ISSN 2277 – 5528
Impact Factor- 4.015

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

BIOMETRIC STEGANOGRAPHY USING VISUAL OBJECT FOR REMOTE AUTHENTICATION

Veda D*1, Bhargavi V2, Harshitha S3 & Navyashree S4
*1Asst Prof, Department of ISE, RajaRajeswari College of Engineering , Bangalore
2,3&4UG Students, ISE, RajaRajeswari College of Engineering, Bangalore

ABSTRACT

Sensitive information is frequently exchanged via wireless network, which requires remote authentication for accessing the information. Remote authentication might be in the form of encrypted information. Intruder attacks such as Trojan Horse may cause serious issues especially in the case of remote operations. Here a robust authentication technique is proposed, which is based on Chaotic encryption and data hiding. If a user wants to be remotely authenticated, initially user has to select a video. Next, user's biometric signal is encrypted using a chaotic encryption method. Then the encrypted image is vectorized and the data hiding process is carried out using Qualified Significant Wavelet Trees (QSWTs). QSWT is used to achieve the invisibility, resistance to attacks and robustness in data hiding. Subsequently, the Inverse Discrete Wavelet Transform (IDWT) is applied to retrieve the hidden information from the stego-object followed by an appropriate decryption process to get back the biometric image. Experimental results prove that the proposed technique would yield security merits and robustness to steganalytic attacks.

Keywords: *Remote authentication, QSWT, Stego-object, Biometrics*

I. INTRODUCTION

Tirupur is one of the largest foreign exchange earning towns in India. There are some 7,000 garment units in the Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person. The two main directions in the authentication field are positive and negative authentication. Positive authentication is well-established and it is applied by the majority of existing authentication systems. Negative authentication has been invented to reduce cyber-attacks. The difference between the two is explained by the following example: Password-based authentication. In positive authentication, the passwords of all users that are authorized to access a system are stored, usually in a file. Thus the passwords space includes only users passwords and it is usually limited (according to the number of users).If hackers receive the passwords file, then their work is to recover the plaintext of a very limited number of passwords. On the contrary, in negative authentication the anti-password space is created, (theoretically) containing all strings that are not in the passwords file. If hackers receive the very large anti-password file, their work will be much harder. This way, negative authentication can be introduced as a new layer of protection to enhance existing security measures within the networks.

The proposed scheme is a positive authentication system and for security reasons elements from at least two and preferably all three, of the following factors should be verified:

- the ownership factor: Something the user has
  (e.g. ID card, security token, cell phone etc.)
- the knowledge factor: Something the user knows
  (e.g., a password, a PIN, a pattern etc.)
- the inherence factor: Something the user is or does
  (e.g., fingerprint, retinal pattern, DNA sequence, face, other biometric identifier etc.)

According to the case study mentioned in [4], the first two factors can easily be hacked by the intruders. So, the human authentication following the inherence factor would tend to give more security than the other factors, because the user inputs their own biometric image and it would make the attackers less to interpret or crack the authentication mechanism. Biometrics have already been incorporated in the remote authentication scheme [1, 2, 3], but only as password substitution in smart cards. Most of the password based authentication schemes are simple and the passwords can easily be guessed or broken [5], [6]. Moreover, it is most of the people's mentality to use the same password across different applications. Thus, if a malicious user determines a single password, it can be used to make attacks across multiple applications. Combination of encryption and steganography can achieve the biometric technique successfully. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood. To confront the problem of user authentication, proposed an efficient wavelet-based steganographic method for biometric signals hiding in video objects, which focuses on optimizing the authentication rate of hidden biometric data over error prone transmissions. Interesting techniques for object-oriented data hiding have been presented for example, however, most of them do not particularly consider the case of biometric data. Thus the main contributions and novelties of the proposed system are as follows. (a) It is one of the first to use video objects to hide their respective biometrics[7]. By this way "dual" authentication is accomplished, the first by visual perception of the figured person, and the second by extraction and matching of the hidden pattern. (b) Biometric signals are encrypted before hiding. The statistical properties of this novel combination are analyzed and presented. (c) A DWT based algorithm is adapted for biometrics hiding. In contrast to most steganographic algorithms that are capacity efficient, the proposed algorithm is very robust to several types of signal distortions. By this way, the proposed scheme contributes to illustrate the perspective of encrypted biometrics authentication systems over error prone networks.

II. RELATED WORKS

Lamport [8] has proposed a method on remote password authentication. In order to stop the intruders from hacking the system a method called one way hash function was implemented. But the disadvantage of this scheme was that a verification table should be maintained on the remote server side. In case if any intruders will hack the table they can easily modify the table.

Liao et al [9] has proposed a method which uses Diffie-Hellman key agreement protocol over insecure networks. It is a method for two computers which is used to generate a shared private key with which they can exchange information across an insecure channel. This shared private key is used to encrypt or decrypt the information. But the disadvantage is it is very difficult to remember the cryptographic keys as they are randomly generated.
Apart from the above mentioned methods comparatively an effective technique was introduced using smart cards **[10][11][12]**. It was efficient in authentication mechanism. But the disadvantage was that the identity of the users was static in every transaction sections. This caused the leakage of information related to user and in turn resulted in ID theft while transmitting messages over insecure channels.

The disadvantages mentioned in the above papers can be solved using Biometrics. It is the most reliable and efficient technique **[9][12][13]**. Biometric traits will be unique in each and every individual. So it would be very difficult to forge, copy or share the traits. One more convenient feature is the need not to be present compulsorily in the time of authentication. But in the earlier schemes it is only used as password authentication in smart card technologies.

Anjali and Kulkarni [18] proposed a method based on transform based data-hiding approach in steganography. This paper uses biometric feature i.e. skin tone to implement steganography. The secret data is hidden inside the skin region of image as an efficient mode security will be obtained.

Dajun He et al[19] has proposed a new way in authentication system called as an object based video authentication system. This system is a combination of watermarking and digital signature techniques for the protection of authenticity between video objects and their associated backgrounds.

K. Zebbiche and F. Khelifi[20]has proposed a method on region based watermarking of biometric images. It embeds the watermark into only the region of interest. It preserves the hidden data from the process of segmentation which would remove the background that is useless by keeping the region of interest unaltered. The disadvantage was that this method promoted negative image of the user, reduces social sharing.

Kamaldeep Joshi and RajkumarYadavproposed a new approach towards hiding the data for image steganography using XOR operation. This method is analyzed on the bases of PSNR, MER, L2RAT and MAXERR. It removes the limitations of LSB method.

DeepaKundur, Yang Zhao and PatrizioCampisi [21] proposed an approach for combined image authentication and compression of color images by making use of a digital watermarking and data hiding framework.

III. PROPOSED SCHEME

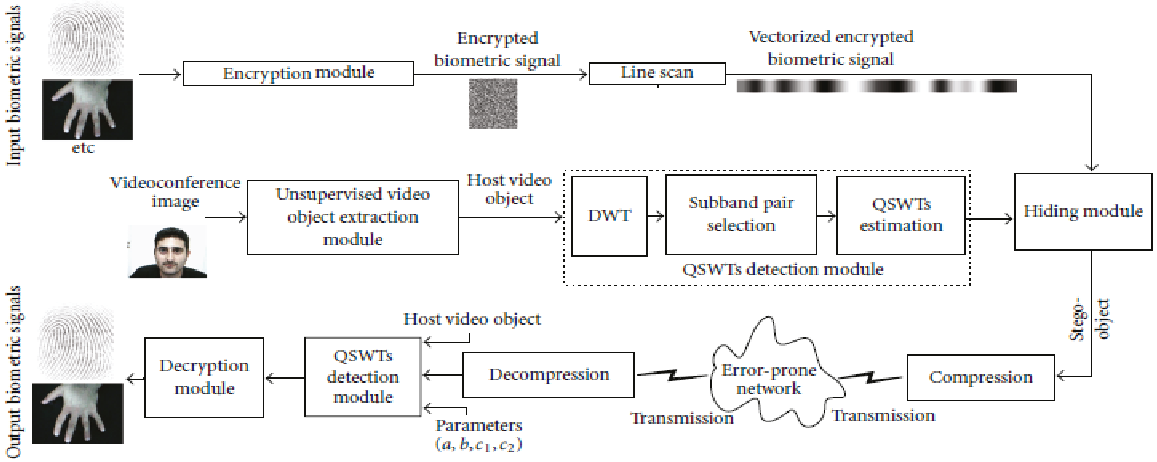


FIGURE 1: An overview of the proposed system.

Fig1 shows the working flow of proposed system and is explained as below.

Proposed system includes the following stages:

a. Video object extraction
b. Input biometric signals and encryption
c. Chaotic encryption based on Lorenz method
d. QSWT
e. HAAR-DWT
f. Formation of stego-object
g. Extraction of image

a. Video object extraction

The video is taken as input from user's webcam and the video consists of multiple frames. One frame is chosen from it. Semantically meaningful objects should be segmented, leaving the background of the frame. Segmentation algorithm should be efficient and achieve faster.

b. Input biometric signals and encryption

Password codes to Identify individual users are replaced with biometric traits like fingerprints, palm, DNA strands and retinal scans. When these images are sent over network duplication should not occur and a high degree of security can be achieved. Biometric image is taken as an input. With the help of C-PRBG(Chaotic Pseudo Random Bit Generator) key will get generated as shown in Fig2. Then read the volume of image as matrix. For example if biometric image is embedded in 128 by128-bit image. 128 by128 matrix of random bits collected would be for key. When applying XOR bit-by-bit to the two matrices, 128 by 128 matrix of encrypted bits are obtained. To decrypt the image, take the encrypted image and compute XOR with the encryption key, bit-by-bit. With this key chaotic encryption is performed. In this encryption method initial condition and control parameters will get initialized. Results of encryption and key are hidden in the frame. Output image of first round is taken as input to second round.

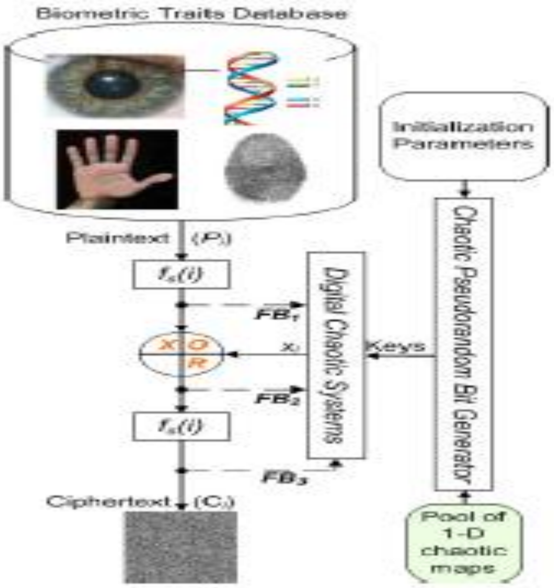


Fig 2: Overview of the encryption module

c. Chaotic encryption based on lorenz system

Compared with low dimension chaotic system, high dimension chaotic encryption which is present in Lorenz system can resist local linear attack, phase space reconstruct attack, entrophy attack etc.

d. QSWT

Watermarking is a technique for labeling digital pictures by hiding secret information in the images. A digital watermark is a kind of marker covertly embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. An original image is decomposed into wavelet coefficients. Then, multi-energy watermarking scheme based on the qualified significant wavelet tree (QSWT) is used to achieve the robustness of the watermarking. Unlike other watermarking techniques that use a single casting energy, QSWT adopts adaptive casting energy in different resolutions.

Algorithm of QSWT:

```
procedure $QSWT_{EST}(I, S, L)$
/* $I$=input frame */
/* $S$=sub band selection (e.g. $LH$) */
/* $L$=sub band level (e.g.3) */
/* Thresholds T1 and T2 are globally defined */
$[LL, LH, HL, HH] \leftarrow DWT(S, L\text{-}1)$
$S_{L-1} \leftarrow LH$
$[LL1, LH1, HL1, HH1] \leftarrow DWT\ (LL, 1)$
$S_L \leftarrow$LH1
$t \leftarrow 0$
$QSWT[t] \leftarrow ø$
$N \leftarrow$ rows $(S_L)$
$M \leftarrow$ columns $(S_L)$
fori = 1 to Ndo
    forj = 1 to Mdo
        if $S_L(i, j)$ is In Node AND $|S_L(i, j)| > T_1$ then
            $C_1 \leftarrow S_{L-1}(2i-1, 2j-1)$ is In_Node AND$|S_{L-1}(2i-1, 2j-1)| > T_2$
            $C_2 \leftarrow S_{L-1}(2i-1, 2j)$ is In_Node AND $|S_{L-1}(2i-1, 2j)| > T_2$
```

```
$C_3 \leftarrow S_{L-1}(2i, 2j-1)$ is In_Node AND $|S_{L-1}(2j, 2j-1)| > T_2$
$C_4 \leftarrow S_{L-1}(2i, 2j)$ is In_Node AND $|S_{L-1}(2i, 2j)| > T_2$
if ($C_1$ AND $C_2$ AND $C_3$ AND $C_4$) then
$QSWT[t] \leftarrow S_L(i, j) + S_{L-1}(2i-1, 2j-1) + S_{L-1}(2i-1, 2j) + S_{L-1}(2i, 2j-1) + S_{L-1}(2i, 2j)$
$t \leftarrow t + 1$
return QSWT
```

e. HAAR-DWT:

Simplest DWT of two dimension consists of two operations-Horizontal and vertical operations.

Step 1: Scan the pixels from left to right horizontally. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as shown in Fig 3. Repeat until all the rows are completed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image(denoted as symbol H).

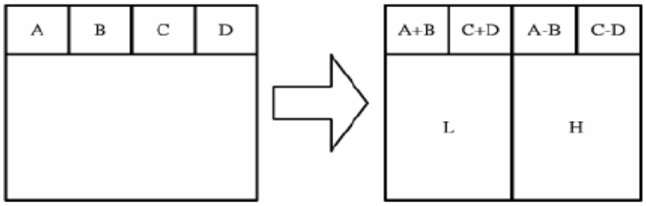


Fig 3: Addition and Subtraction of pixels horizontally.

Step 2: Scan the pixels from top to bottom vertically. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as shown in Fig 4. Repeat until all the columns are completed. Finally obtaining 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

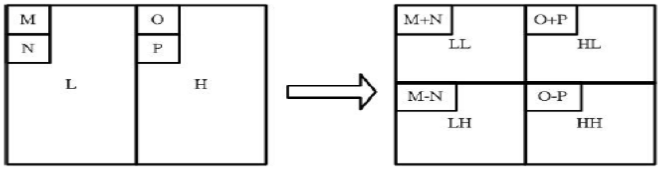


Fig 4: Addition and Subtraction of pixels vertically.

f. Formation of stego-object:

The Fingerprint image of 128×128 size is embedded into LL, and this obtained image is called stego Image.
Extraction of stego image:

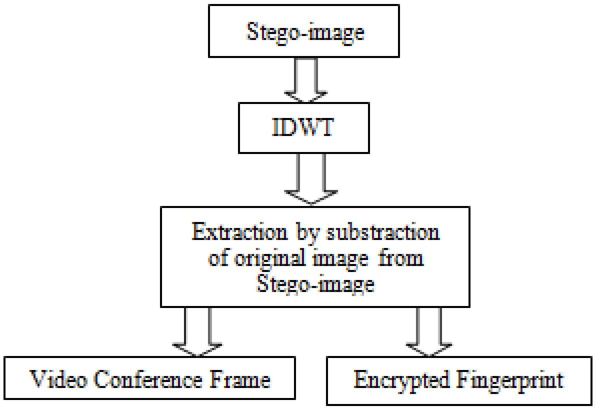

Stego-image
IDWT
Extraction by substraction of original image from Stego-image
Video Conference Frame
Encrypted Fingerprint

Fig 5: Extraction of Stego-image.

Stego-image is decompressed to original image by Inverse Discrete Wavelet Transform (IDWT) and the fingerprint is extracted from it. Again it has become two separate images of the same original data given.

IV. EXPERIMENTAL RESULTS

The image of the user will be captured with the help of an image acquisition device (Fig. 1) i.e. webcam. The user has to select a biometric image and give as an input.The biometric image will be encrypted and further vectorized.The vectorized object is hidden inside the host object and hence stego-object is obtained (Fig. 2). The histogram image and correlation images of the original biometric image and encrypted image is obtained (Fig. 3).The stego object is further transferred to other system through wireless network and the received stego-object is decrypted and separated from cover image (Fig. 4).The decrypted image is compared with the original image.

Following shows the different stages of biometric steganography using video object.

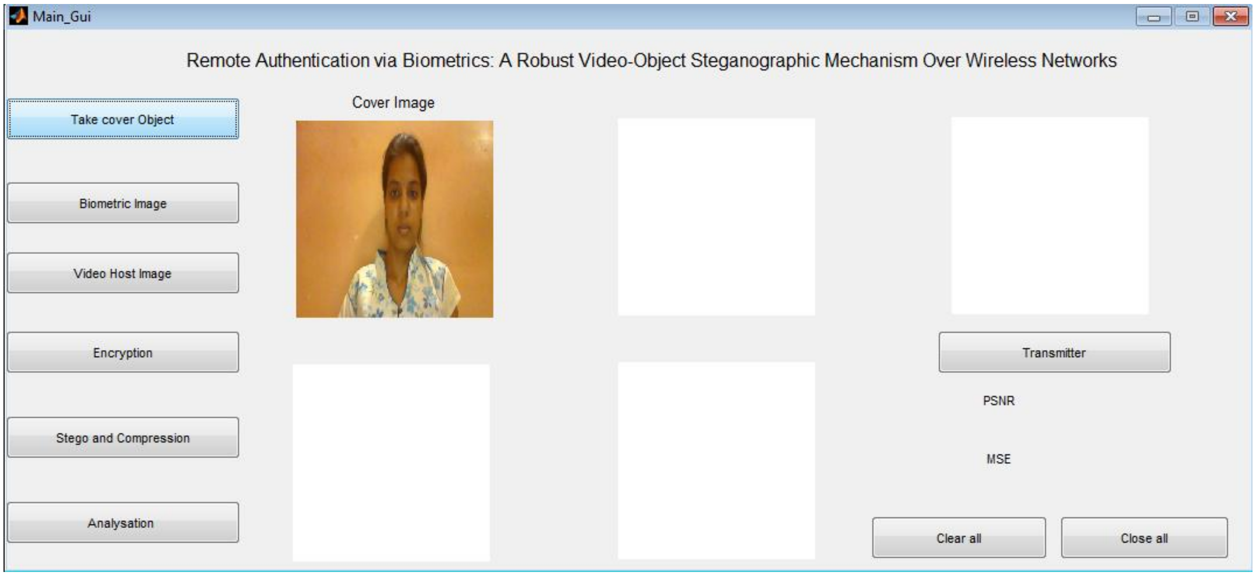
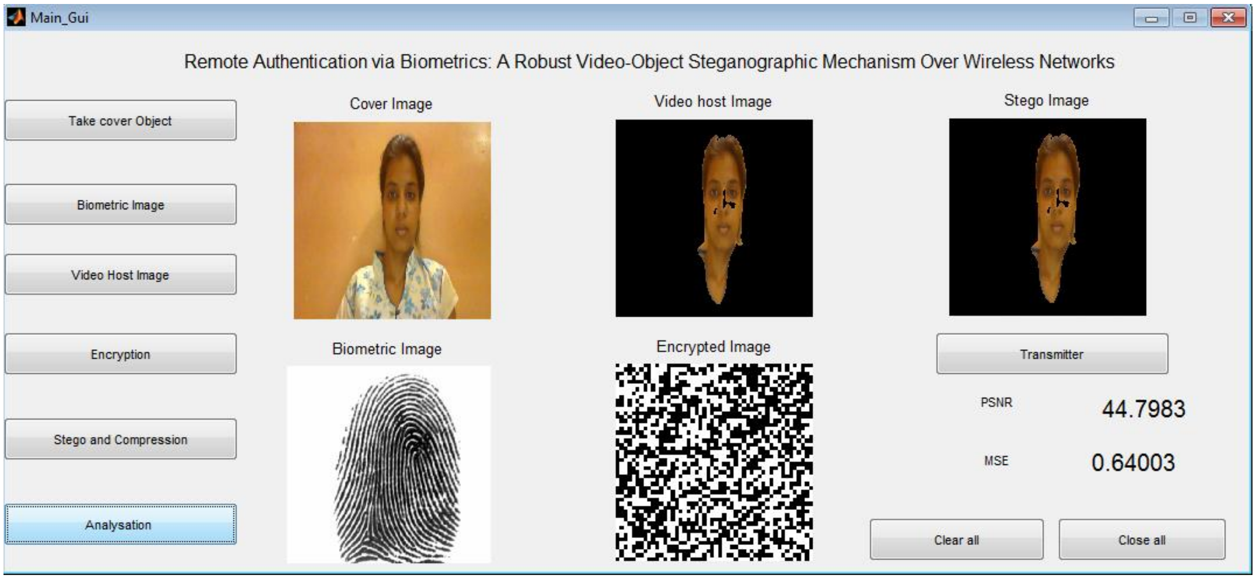


Fig. 1: Capturing of host image from webcam.



PSNR 44.7983

MSE 0.64003

Fig. 2: Obtainment of stego-image.

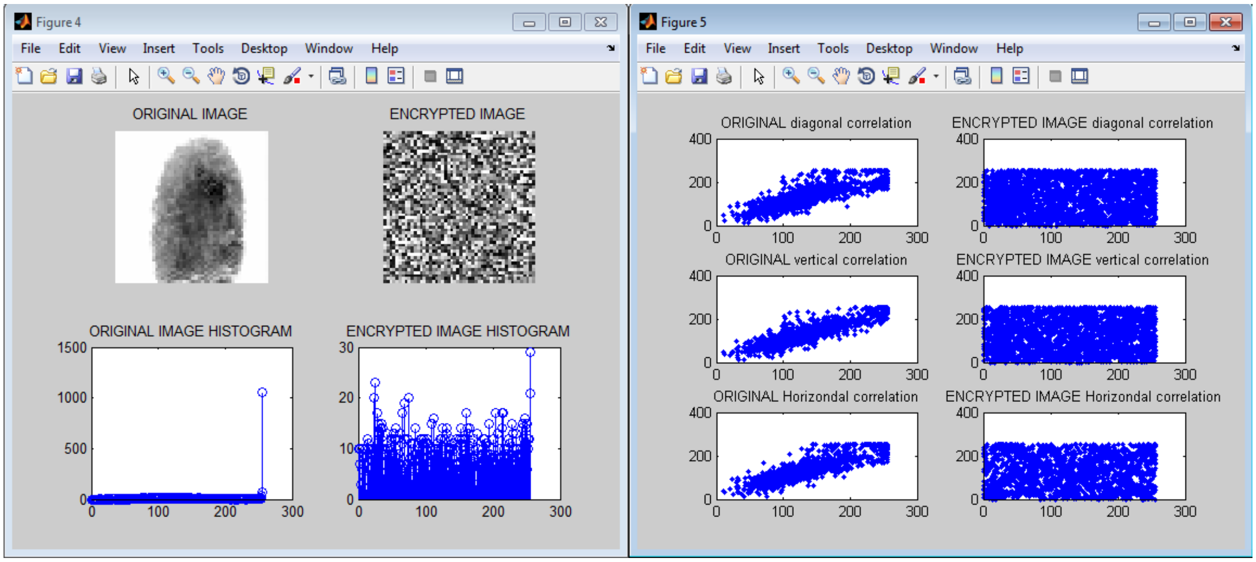
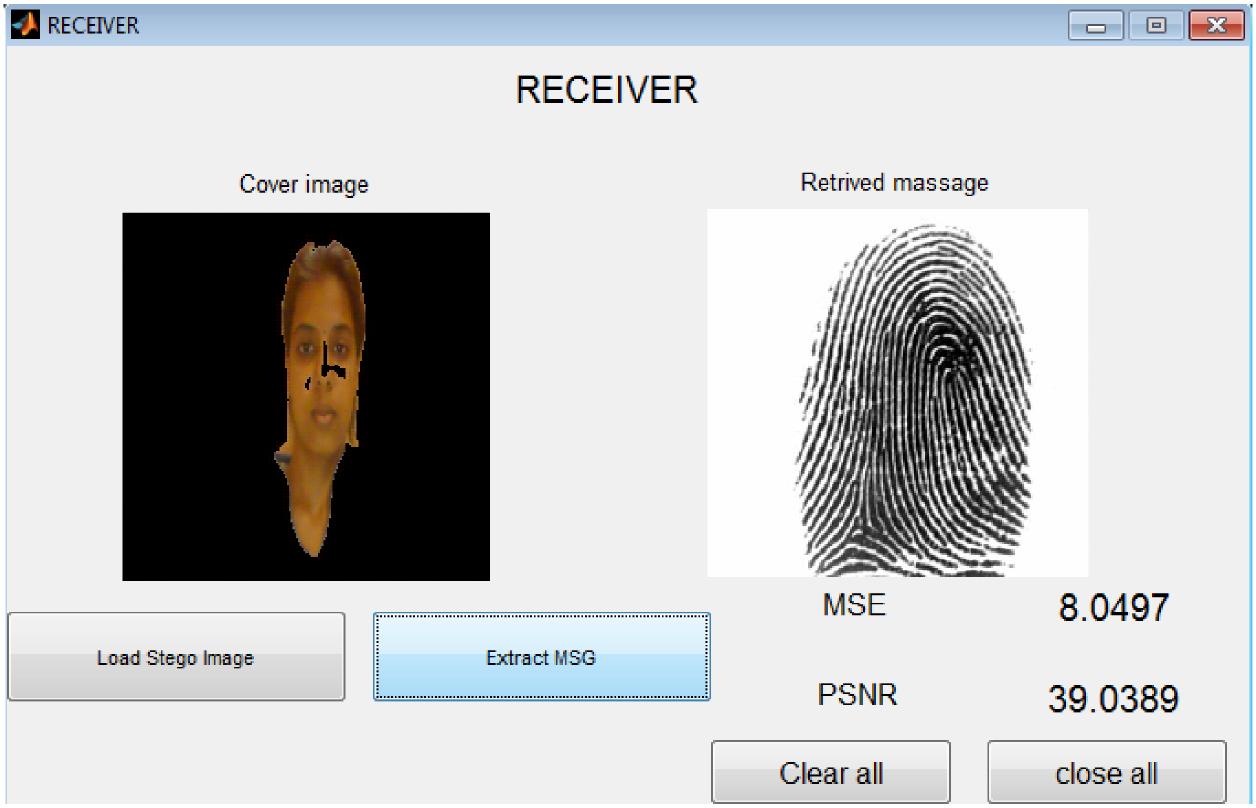


Fig. 3: Histogram and Correlation graphs



MSE 8.0497

PSNR 39.0389

Fig. 4: Retrieval of cover and biometric image at the receiver side.

V. CONCLUSION

The proposed technique yields best security in the authentication process. When an intruder tries to attack, he/she has to know if steganography is used in the authentication process. Even if the intruder knows the existence of steganography and tries to steal the stego image, he/she will end up with vectorised numbers. This would create confusion to the cracker to decide what these numbers are.

Steganography by itself does not ensure secrecy, it is combined with a chaotic encryption system. Proposed procedure, outputs a stego-object that can resist different signal distortions, and steganalytic attacks. Results indicate that the use of QSWTs provides high levels of robustness, keeping at the same time the ease of implementation and the compatibility to well-known and widely used image and video. Lastly the system is able to recover the hidden encrypted biometric signal under different losses.

The application of the proposed system could be a smart interview system wherein a candidate can give an interview from a remote location using his face image and finger biometric.

VI. ACKNOWLEDGEMENT

The authors would like to express sincere thanks for encouragement and constant support provided by the Management RRGI, and Principal RajaRajeswari College ofEngineering, Bangalore-74, India during this research work.

REFERENCES

[1] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem", The Journal of Supercomputing, vol. 63, no. 1. 2013

[2] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics", Expert Systems with Applications, vol. 41, no. 4, pp. 1411–1418, 2014.

[3] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multiserver authentication with key agreement scheme", in Computational Science and Its Applications, ser. Lecture Notes in Computer Science, vol. 7335. Spinger-Verlag, 2012.

[4] "Identity fraud report: Data breaches becoming a treasure trove for fraudsters", Javelin Strategy and Research, Tech. Rep.

[5] M. Jakobsson and M. Dhiman, "The benefits of understanding passwords", in Mobile Authentication, ser. Springer Briefs in Computer Science. Springer New York, 2013, pp. 5–24.

[6] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords", in Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010, pp. 162–175.

[7] S. Li and W. Li, "Shape-adaptive discrete wavelet transforms for arbitrarily shaped visual object coding", IEEE Transactions on Circuits and Systems for Video Technology, vol. 10(5), Aug. 2000, pp. 725–743.

[8] L. Lamport, "Password authentication with insecure communication,"Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[9] W. Stallings, "Cryptography and Network Security: Principles and Practices". Prentice Hall, 5th edition, Upper Saddle River, NJ, USA, 2010.

[10] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," Journal of Computer and System Sciences, vol. 72, pp. 727–740, 2006.

[11] Y.-y. Wang, J.-y. Liu, F.-x. Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," Computer Communications, vol. 32, no. 4, pp. 583–585, Mar. 2009.

[12] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme'," Computer Communications, vol. 34, no. 3, pp. 305–309, Mar. 2011.

[13] E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme'," International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(B), pp. 3661–3675, May 2012.

[14] K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometricrecognition," IEEE Transactions on Circuits Systems for Video Technology,vol. 14(1), pp. 4–20, 2004.

[15] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1–5, Jan. 2010.

[16] Anjali A Shejul, U L Kulkarni "A dwt based approach for image steganography,"International Conference on Data Storage and Data Engineering, 2010.

[17] D. He, Q. Sun, and Q. Tian, "A secure and robust object-based video authentication system," EURASIP Journal of Applied Signal Processing, vol. 2004, pp. 2185–2200, 2004.

[18] *K. Zebbiche and F. Kheli_, ``Region-based watermarking of biometric images: Case study in fingerprint images,'' Int. J. Cryptography Inf. Secur., vol. 2008, Jun. 2008, Art. ID 492942.*

[19] *D. Kundur, Y. Zhao, and P. Campisi, ``A stenographic framework for dualauthentication and compression of high resolution imagery,'' in Proc. IEEE Int. Symp. Circuits Syst., vol. 2. May 2004, pp. 1-4*