A Novel Data Encryption Technique by Genetic Crossover of Robust Finger Print Based Key and Handwritten Signature Key

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

[1] **Assistant Prof, Dept. of IT, JIS College Engineering, Kalyani, West Bengal, India.**

[2] **Assistant Prof, Dept. of CSE, Hooghly Engineering & Technology College, Pipulpati, Hooghly, West Bengal, India.**

[3] **Professor, Dept. E&TC, Bengal Engineering & Science University, Shibpur, Howrah, West Bengal, India.**

Abstract

Unimodal biometric systems have to contend with a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality; phishing attacks spoof attacks, and high false acceptance rates. In order for the biometrics to be ultra-secure and to provide more-than-average accuracy, more then one form of biometric identification is required. Hence some of these limitations can be addressed by a combination of different biometric recognition technologies that integrate the evidence presented by multiple sources of information. In the proposed work Fingerprint Key and Signature Keys are generated from the Fingerprint and Handwritten Signature of the legitimate user. The system is quite robust because it is trained by Artificial Neural Network and Machine Intelligence. Two Combined Keys are generated by Genetic crossover of those two keys. Finally by interleaving the combined keys Encryption Key is generated. In this approach there is a significant improvement over the traditional Unimodal biometric authentication techniques.

Keywords: *ANN; Minutiae; Center of Gravity;Aspect Ratio; Training; SHA-512, Crossover*

1. Introduction

Biometrics, described as the science of recognizing an individual based on her physiological or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual's identity. Different biometrics such as fingerprints, hand geometry, iris, retina, face, hand vein, facial thermogram,signature, voice, etc. to either validate or determine an identity [1].Most biometric systems deployed in real-world applications are unimodal, i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint *or* face). Some of the limitations imposed by Unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [2]. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [3]. Minutiae are local discontinuities in the fingerprint pattern. All popular AFIS are minutiae-based [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]. Signature is a socially accepted authentication method and is widely used as proof of identity in our daily life. Signature verification can be classified into two categories: signature verification [11, 12] and offline signature verification [13].All the Signature verification system of today are verification system and the features that are mostly used are Baseline Slant Angle, Aspect Ratio, Center of Gravity.Figure 1 illustrates the structure of Minutiae, center of gravity and Baseline slant angle of handwritten signature.

Figure 1: Minutiae (a) Ridge ending (b) Bifurcation Signature (c) Center of Gravity (d) Slant angel

Artificial Neural Network: Artificial 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 [14]. A Multi-Layer-Perceptron (MLP) is a kind of feed-forward ANN model consisting of three adjacent layers; the input, hidden and output layers. Each layer has several PEs. Figure 2 illustrates the structure of a MLP

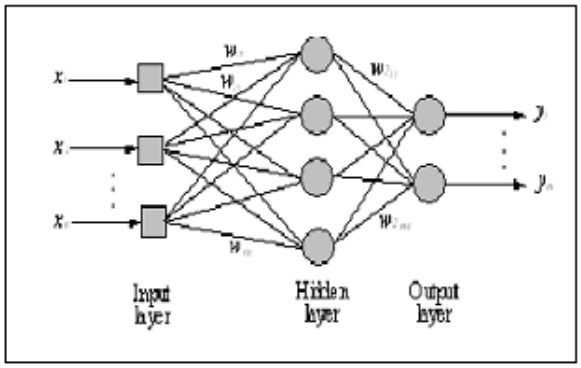

Figure 2: A schematic diagram of a MLP neural network

2. Proposed Algorithm

Following are the main steps of proposed algorithm.

a. Biometric Fingerprint 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. Handwritten Signature Key generation

c. Generation of two intermediate keys by genetic crossing over of Biometric key and Signature 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 Final 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.

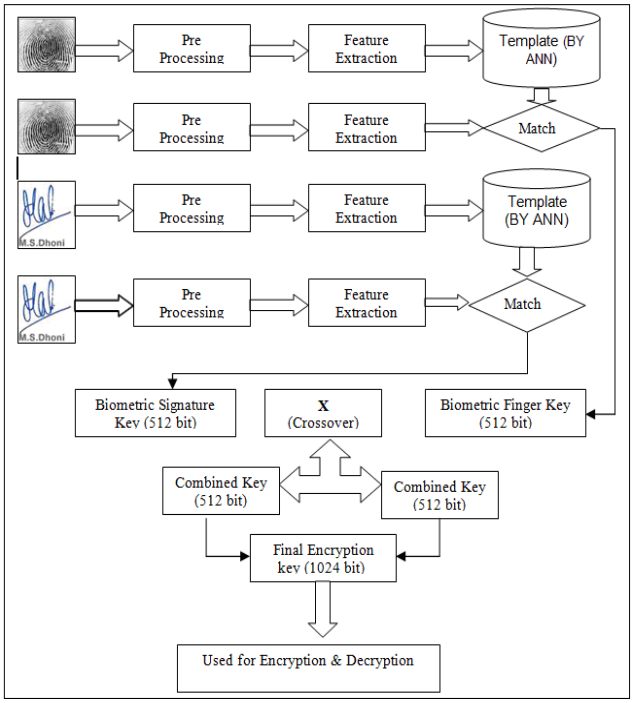

Figure 3: Schematic diagram: The sequence of multimodal authentication process.

3. Explanation of Algorithm

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

Step 2: Then the image (Fingerprint) 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.

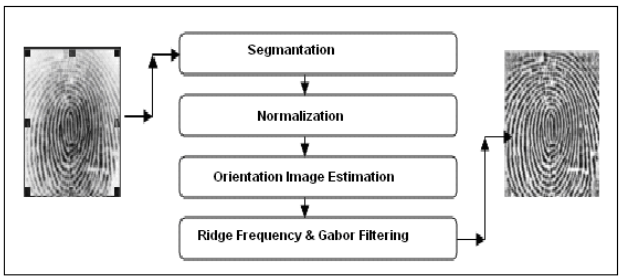

Figure 4: A schematic diagram of a fingerprint Enhancement

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.

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*

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

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

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

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

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

The new weights between output layer and hidden layer are updated

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

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

$$E(MSE) = \Sigma E(Im) \quad (e)$$

Step 5: A Finger 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 (7.5.0) and Java

Step 6: A finger 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 5 illustrates the Biometric key generation process. Figure 5 illustrates the Key Generation process with SHA512

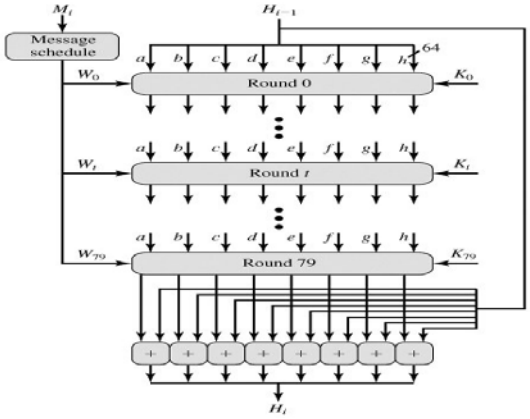

Figure 5: A schematic diagram of key Generation process with SHA512

Step 7: After obtaining the signature image various preprocessing operation are performed to remove the noise caused by the scanner. The image is then cropped, to the bounding rectangle of the signature. Finally transform the signature image from color to grayscale, and to black and white. Figure 6 illustrate the Image enhancement process.

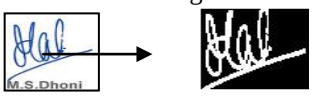

Figure 6: A schematic diagram of a Signature Enhancement

Step 8: From the enhanced signature image we calculate the center of gravity, slant angel also the aspect ratio of the image .stores those value. Training, signature template creation as well as generating the signature biometric key from the signature template is same as step 4, step 5 and step 6.

Step 9: Two Combined keys of 512 bit each are generated by Genetic Crossover of Finger Key and Signature Key. Figure 7 illustrates the Genetic finger biometric key and genetic signature key generation process

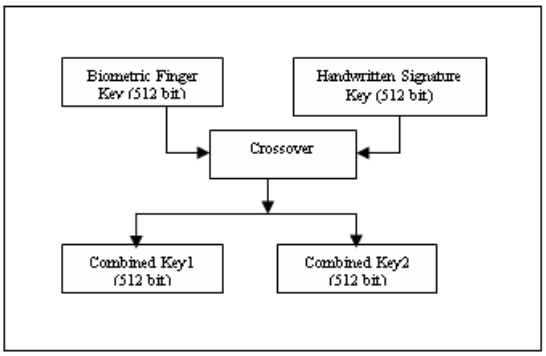

Figure 7: Two combine keys are generated by Crossover

Step 10: A Final key of length 1024 bit is generated by interleaving two Combined Keys obtained from the previous step. Figure 8 illustrates the Final Key generation process.

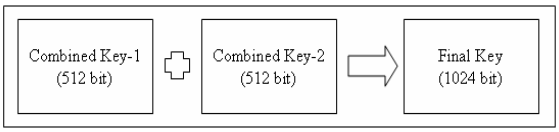

Figure 8: A Final key of length 1024 bit is generated

Step 11: Taking the File from the user encrypts the data using the Final 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 Final key .Given file is now encrypted.

Step 12: Taking the Sample fingerprint and Handwritten Signature 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 Fingerprint Biometric key (512 bit) and Signature Biometric key from the template. The Final key (1024) is generated using the finger biometric key and signature biometric key. Decrypt the encrypted file using the Final Key.

4. Results & Discussions

In this section, we have presented the experimental results of the proposed approach, which is implemented in MATLAB (7.5) and Java (JDK1.6). We have tested the proposed approach with different sets of input images. Initially Fingerprints and Handwritten Signature are scanned using standard Bio-sensor scanner with required resolution. As there can be some imperfection in the capture of images, enhancement has been done followed by extraction of feature (Minutiae points for fingerprint and slant angle, aspect ratio and center of gravity for handwritten signature). Figure 9 illustrate the different stage of the fingerprint image, Handwritten Signature image.

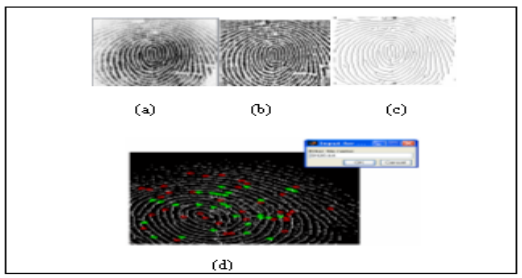

Figure 9: (a) Raw Image, (b) Enhanced Image, (c) Thinned Image and (d) Image with Minutiae points.

Figure 9: (e) Raw Image (f) Enhanced, Cropped Image (g) Image with Center of gravity (h) Image with Slant Angle

Figure 10 and 12 shows the data that are not match with the template data while figure 11, 13 shows data that are closely matched with the template. Figure 14 shows finger Biometric key generated from template while figure 15 shows Signature Biometric key generated from template and figure 16 shows combine key generation process.

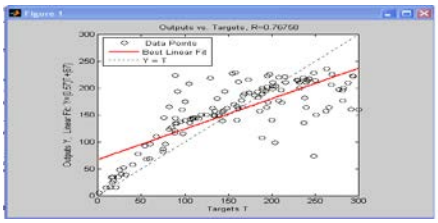

Figure 10: Showing result that is not matched with template (Target output vs. Computed output on Test data)

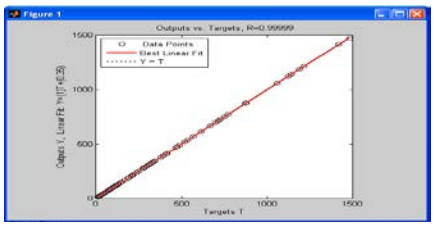

Figure 11: Showing result that is closely matched with template (Target output vs. Computed output on Test data)

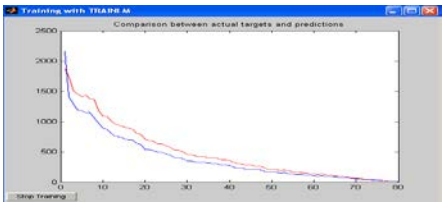

Figure 12: Showing result that is not matched with template (Compersion between Actual data and Predicted data)

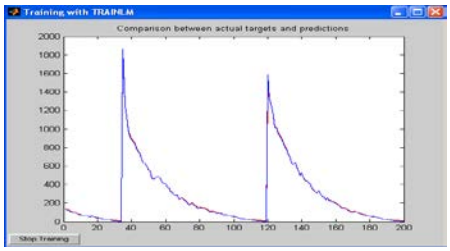

Figure 13: Showing result that is closely matched with template (Compersion between Actual data and Ppredicted data)

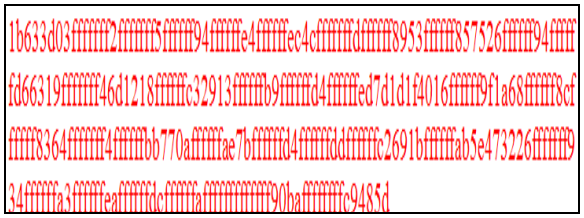

Figure 14: Finger Biometric key generated from template.

Figure 15: Signature key generated from template.

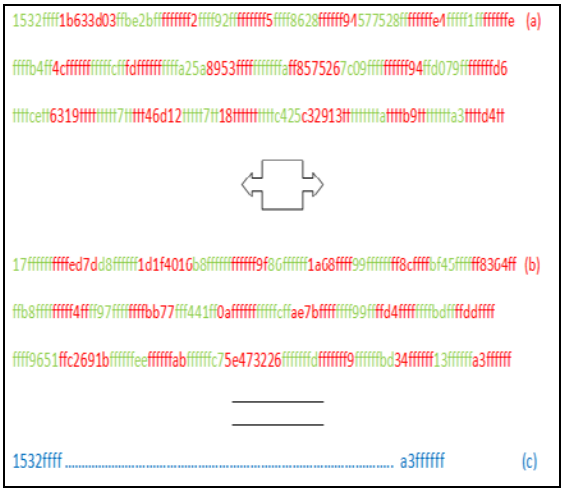

Figure 16: (a) & (b) Combine Key (512 bit) Generations by Crossing over of Signature Key & Finger Print Key (c) Final key (1024 bit)

5. Conclusions

The proposed approach minimizes the shortcomings of Unimodal authentication technique by using ANN. Most of the available 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).Also in this approach combined the use of handwritten signature technique and fingerprint system is to eliminate the limitation of Unimodal system. 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.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.

[2] A. Ross and A. K. Jain, “Information fusion in biometrics,” Pattern Recognition Letters, vol. 24, pp. 2115– 2125, Sep 2003.

[3] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, “Is independence good for combining classifiers?,” in Proc. of Int’l Conf. on Pattern Recognition (ICPR), vol. 2, (Barcelona, Spain), pp. 168–171

[4] Zhang Tanghui, Tian Jie, He Yuliang, Yang Xin, "A Combined Fingerprint Matching AlgorithmBased 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] 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.

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

[8]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.

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

[10]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

[11] A. Jain, F. Griess, and S. Connell. On-line signature verification. Pattern recognition, 35(12):2963 2972, 2002

[12] V. Nalwa. Automatic on-line signature verification. Proceedings of the IEEE, 85(2):215– 239, 1997

[13] M. Kalera, S. Srihari, and A. Xu. Offline signature verification and identification using distance Statistics, 2004.

[14]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