ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

# Biometric Authentication using Steganography via Chaotic Encryption and Data Hiding.

**MK Bharathi*, and E Nagarajan*.**

Department of Computer Science, Sathyabama University, Chennai-600119, Tamil Nadu, India.

**ABSTRACT**

Wireless network becomes more popular in transferring sensitive information since it provides many security features such as Wi-Fi Protected Access and Wired Equivalent Privacy protocols. Though, it is critical due to many threats such as MAC spoofing, man-in-the-middle attacks, Denial of service, Network injection, Caffe Latte attack, etc. In order to safeguard the information transferred via wireless network, we proposed a method of steganography using chaotic encryption and Qualified Significant wavelet tree (QSWT) concepts. In our proposed system, user gives their face and biometrics (i.e. fingerprint) for authentication. The biometric signal is encrypted and then it is hided into the human face using QSWT technique to produce the stegno-object. It is then compressed and sent to the server. It aims to improve a) robustness against noise and compression, b) good encryption scheme and c) easy implementation.

**Keywords:**Steganography, Chaotic encryption, QSWT, Biometrics

***Corresponding author***

ISSN: 0975-8585

## INTRODUCTION

Wireless network becomes top rated now a days in all concern. Security in such wireless network is very essential due to the following reasons: Theft of sensitive information, private connection abuse, DOS attacks, stealing band width etc. In order to protect the data completely over the wireless network we need to undergo encryption, authentication & steganography mechanisms.

### Encryption

The encryption is used to secure data during transmission via network that is through internet, e-commerce, mobile telephones, Bluetooth device, wireless intercom system, bank automatic teller machine & wireless microphones [2]. There are three basic types of encryption algorithm as hashing, symmetric or private key cryptography and asymmetric or public key cryptography. Symmetric cryptography includes AES (Advanced Encryption Standard) Blowfish, Camellia, DES (Data Encryption Standard), Mars, etc. whereas asymmetric includes RSA (Rivest-Shamir-Adleman), SSH (Secure Shell), DH (Diffie-Hellman) and SSL (Secure Socket Layer Certificate) [1].

### Authentication

Authentication is an essential element for atypical security procedure. It defines a process of proving the users identity who is trying to access resources or logon. There are several authentication mechanism, but all support the above same purpose and some of them are password authentication, smart card authentication, Biometric authentication.

### Steganography

Steganography [3] is a mechanism for hiding sensitive data in innocuous data such as MP3 music file, picture, etc. Several steganography techniques such as LSB (Least Significant Bit) encoding, Low frequency encoding, mid frequency encoding, etc. are in use and it can be difficult to detect when it is properly implemented.

Apart from general discussions on the above three schemes, let us include the related works on biometric authentication according to the reference [4]. Lamport [5], in 1981, proposed the concept of authentication via insecure channel and this leads to failure because of various attacks. Many researches undergoes different schemes to improve security. Li at al [6], in 2001, used neutral network for remote authentication. In their scheme, they need large memory for storing public parameters which results in higher computational costs. In 2002, Lee at al [7] proposed fingerprint based remote authentication. In their approach, a user inserts their smart card for login purpose, enters their identity and password, and imprints their finger print through finger print input device. Later, in 2004, Lin and Lai [8] and Chang and Lin [9] point out that the above scheme could not tackle the masquerade attacks. Li and Hwang [10], in 2010 proposed a scheme on bio-metricsbased authentication, smart card, nonce and one way hash function. The use of random nonce and one way hash function is more efficient,but it does not have proper authentication and cannot tackle man-in-the-middle attack. This was found by Li et al [11], in 2011. Chang and Chen [12], in 2014 proposed a multi-server authentication scheme. Mishra et al [13], found that the above proposal scheme does not tackle stolen smart card attack and impersonation attacks. In the schemes mentioned in this section, uses bio-metrics, simply an authentication tool in smart card technology. After analysis of their complete potentiality, biometric signals can be implemented in crypto-steganography hybrid schemes [14].

## PROPOSED METHOD

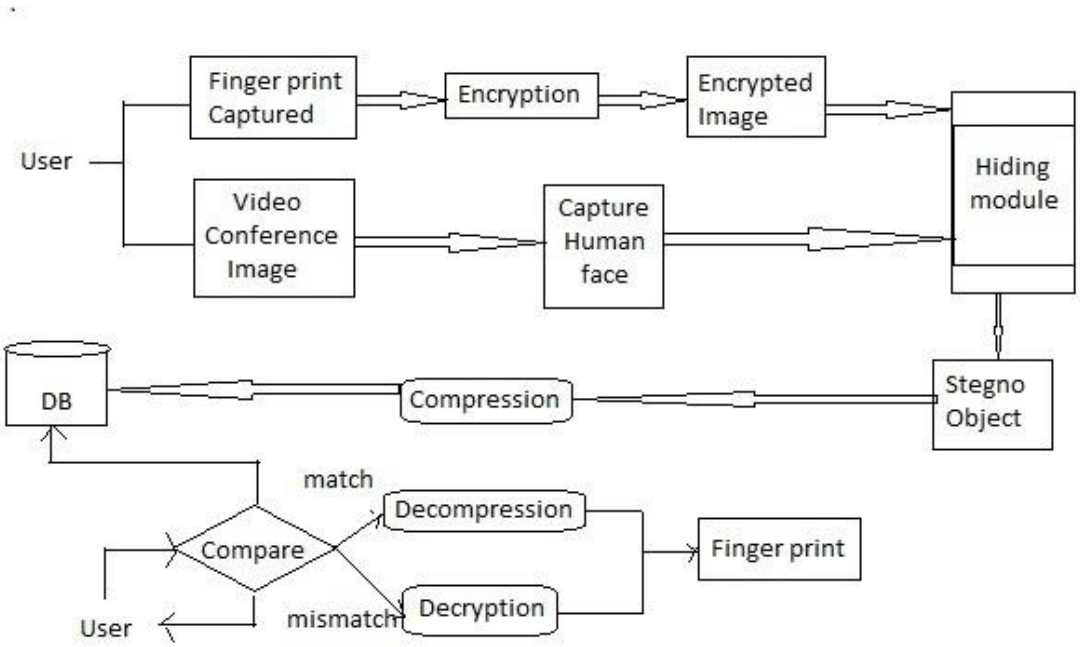
The proposed bio-metric authentication mechanism through wireless network is aim to work well under the compression and lossy transmission. It ensures,

a) Good encryption scheme,
b) Robustness against noise & compression and
c) Easy implementation.

ISSN: 0975-8585

Overall architecture of the proposed method is referred in Figure 1. User who need to access the application need to do authentication. Thesystemrecognize the user's video conference image and from that human face is captured. Then, eliminate the background blocks and stored as the host image. Once the user inputs his face, he have to imprints their fingerprint using the fingerprint input device. The fingerprint is encrypted before undergoing steganography mechanism using algorithm 1.

**Figure 1: Architecture of the proposed system**



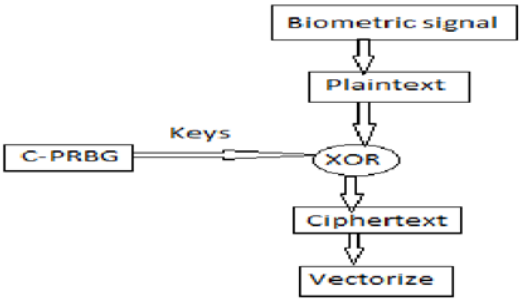

**Algorithm 1** Chaotic Encryption

```
1:  procedure encryption (fingerprint)
2:      Plaintext[i] ← fingerprint
3:      Key[i] ← C-PRBG
4:      Cipher[i] ← plaintext[i] ^ key[i]
5:      while (Cipher)
6:          fori = 1 to n do
7:              Vectorize
8:          end for
9:      end while
10: return
```

Figure 2 provides the block diagram of the encryption procedure. In that, fingerprint of the user which is captured using the fingerprint input device is converted into the plain text with 0's and 1's byte values. C-PRBG (Chaotic-Pseudo Random Bit Generation) generates the key equal to the size of the plaintext and that executes chaotic mechanism, i.e. XOR operation to convert it into the cipher text. The produced cipher text is the encrypted file for the users' fingerprint and it is vectorized.

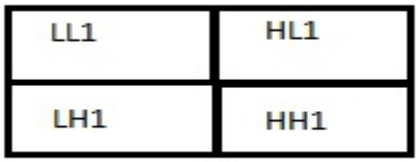
ISSN: 0975-8585

**Figure 2: Block diagram for encryption procedure**




Once we obtain the vectorized encrypted biometric signal, QSWT is performed for hiding the vectorized encrypted biometric signal into the host image. The procedure for QSWT is explained in Algorithm 2. In that, host image is decomposed into four sub bands of lower resolution image (LL), horizontal detail component (HL), vertical detail component (LH) and diagonal (HH) detail component as mentioned in Figure 3. Out of the four sub bands the lower resolution detail component is neglected and three high resolution detail components that is sub bands {HL, LH, HH} are selected. Each bit from the vectorized encrypted biometric signal is embedded into the selected sub band of higher frequency. This process is repeated, until each and every bit of the fingerprint gets hided into the human face.

**Figure 3: Sub band blocks of QSWT**




**Algorithm 2** QSWT Detection

1: **procedure** QSWT (host_image)
2: Decompose host_image→ {LL, HL, LH, HH}
3: Select {HL, LH, HH}
4: **for**i = 1 to n
5: Embed Vectorized Cipher[i] → {HL, LH, HH}
6: **end for**
7: **return**

After embedding, stegno-object is obtained. It has to compress, to store in the server. Again, when the user wants to access the system where he did authentication and creates their own account, the following steps are happened with the system. First, the system asks for the user's face. The server matches this input face with already registered face that is stored in the database. If it matches, then it asks for the fingerprint to imprint. The server extracts the hided fingerprint from the stegno-object, decrypted and it matches with the currently entered biometric signal. If it matches, the system allow to access the application, else denied.

ISSN: 0975-8585

## IMPLEMENTATION AND RESULTS

The implementation of the proposed biometric based steganography mechanism is examined under various factors like effectiveness, security, efficiency and robustness. Figure.4and Figure. 5illustrates the indicative results of the proposed system for the input A and input B. The samples from the POLY-BIO [15] project, a biometric database is taken for examination contains about 1,500 biometric signals, out of them 300 are fingerprints. The general flow of the proposed system includes: a) Capturing human face from video conferencing frame, b) Imprint the user's fingerprint, c) Segmentation of the captured human face into the host image, d) Encryption of the biometric signal, e) Hiding the encrypted biometric signal into the host image using QSWT, f) Compression of the stegno-object and stored in the server, g) Decompression of the stegno object for authentication during accessing application and h) Decryption of the biometric signal.

**Figure 4: Indicative results: (a) Capturing human face from video conferencing frame, (b) Imprint the fingerprint, (c) Segmentation of host image, (d) Encrypted fingerprint, (e) Stegno-object, (f) Compressed stegno-object, (g) Decompressed stegno-object and (h) Decrypted fingerprint**

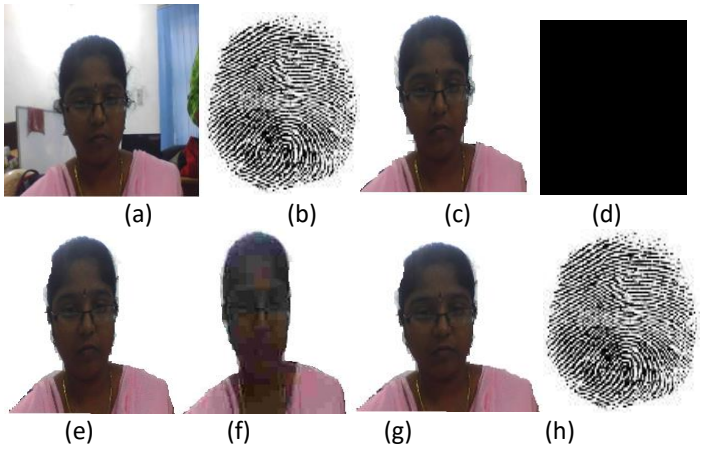
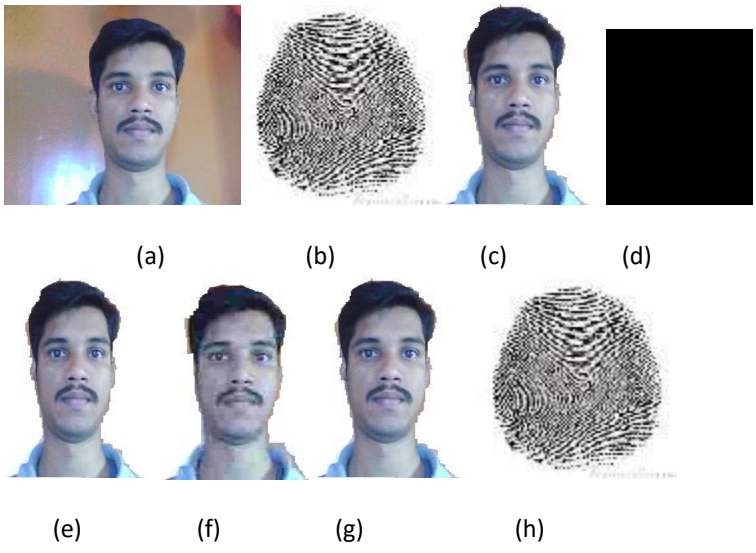



**Figure 5: Indicative results: (a) Capturing human face from video conferencing frame, (b) Imprint the fingerprint, (c) Segmentation of host image, (d) Encrypted fingerprint, (e) Stegno-object, (f) Compressed stegno-object, (g) Decompressed stegno-object and (h) Decrypted fingerprint**



Once the user's face and fingerprint is captured, algorithm 1 and algorithm 2 are executed for fingerprint encryption and embedding of encrypted fingerprint into the host-image for producing the Stego-object respectively. The results of the mean energy squared values which is recorded with the smallest scale filter at each orientation are represented in Table 1. After these values are obtained, the RGB values of the fingerprints (assumed) for the input A and input B are found and embedded with each orientation as in Table 2. This produces the stego-object and it is stored in the server as in Fig. 4f and 5f.

| Input A | Input B |
|---|---|
| 3.5941 | 7.1218 |
| 2.4361 | 4.0816 |
| 2.7265 | 3.2648 |
| 3.8820 | 4.0028 |
| 3.0025 | 3.5647 |
| 2.7878 | 4.1429 |

**Table 1:Mean energy squared values**

| | | | | | |
|---|---|---|---|---|---|
| Input A | X00 | 242 | 241 | 241 | 241 |
| | X02 | 241 | 240 | 241 | 241 |
| | X00 | 240 | 239 | 241 | 242 |
| | X22 | 240 | 238 | 241 | 242 |
| | XX01 | 242 | 241 | 241 | 241 |
| | YY01 | 242 | 242 | 241 | 241 |
| Input B | X00 | 255 | 255 | 255 | 249 |
| | X02 | 255 | 239 | 255 | 242 |
| | X00 | 254 | 239 | 255 | 255 |
| | X22 | 255 | 255 | 253 | 254 |
| | XX01 | 255 | 255 | 254 | 255 |
| | YY01 | 254 | 255 | 255 | 254 |

**Table 2:RGB values embed with each orientation**

## CONCLUSION

Biometric signal plays a key role in day-to-day lives, since from government sector to private sector,use this for authentication purpose in all crucial procedures. The current implementation cannot estimate a quality of service and since chaotic encryption is a new field of research, it takes some time to mature in security analysis. Taking the above into consideration, the further development integrates the biometric authentication techniques into the real time applications.

## REFERENCES

[1] Rajan Mishra, Shashi Mehrotra Seth. Comparative Analysis on Different parameters of Encryption Algorithms for Information Security. International Journal of Computer Sciences and Engineering, 2014; 2(4): 76-82.

[2] Kumar N, Gupta P, Sahu M, Rizvi, MA. Boolean Algebra based effective and efficient asymmetric key cryptography algorithm: BAC algorithm. Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), International Multi-Conference, 2013; 22-23: 250 – 254.

[3] HojjatAdeli, Tai-hoon Kim, Carlos Ramos, Byeong-Ho Kang. Signal Processing, Image Processing and Pattern Recognition. International Conferences, Held as Part of the Future Generation Information Technology Conference, December 8-10, 2011.

[4] Nagarajan E, SatyaSravani V. Knowledge abstraction from MIMIC II using apriori algorithm for clinical decision support system. Indian Journal of Science and Technology , 2015; 8(8): 728-730.

[5] Lamport L. Password authentication with insecure communication. Communications of the ACM, 1981; 24(11): 770–772.

[6] Lin IC, Li LH and Hwang MS. A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Networks, 2001; 12(6): 1498–1504.
[7] Ryu SR, Lee JK and Yoo KY. Fingerprint-based remote user authentication scheme using smart cards. Electronics Letters, 2002; 38(12): 554–555.
[8] Lai YY and Lin CH. A flexible biometrics remote user authentication scheme. Computer Standards & Interfaces, 2004; 27(1): 19–23.
[9] Lin IC and Chang CC. Remarks on fingerprint-based remote user authentication scheme using smart cards. ACM SIGOPS Operating Systems Review, 2004; 38(4): 91–96.
[10] Hwang MS and Li CT. An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications, 2010; 33(1): 1–5.
[11] Niu JW, Li X, Ma J, Wang WD and Liu CL. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications, 2011; 34(1): 73-79.
[12] Chen MC and Chuang MC. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Experts Systems with Applications, 2014; 41(4): 1411-1418.
[13] Das AK, Mishra D and Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications, 2014; 41(18): 8129-8143.
[14] Nicolas Tsapatsoulis and KlimisNtalianis. Remote Authentication via Biometrics: A RobustVideo-Object Steganographic Mechanism OverWireless Networks. IEEE Transactions on Emerging Topics in Computing, 2015.
[15] Tsapatsoulis N, Kounoudes A, Theodosiou Z, and Milis A. Polybio:Multimodal biometric data acquisition platform and security system. Biometrics and Identity Management, 2009; 216–227.