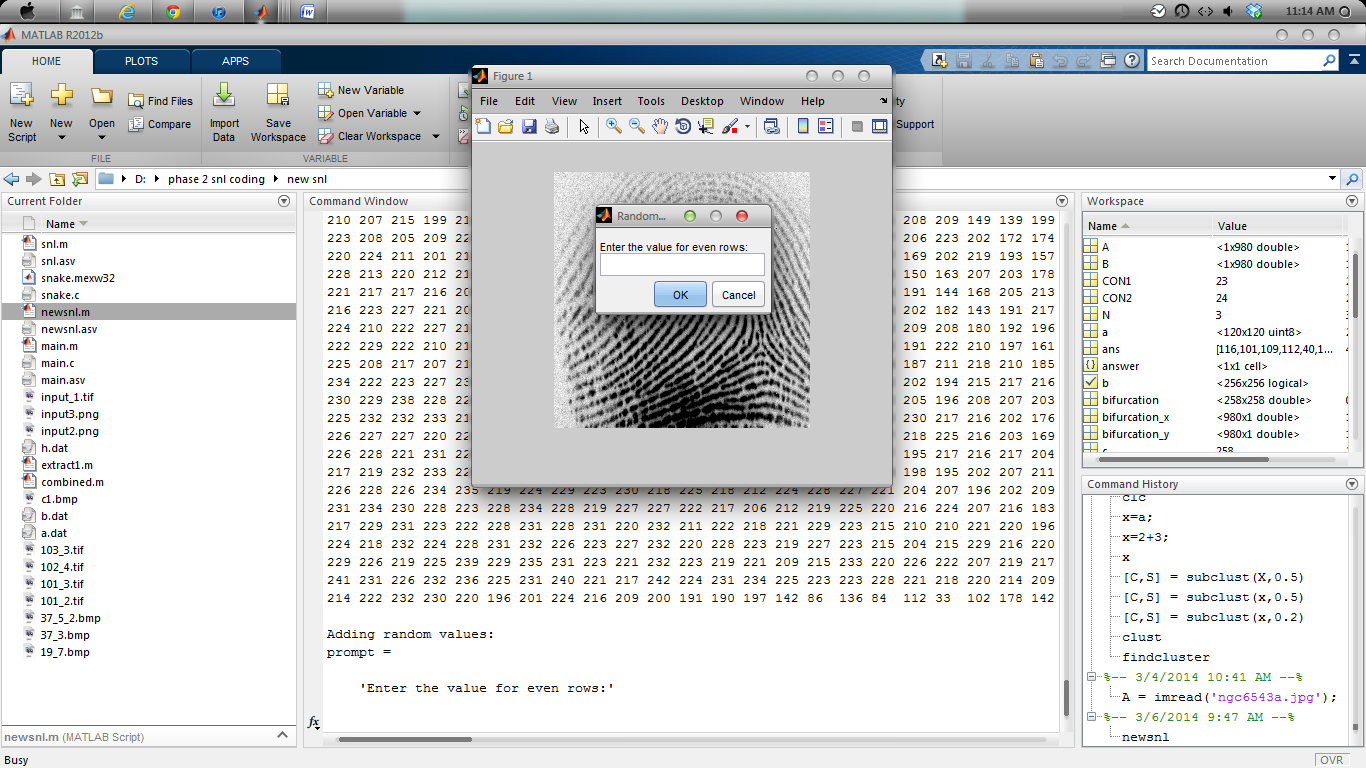
****

Fig.5. Permuted image

In this encrypted image used to swapping pixel based on snake ladder technique after that artificial key values introduced on the image.

**Shows the combined fingerprint image modification result between original fingerprint image and (SNL) encrypted image.**

The Original fingerprint image vs the Encrypted image is shown and thus the difference in the images is seen in Fig.6 below.

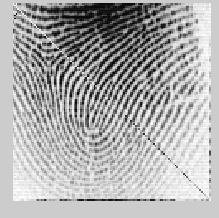


Fig.6. Original image and Encrypted Image(SNL)

The values of the histogram are plotted based on the initial pixel values of the 4x4 matrix. There exists variations among the two histograms as shown in the Encrypted image in Fig.7.

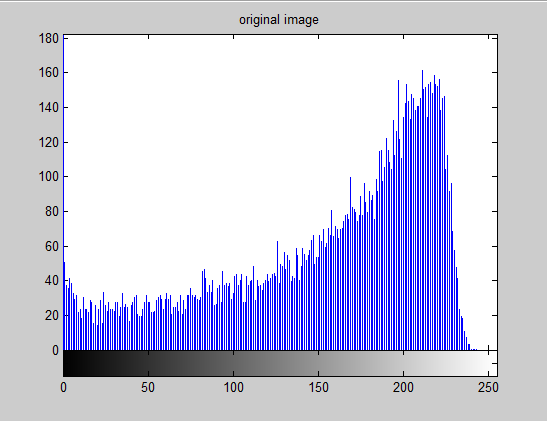


Fig.7. Histogram of Original image

Fig.8. shows the histogram of the encrypted image after SNL approach and thus the variations from Fig.5. and Fig.6. is seen through the histograms. This is obtained as a result of different computations and approaches performed on the 4x4 matrix.

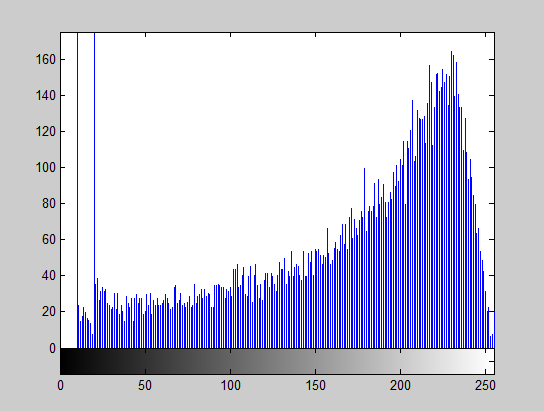


Fig.8. Histogram of Encrypted image(SNL).

After the insertion of artificial minutiae points the sequence of the matrix of pixel values are displayed in the output window as shown in Fig.9 below:

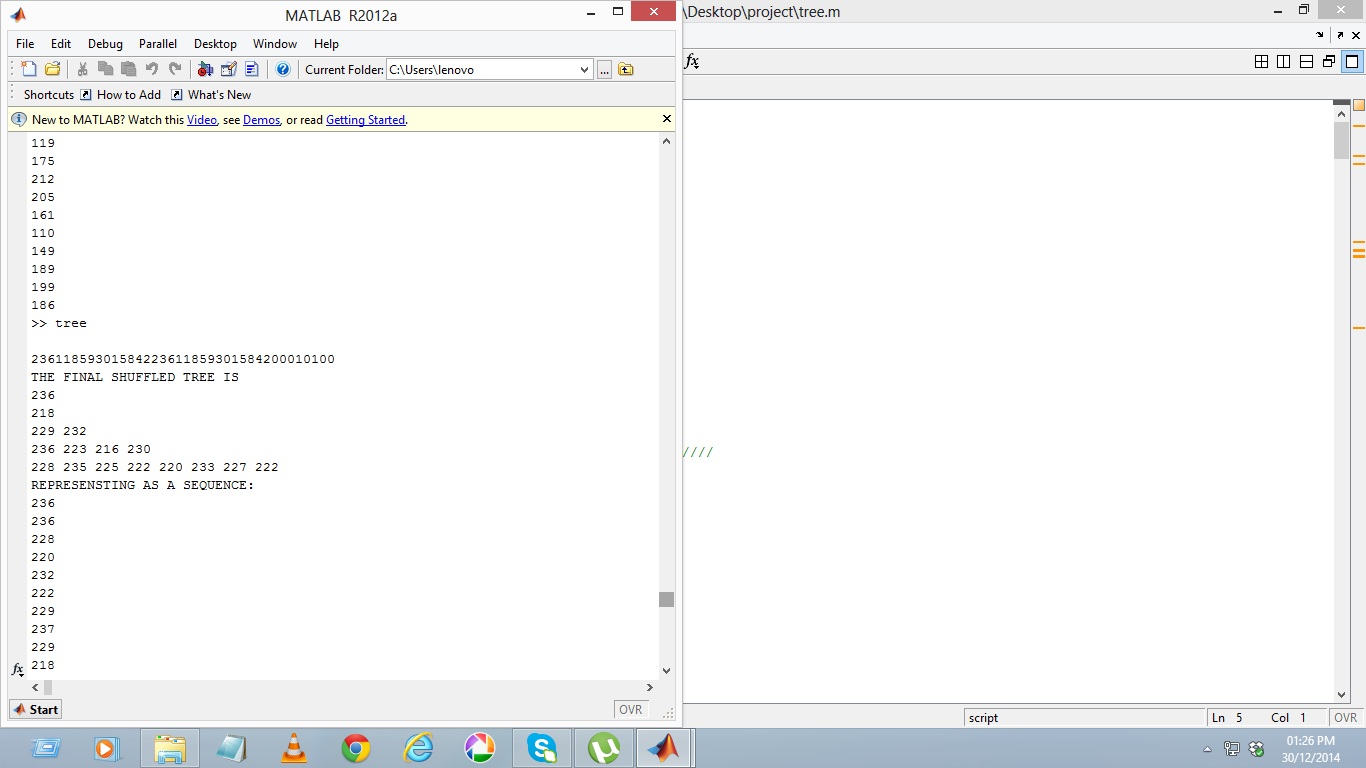


Fig.9. Sequence output

The overall tree shuffling approach and its implementation is shown in Fig.10. along with the tree algorithm below:

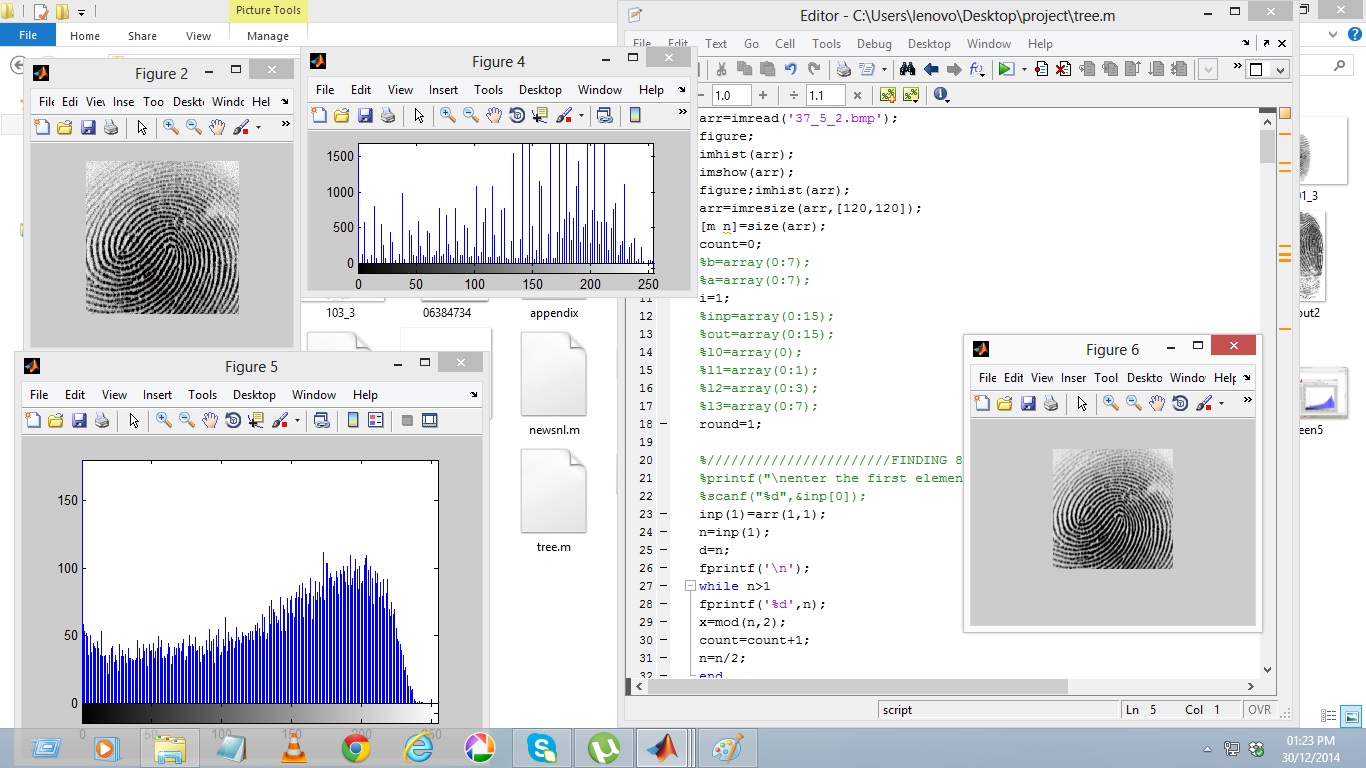


Fig.10. Tree shuffling approach

During the authentication phase, similarity score is computed as shown in Fig.11 ,between the query fingerprint and the rest of the fingerprints in the data base. Those templates with which the similarity score exceeds the threshold value are found to be the matched templates.

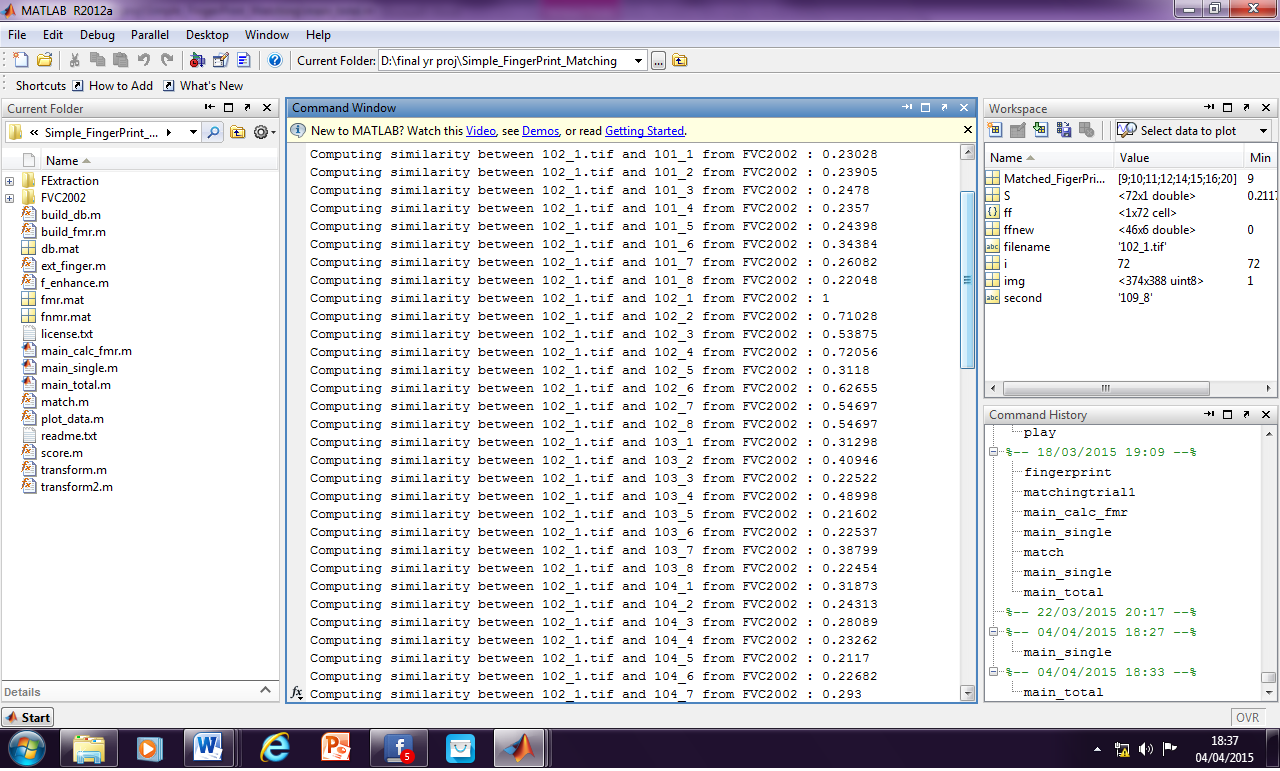


Fig.11 . Computing similarity scores

V. PERFORMANCE ANALYSIS

Fingerprint recognition system is tested on a different fingerprint dataset (FVC2002 and FVC2004).The database is divided into two different parts, training data set and authentication dataset. Every person has eight fingerprints in the database. Amongst these images some of the images belong to class 1 (R, L, M) from dataset and some of them belongs to class 2 (A, W) different parameters that have been analyzed for the system performance, such as, false reject rate, false acceptance rate, equal error rate, EER performance study of different methods, recognition rate, recall a time per pattern analysis. These areas discussed below.

***A. False Reject Rate***

To calculate FRR, the authentic match was performed. For authentic match, every fingerprint of each person is compared with other fingerprints of the same person. The FRR is defined as follows,

FRR= x100% (5)

***B. False Acceptance Rate***

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

**C. Equal Error Rate**

The EER is used as a performance pointer. The EER indicates the point where the FRR and FAR are equal.

FAR= x100% (6)

***D. EER Performance Study***

Following Table I create different EER values for dissimilar methods, EER is calculated by averaging FAR and FRR.

TABLE I

EER (%) OF PROPOSED SNL METHOD WITH OTHER METHODS

|  |  |
| --- | --- |
| Methods | EER % |
| Minutiae based | 6.68 |
| Geometry moments based | 3.57 |
| Zemike moments based | 3.23 |
| Proposed | 2.1 |

The following is the graph corresponding (Equal Error Rate) to the above table.

The graph shows eq (5), (6) the different values of EER for the different methods. For proposed method EER value is less than the other EER values so the recital of system is improved.

TABLE II

RECOGNITION RATE

|  |  |  |  |
| --- | --- | --- | --- |
| Classifier | Training  Dataset | Testing  Dataset | Average  Recognition  Rate |
| SNL | **100%** | **80%** | **90%** |

The recognition rate of SNL for training and testing dataset are following Table II. After receiving class of fingerprint and ID, it needs to authenticate that fingerprint image. So comparison measure is used for verification of testing fingerprint.

VI. CONCLUSION

This system provides the security using a snake ladder approach by swapping the fingerprint features that are extracted by applying various shuffling mechanisms. Thus the new virtual identity is stored in the database. In the authentication process, two query fingerprints from the different two fingers that are registered into authentication system. This forms the fingerprint matching process for matching the two query fingerprints beside the enrolled template. To achieve the EER rate 2.1%.This fingerprint recognition system of future work is used in cloud security and it makes use the secured minutiae template from the database. Fingerprint security is used in android applications mobiles and bank security system. Although studying user behavior is a primary focus in the field of computer security, it is significant. The better we do to secure systems, the more likely the weakest component of the system would be users. Thus security is being provided and hence retrieval of data from database is difficult thus providing suitable security.

##### References

1. 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.
2. 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.
3. 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.
4. S. Li and A. C. Kot, “Attack uses reconstructed fingerprint,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
5. S. Li and A. C. Kot, “Privacy protection from fingerprint database,” IEEE Signal Process. Let., vol. 18, no. 2, pp. 115–118, Feb. 2011.
6. S.Li and A. C. Kot proposed, “A novel system for fingerprint privacy protection”, IEEE Transaction, Dec 2011.
7. A. Ross and A. Othman, “Visual cryptography for biometric privacy,” IEEE Transaction. Inf. Forensics, Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.
8. B. J. A. Teoh, C. L. D. Ngo, and A. Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,”Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.
9. A. Kong, K. -H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of biohashing and its variants,” Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006.
10. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” IEEE Trans. Pattern Anal. Mach.Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.
11. A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template transformation A security analysis,” in Proc. SPIE, Electron. Imaging,Media Forensics and Security, San Jose, Jan. 2010.
12. K. Nandakumar, A. K. Jain, and S. Pankanti, “Fingerprint-based fuzzy vault: Implementation and performance,” IEEE Trans. Inf. ForensicsSecurity, vol. 2, no. 4, pp. 744–57, Dec. 2007.
13. W. J. Scheirer and T. E. Boult, “Cracking fuzzy vaults and biometric encryption,” in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.
14. S. Li and A. C. Kot, “Privacy protection from fingerprint database,” IEEE Signal Process. Let., vol. 18, no. 2, pp. 115–118, Feb. 2011.
15. A. Ross and A. Othman, “Visual cryptography for biometric privacy,”IEEE Trans. Inf. Forensics, Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.
16. B. Yanikoglu and A. Kholmatov, “Combining multiple biometrics to protect privacy,” in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.
17. A. Ross and A. Othman, “Mixing fingerprints for template security and privacy,” in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.
18. A. Othman and A. Ross, “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.
19. E. Camlikaya, A. Kholmatov, and B. Yanikoglu, “Multi-biometric templates using fingerprint and voice,” Proc. SPIE, vol. 69440I, pp. 69440I-1– 69440I-9, 2008.
20. K. G. Larkin and P. A. Fletcher, “A coherent framework for fingerprint analysis: Are fingerprints holograms?,” Opt. Express, vol. 15, pp. 8667–8677, 2007.
21. A. K. Jain and J. Feng, “Latent fingerprint matching,” IEEE Trans. Pattern Anal. Mach. Intel., vol. 33, no. 1, pp. 88–100, Jan. 2011.
22. J. Feng and A. K. Jain, “Fingerprint reconstruction: From minutiae to phase,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp. 209–223, Feb. 2011.
23. R. Cappelli, A. Erol, D. Maio, and D. Maltoni, “Synthetic fingerprint image generation,” in Proc. 15th Int. Conf. Pattern Recognition, Sep. 3–7, 2000, vol. 3, pp. 471–474.
24. U. Ulugdag, “Secure Biometric Systems,” Ph.D. thesis, Michigan State Univ., East Lansing, MI, 2006.
25. C. L. Wilson, G. T. Candela, and C. I. Watson, “Neural network fingerprint classification,” J. Artif. Neural Netw., vol. 1, no. 2, pp. 203–228, 1994.