A NOVEL DATA ENCRYPTION TECHNIQUE BY GENETIC CROSSOVER OF ROBUST BIOMETRIC KEY AND SESSION BASED PASSWORD

Tanmay Bhattacharya[1], Sirshendu Hore [2], Ayan Mukherjee [3] and S. R. Bhadra Chaudhuri [4]

[1] Sr. Lecturer, Dept. of IT, JIS College Engineering, Kalyani, West Bengal, India.
tb.jisce@gmail.com

[2] Lecturer, Dept. of CSE, Hooghly Engineering & Technology College, Pipulpati,Hooghly, West Bengal, India.
shirshendu_hore@yahoo.com

[3] Lecturer, Dept. of CSE, Institute of Science & Technology, Chandrakona Town,Paschim Medinipur, West Bengal, India.
ayanmca@gmail.com

[4] Professor, Dept. of E&TC Engg., Bengal Engineering & Science University, Shibpur, Howrah, West Bengal, India.
prof.srbc@gmail.com

ABSTRACT

In Fingerprint based Biometric authentication image of the fingerprint can be scanned and can be used later on for the purpose of authentication. So this process does not provide very high security. This paper proposes another level of security by using the concept of combined key. The key is obtained by crossing over of the Session key generated from the password given by the legitimate user and the Biometric key generated from the fingerprint of the same user. The proposed approach trained the system by Artificial Neural Network in such a way that a small portion of the fingerprint is enough to generate the Biometric key which minimizes the chance of false rejection. So in this approach there is a significant improvement of the traditional authentication techniques.

KEYWORDS

ANN; Minutiae; Sessionbased; Training; SHA-512, Crossover;

1. INTRODUCTION

Fingerprints have long been used in the identification of individuals because of a well-known fact that each person has a unique fingerprint. Classification is usually performed by noting certain features. The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. The three basic patterns of fingerprint ridges are Arch, Loop, and Whorl. Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice only ridge ending and ridge bifurcation minutiae types are used in fingerprint identification. All popular AFIS are minutiae-based [2] [4] [5] [6]. Usually each minutiae is described by the position in the coordinate, the direction it flows and the type, whether it is ridge ending or bifurcation. [7] [8] [9] [10] [12] [13].Figure 1 illustrates the structure of Minutiae.

DOI : 10.5121/ijnsa.2011.3209

Figure 1: Minutiae (a) Ridge ending (b) Bifurcation

Artificial Neural Network: **A**rtificial neural networks are constituted of artificial neurons. An ANN is a system consisting of processing elements (PE) with links between them. A certain arrangement of the PEs and links produce a certain ANN model, suitable for certain tasks [1] [3]. A Multi-Layer Perceptron (MLP) is a kind of feed-forward ANN model consisting of three adjacent layers; the input, hidden and output layers [1]. Each layer has several PEs. Figure 2 illustrates the structure of a MLP

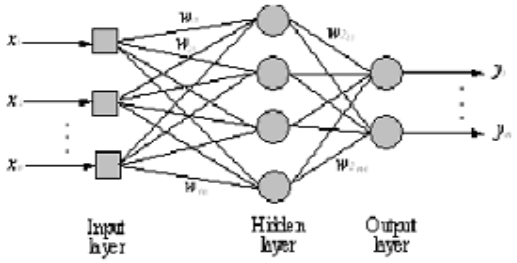

Figure 2: A schematic diagram of a MLP neural network

2. PROPOSED ALGORITHM

Following are the main steps of proposed algorithm.

a. Biometric Key Generation
   - Step 1 Image Acquisition
   - Step 2 Enhancement of the Image
   - Step 3 Feature extraction
   - Step 4 Training with different sample images using ANN
   - Step 5 Template Finger print is obtained
   - Step 6 Biometric Key of 512 bit is generated from the given template.

b. Session Key generation
c. Generation of two intermediate keys by genetic crossing over of Biometric key and Session key.
d. Final Encryption Key generation
e. Encryption of data using Final Encryption Key once fingerprint is match with the template.
f. Decryption of data is done using the Encryption key after fingerprint is match with the template.

The sequence of steps for complete authentication process is given in the schematic diagram. Figure 3 illustrates the scheme.

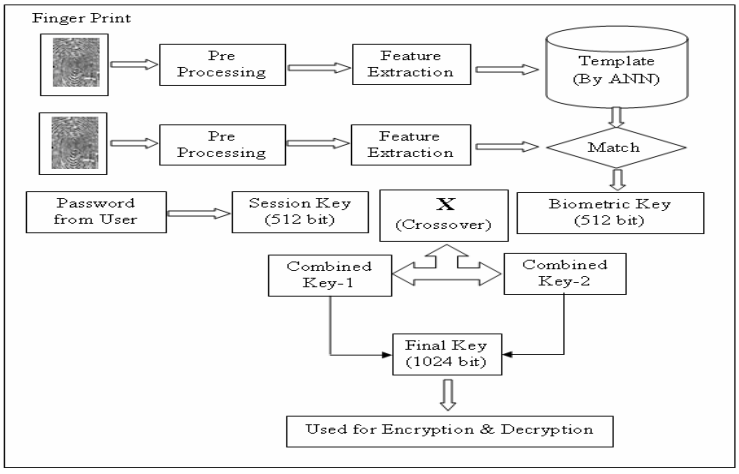

Figure 3: Schematic diagram: The sequence of fingerprint authentication process

3. EXPLANATION OF ALGORITHM

Following are the steps involved in the Biometric Key generation

Step 1: In the initial phase the Fingerprint image is obtained using Bio-sensor scanner which is a flatbed scanner with 600 DPI.

Step 2: Then the image is preprocessed to remove the noise using various preprocessing techniques like segmentation, Normalization, Orientation, Ridge frequency estimation and, Gabor filtering. Figure 4 illustrate the Image enhancement process.

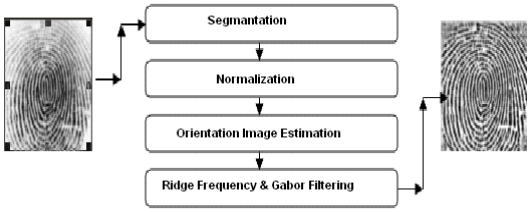

Figure 4: A schematic diagram of a Image Enhancement

Step 3: Enhanced image is then binaries and thinning operation is performed to make the ridges single pixel width. Try to find the location of "1" in the thinned image. The number "1" basically represent the ridges. Taking a '3*3' window mask with 1 as a starting point finding the absolute difference between the center pixel and neighborhoods pixel. If the value is 1(ridge ending) or 3 (bifurcation) then find the angel at which the ridge is moving. Store the coordinates, angles and the calculated values. Figure 5 illustrate enhanced image, Thinned image and image with minutiae points.

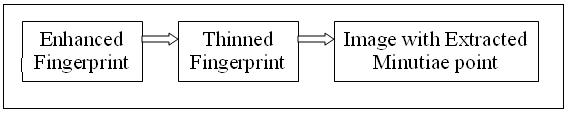

Figure 5: A schematic diagram of (a) Enhanced image, (b) Thinned Image and (c) Minutiae Point

Step 4: Before the ANN training the data was divided into three datasets; the training, validation and test. Here data are Minutiae points (ridge ending and bifurcation) which are extracted from a set of fingerprint images. The training set was used to train the MLP, the validation set was used for early-stopping of the training process and the test set was used to evaluate the MLP performance after completion of the training process. The training data set consist of different sample images.

Steps involved:

Forward propagation: The output of each node in the successive layers is calculated

$$O \text{ (output of a node)} = 1/(1+\exp(-\Sigma W_{ij} x_i)) \quad \text{(a)}$$

The Error E (Im) of an image pattern Im is calculated with respect to Target (T)

$$E(Im) = 1/2(\Sigma T(Im) - O(Im))\,2 \quad \text{(b)}$$

Reverse Propagation: The error δ for the nodes in the output layer is calculated

$$\delta(\text{output layer}) = o(T) - o(\text{Im}) \quad \text{(c)}$$

The new weights between output layer and hidden layer are updated

$$W(n+1) = W(n) + \acute{\eta}\,\delta(\text{output layer}) \quad \text{(d)}$$

The training of the network is stopped when the desired mean square error (MSE) is achieved

$$E(MSE) = \Sigma E(Im) \quad \text{(e)}$$

Step 5: A Template is created using the training sets .The implementation and simulation were carried out with the aid of neural networks built in function using Matlab. (MATLAB7.5.0 (R2007 b)).

Step 6: A biometric key of length 512 bit is generated using SHA512 hash algorithm. With SHA512 a variable-length message is converted into a fixed-length output of 512 bits. The input message is broken up into chunks of 1024 -bit blocks (sixteen 64-bit little endian integers); the message is padded so that its length is divisible by 1024. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 128 bits less than a multiple of 1024. The remaining bits are filled up with a 128-bit integer representing the length of the original message; after initialization of SHA512 buffer with a Eight-word buffer (A,B,C,D,E,F,G,H) ,compute the message digest and finally process message in 16-word blocks to get the output. Figure 6 illustrates the Biometric key generation process. Figure 6-A illustrates the Key Generation process with SHA512

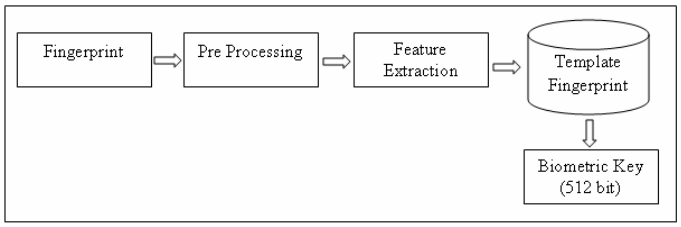

Figure 6: A schematic diagram of Biometric key Generation

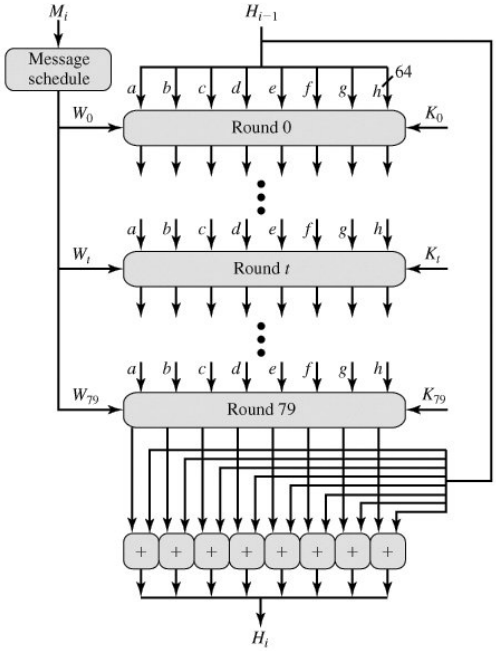

Figure 6-A: A schematic diagram of key Generation process with SHA512

Step 7: Taking a session based password from the user generate a session key of length 512 bit with SHA512 key generation algorithm using step 6. Figure 7 illustrates the Session key generation process.

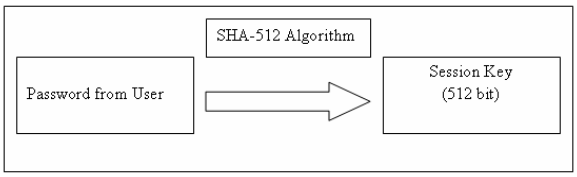

Figure 7: A Session key of length 512 bit is generated

Step 8: Genetic Crossover operation is applied between the Biometric key (512 bit) and session key (512 bit) to generate two combined keys. Figure 8 and Figure 18 illustrates the generation process of Combined Key -1 and Combined Key -2.

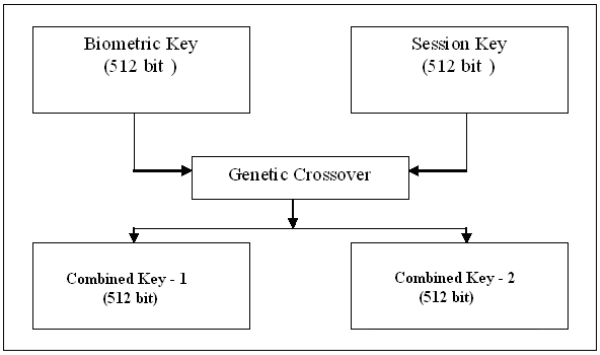

Figure 8: Two combine keys are generated by Crossover

Step 9: The Final Encryption key of length 1024 bit is generated by combining Combined Key -1 and Combined Key -2. Figure 9 and Figure 18 illustrate the Final Encryption Key generation process.

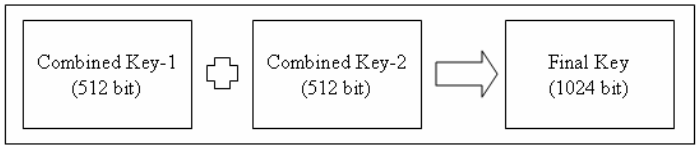

Figure 9: A Final Encryption key of length 1024 bit is generated

Step 10: Taking the File from the user encrypts the data using the Final Encryption key. After taking the file from the user store it in a temporary array after converting the character of the file into their corresponding binary format. Stored the binary values in the 8x8 matrix which is filled up row wise where each row corresponds to a single character. Perform columnar transposition on the matrix. Finally perform the bitwise AND operation on the data using Encryption key. Given file is now encrypted.

Step 11: Taking the Sample fingerprint from the user extract the feature and compare it with the template to find whether the matching score is within the threshold. If it is within the range then generate the Biometric key (512 bit) from the template. A session key (512 bit) is created after accepting the password from the user. The Final Encryption key (1024) is generated using the combined key -1 and combined key-2. Decrypt the encrypted file using the Final Encryption key.

4. RESULTS AND DISCUSSIONS

In this section, we have presented the experimental results of the proposed approach, which is implemented in MATLAB (Matlab7.5.0 (R2007b)) we have tested the proposed approach with different sets of input images. Initially Fingerprints are scanned using standard Bio-sensor scanner with required resolution. As there can be some imperfection in the capture of fingerprint due to lighting condition as well as dirt in the fingerprint enhancement has been done followed

by binarization and thinning. Minutiae points are than extracted from the fingerprint. Figure 10 illustrate the different stage of the fingerprint image.

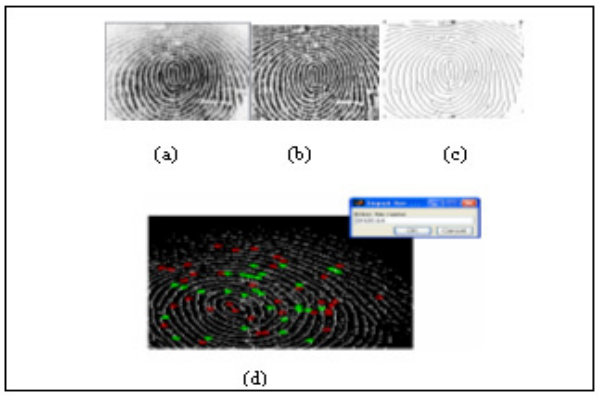

Figure 10: (a) Raw Image, (b) Enhanced Image, (c) Thinned Image and (d) Image with Minutiae points.

The Figure 11 illustrates the schematic diagram of training process using ANN based on extracted Minutiae points

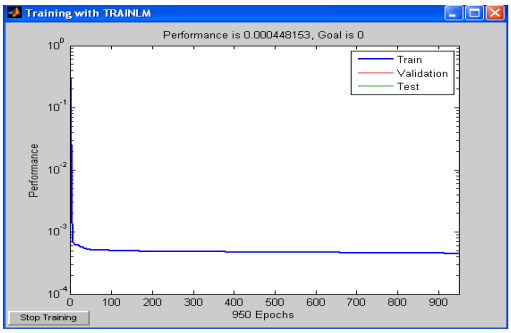

Figure 11: ANN Training process (Learning Performance Vs Epoch on extracted Minutiae points)

Figure 12 and 14 shows the data that are not match with the template data while figure 13, 15 shows data that are closely matched with the template**.** Figure 16 shows Biometric key generated from template while figure 17 shows session key and figure 18 shows combine key generation process.

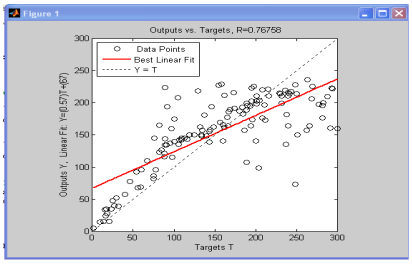

Figure 12: Showing result that is not matched with template (Target output vs. Computed output on Test data)

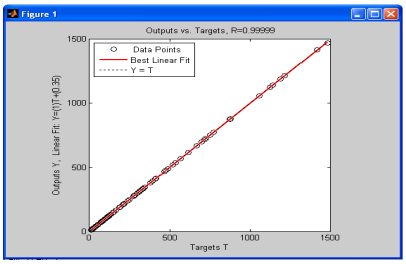

Figure 13: Showing result that is closely matched with template (Target output vs. Computed output on Test data)

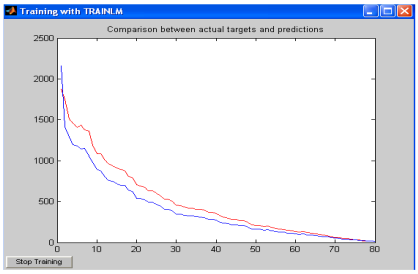

Figure 14: Showing result that is not matched with template (Compersion between Actual data and Predicted data)

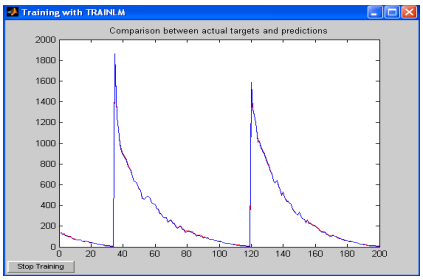

Figure 15: Showing result that is closely matched with template (Compersion between Actual data and Ppredicted data)

```
07E547D9-586F6A73- F73FBAC0-435ED769-51218FB7- D0C8D788-
A309D785-436BBB64-2E93A252- A954F239-12547D1E-8A3B5ED6-
E1BFD709-7821233F- A0538F3D- B854FEE6
```

Figure 16: Biometric key generated from template.

5B722B30-7FCE6C94-4905D132-691D5E4A-2214B7FE-92B73892-0EB3FCE3-A90420A1-9511C301-0A0E7712-B054DAEF-5B57BAD5-9ECBD93B-3280F210-578F547F-4AED4D25

Figure 17: Session Key after accepting password from the user.

Figure 18: (a) & (b) Combined Key generation by Crossing over of Biometric Key & Session key (c) Final Encryption key (1024 bit) generation by mixing keys (a) and (b)

5. CONCLUSIONS

The proposed approach minimizes the shortcomings of fingerprint based authentication technique by using ANN. Most of the applications use full fingerprint but in this approach a portion of the Fingerprint is good enough to generate the biometric key and hence minimizes False Rejection Ratio (FRR). In this approach traditional session based password technique is also applied to eliminate the limitation of static biometric key encryption. So using this approach sensitive data can be made more secure than any traditional technique. Experimental results are also satisfactory. This research has may be further extended using more reliable biometric features.

6. REFERENCES

[1] B.Jayaraman, C.Puttamadappa , E.Anbalagan ,E.Mohan and Srinivasarao Madane, Fingerprint Authentication using Back-propagation Algorithm of International Journal of Soft Computing 3(4) :282-287, 2008 ISSN:1816-9503.

[2] Junita Mohamad-Saleh and Brian S. Hoyle: Improved Neural Network Performance Using Principal Component Analysis on Matlab: International Journal of The Computer, the Internet and Management Vol.16. N.o.2 (May-August, 2008) pp 1-8.

[3] Younhee Gil, Dosung Ahn, Sungbum Pan, Yongwha Chung: Access Control System with High Level Security Using Fingerprints: Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03)0-7695-2029-4/03 $ 17.00 © 2003 IEEE .

[4] Zhang Tanghui, Tian Jie, He Yuliang, Yang Xin, "A Combined Fingerprint Matching Algorithm Based on Similarity Histogram",Chinese Journal of Computers, 2005, Vol.28(10), pp.1728-1733.

[5] Anil Jain, Arun Ross, "Fingerprint Matching Using Minutiae and Texture Features", ICIP, 2001, pp.282-285.

[6] Zsolt Miklos Kovocs-Vajna" A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping"IEEE Tran's on.PAMI, 2000, Vol.22 (11), pp.1266-1276.

[7] Anil K. Jain, Salil Prabhakar, Lin Hong, Sharath Pankanti, "Filterbankbased Fingerprint Matching", IEEE Tans on. Image Precessing, 2000, Vol.9 (5), pp.846-859.

[8] Anil K. Jain, Salil Prabhakar, Shaoyun Chen, "Combining Multiple Matchers for A High Security Fingerprint Verification System", Pattern Recognition Letters, 1999, Vol.20 (11-13), pp.1371-1379.

[9] A. K. Jain, L. Hong, S. Pantanki and R. Bolle, An Identity Authentication System Using Fingerprints, Proc of the IEEE, vol, 85, no.9,1365-1388, 1997.

[10] Hong, L., Y.Wan and A.K.Jain, 1998. Fingerprint Image Enhancement: Algorithm and performance Evaluation. IEEE. Trabs. PAMI, 20(8): 777-789.

[11] Jain, A., Hong, L., Bolle, R.: On-line Fingerprint Verification. IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.19, No.4 (1997) 302–313.

[12] Anil K. Jain, Salil Prabhakar, Lin Hong "A Multichannel Approach to Fingerprint Classification", IEEE Trans on. PAMI, 1999, Vol.21 (4), pp.348-359.

[13] Tanmay Bhattacharya, Sirshendu Hore , Ayan Mukherjee ,S. R. Bhadra Chaudhuri "A Novel Highly Secured Session Based Data Encryption Technique Using Robust Fingerprint Based Authentication" Advances in Networks & Communications, CCSIT Part 2 (2011) pp 422-431, Springer.