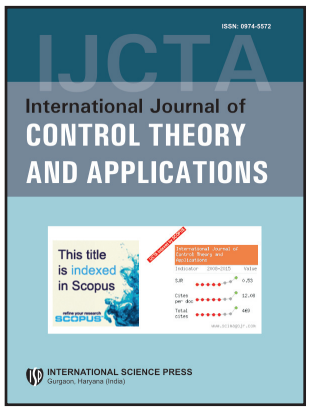

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 25 • 2017

Investigation on Remote Verification Scheme Applying Biometrics in Wireless Networks using Steganographic Method

Bestley Joe S[a] and Mathan N[b]

[a-b]Assistant Professor, Dept. of. EIE., Assistant Professor, Dept. of. ECE., Sathyabama University, Sathyabama University, Chennai-600 119. Chennai-600 119. Email: [a]bestleyjoe@gmail.com; [b]mathanmaestro@hotmail.com

Abstract: Steganography is an art of hiding any data may be a file, image, video or message. In advanced steganography, electronic communications may incorporate steganography coding within a transport layer, for example, an archive, record, picture, document or codes. Media files are perfect for steganographic transmission due to their huge size. In remote networks delicate data is regularly exchanged, requiring remote validation. Remote validation includes the submission of encoded data, alongside visual and sound effects. Nevertheless, in these remote data transfer also we have trojan horse and other attacks making the data transfer insecure. This paper is based on a research outcome that proposes a strong validation system based on semantic division, secure force encryption and information hiding. Execution is done using MATLAB with sample images for proving the proposed model's qualification.

Keywords: Image processing, biometrics, steganographic method, remote verification, wireless networks.

1. INTRODUCTION

A. Literature Survey

Users in remote location can authenticate using password-based verification procedures and are broadly investigated, with present-day research increasingly joining a users biometrics with a password to design a remote user validation scheme that improves the level of the safety from hacking [1]. As, these verification methods are intended for a unique server environment and results in clients expecting to enroll generally when they have to get to different application servers. To take care of this issue, the authors have proposed an unknown multi-server validating key agreement system in view of trust figuring using smart cards, passwords, and biometrics. This system underpins multi-server situations as well as accomplishes numerous security prerequisites. Moreover, this system is a lightweight validation method which just uses the nonce and a hash work. From the consequent examination done by the authors, the proposed a method that can oppose a few sorts of security attacks, and to have more security components than other equivalent schemes.

A wide variety of frameworks require dependable individual acknowledgment methods to either confirm or decide the uniqueness of an individual asking for their services. The reason for such methods is to guarantee that the rendered services are obtained to a genuine user, and not any other individual[2]. Samples of such applications assimilate secure approach to structures, monitoring stations, portable PCs, PDAs and ATMs. Without individual acknowledgment schemes, these frameworks are powerless against the clutches of an intruder. In this research work, the authors have also given a brief overview of the field of biometrics and summarized some of its advantages, disadvantages, strengths, limitations, and other related privacy concerns.

An information theoretic way to deal with get an assessment of the quantity of bits that can be covered up in still pictures, or the limit of the information concealing channel is also worked out[3]. The target of this work is to justify how the expansion of the message signal or signature in an appropriate transform domain instead of the spatial domain can altogether enhance the channel limit. A large portion of the cutting edge schemes grew up to this point for information covering up have installed bits in some transform domain, as it has dependably been certainly comprehended that disintegration would offer assistance. Though most schemes stated in the writings use DCT or wavelet decomposition for data embedding, the choice of the transform is not clear. The authors have compared the achievable information concealing capacities with regards to different deteriorations like DCT, DFT, Hadamard, and sub band transforms and demonstrated that the DFT decay performs best among the ones analysed.

A general feature among many techniques involves user identity (ID) in all transaction periods[4], which may leak somehow to create risk during transmission of information. A dynamic ID based remote validation method was done through six different ways. All the six except one were vulnerable to attack.

A chaotic approach was found which was later broken into four cryptanalytic methods and found some drawbacks [5]. Initial trials showed vulnerable to attacks but the improved encryption scheme got higher security. The authors stated that the problem can be solved by modifying chaotic cryptosystem from the original one.

A security analysis was evaluated and proposed the secure force algorithm [6]. Also a comparison of secure force 64, 128 and 192 bit architecture based on avalanche effect, entropy change analysis, image histogram and computational time was also performed. The research work also emphasized the possible solutions for the weakness of the SF algorithm.

B. Existing System and its Drawbacks

Password based remote user validation strategies are broadly analyzed, with present-day research increasingly consolidating an individual's biometrics with a password to develop a remote user authentication procedure that enhances the level of the security. But, these verification procedures are intended for a single server conditions and results in users expecting to register normally when they need to open different application servers.

Also the encoding methods used in these validation schemes are obsolete, long and unsafe. MIM (man in middle) attackers are easily able to hack into these verification schemes thereby getting access or sometimes even stealing the susceptible and secret information.

Drawbacks:

1. **Traceable problem:** The confidentiality of users in cryptography incorporates secrecy and untraceability, where secrecy here implies that an attacker can't get the users genuine character, and untraceability means that an attacker can't obtain the users activities.
2. **The distribution of PSK:** The scattering of the PSK is a trade off issue. If the PSK is simply kept in the RC, the servers trade off issue won't occur. Yet, most of the users can't be checked adequately if

the RC crashes (i.e., a unique point failure issue). But, the verification delay and the correspondence between the RC and the servers will increase liberally in light of the fact that the server needs to get the PSK from the RC to play out the confirmation framework inevitably. On the other hand, the servers give a defect tolerant limit (i.e., when the RC crashes, the validation technique can regardless be executed in light of the fact that the servers can show this strategy) if they keep the PSK.

3. **The two factor authentication scheme:** The two-factor validation method (i.e., using smart card and password) is starting now the most generally perceived validation mode. Tragically, many two-factor methods just guarantee the structures security when either the password or his smart card is stolen, however not both. Besides, the secret key does not have the attribute of uniqueness biometric and can't be put away in an outside devices.

C. Proposed System and its Merits

This project proposes a new validation scheme based on semantic segmentation, secure force encryption and data hiding. Assuming that a client X wants to be verified remotely for data access, at first X's video object (VO) is consequently portioned, utilizing a head and-body identifier. After that, one of X's biometric signals is encoded by a secure force algorithm. In this way the encoded signal is embedded to the most valuable wavelet coefficients of the Video Object, manifesting its Qualified Significant Wavelet Trees (QSWTs). QSWTs offer both intangibility and noteworthy resistance inspite of lossy transmission and compression, circumstances that are usually happening in wireless communications. Finally the Inverse Discrete Wavelet Transform (IDWT) is applied to exhibit the stego-object (SO). The framework has the following advantages:

(a) This technique approaches both spatial and transient domains, which prompts to distinguishing different malicious changes in spatial and time spaces.

(b) It is quicker and has reduced intricacy contrasted with existing algorithms, making it useful and reasonable for real-time applications. The existing algorithms take hours to complete the process whereas the SF algorithm takes less than 10-15 minutes.

(c) Hiding capacity of the secret data bits is high. The SF algorithm currents works on a 64-bit, 128-bit and 192-bit capacity which makes this accessible to a large number of bits storage scheme.

(d) Hiding capacity is depended on the pixel number relating to the two highest peaks of the image histogram. Here the hiding module is based on DWT and QSWT domains thus making the encryption very safe from attacks.

2. THEORY OF OPERATION

A. Block Diagram of the System

Experimental outcomes are with respect to: (a) security advantages of the proposed encryption technique, (b) quality to steganalytic strikes to various transmission errors and JPEG compression proportions and (c) bandwidth expanding measures, demonstrate the promising execution of the proposed biometrics-based verification system. The block diagram has the following operations:

Videos to frames: The sorting out of useful important information from the video is done in order to process the video data efficiently and decrease the transfer of collision in the network, so huge attention is given to video processing technology and its corresponding data segmentation as it is one of the widely used technique along

with its key frame extraction. The recent research works are concentrated on the background information and histogram as a key parameter for the frame conversion.

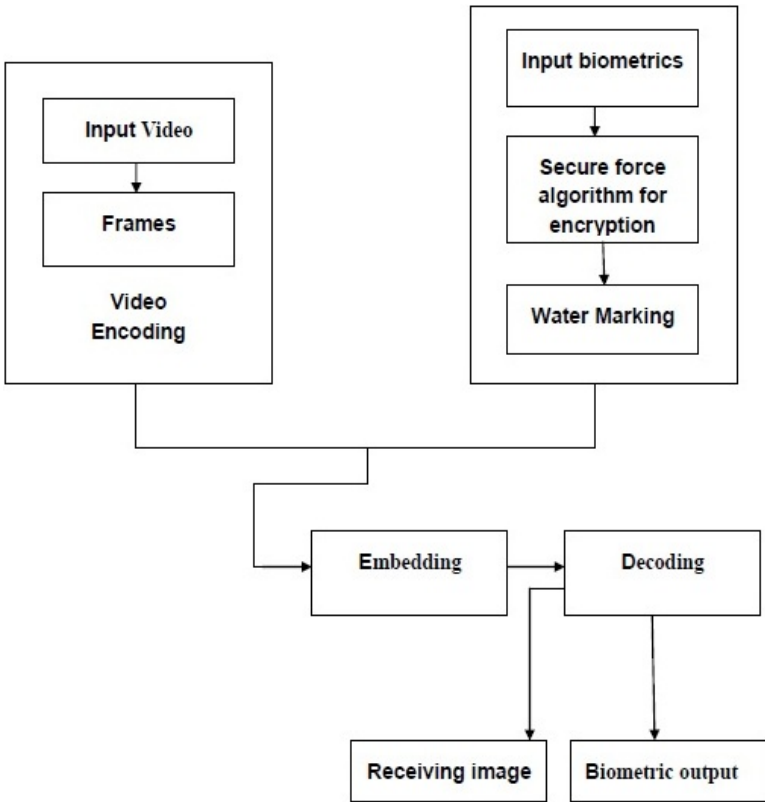

Figure 1: Block diagram of the system

Figure 2: Video to frames

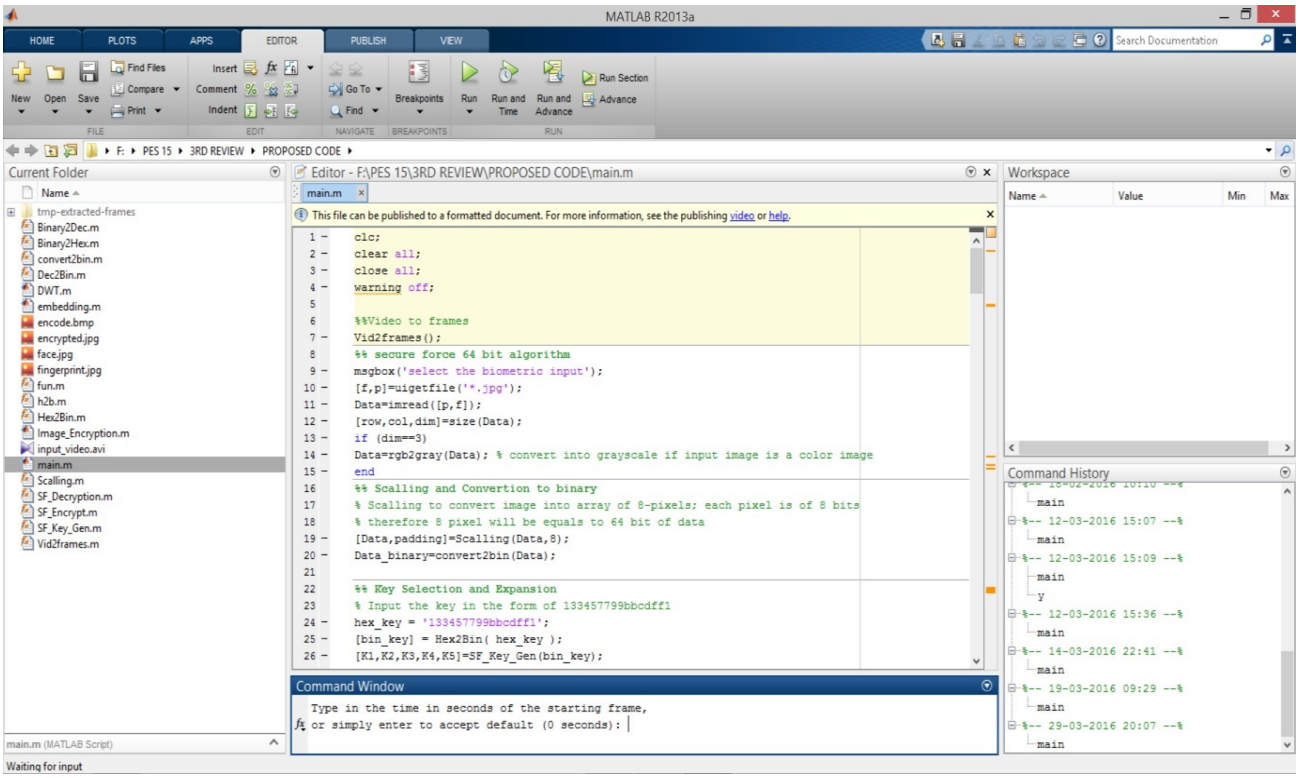

Figure 3: Steps of program before video to frame conversion

Gray scale input: In image computing, the gray scale is the value of each pixel in a single sample that carries only the intensity information. The weakest intensity has blacks stronger intensities have whiter spaces in the picture. The gray scale images gave shades of gray in between and they indicated the intensity in electromagnetic spectrum.

Figure 4: Gray Scale input

Encryption process: The encryption process done here is based on secure force (SF) algorithm that reduced the code size to a great extent. This enhanced the possibility of low-complexity architecture to wireless sensor networks and also has less power utilization. To implement the security operation every encryption round had six numerical operations over a 4-bit information. This procedure is done to create sufficient amount of diffusion and confusion in the data to encounter to counterattack any type of attacks.

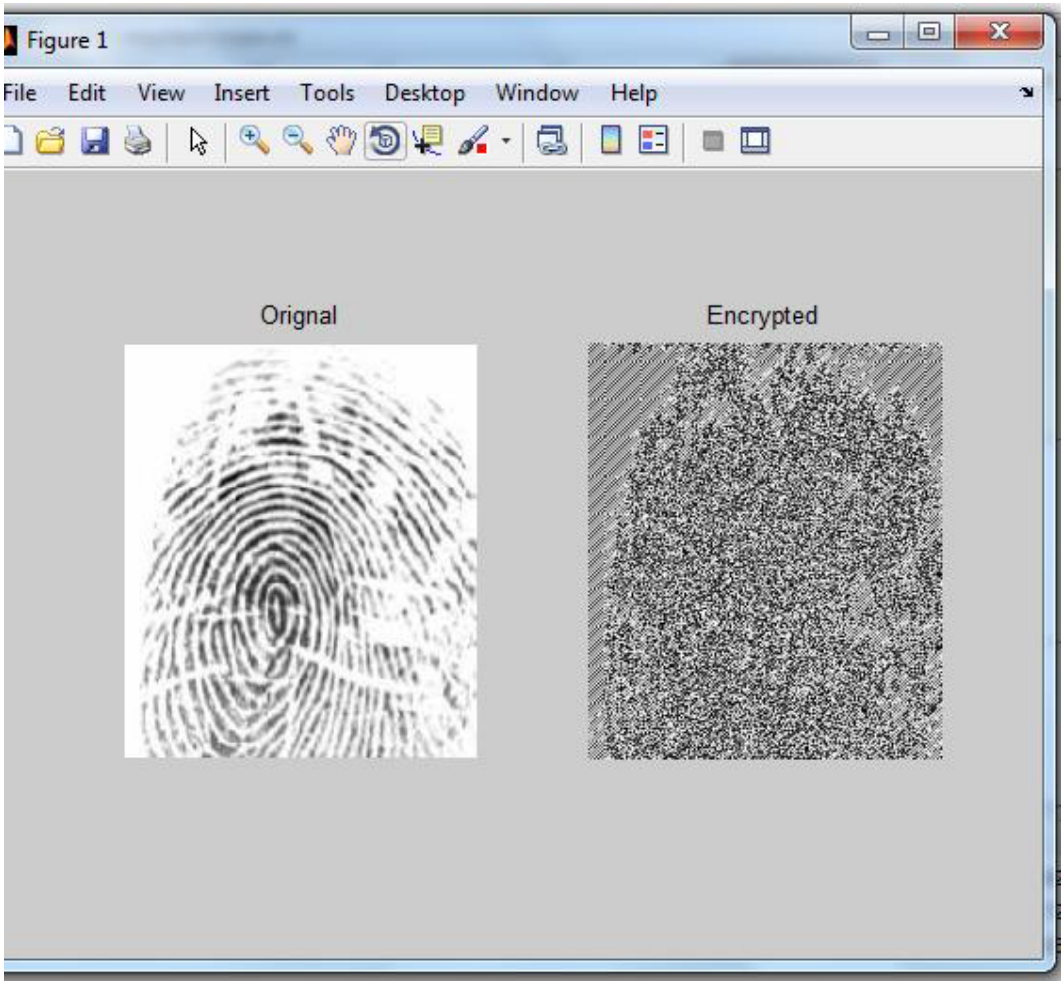

Figure 5: The encrypted image

Vectorization: Matlab's matrix algebra syntax or array operators are used to implement vectorization and to perform calculation without the explicit use of loops.

Vectorization is advantageous because of the following points:

1: Vectorization enables writing of code that is compact and idiomatic.

2: Compact, idiomatic code is easier to read and debug.

3: Vectored code is faster, even though the same computations are performed.

DWT and QSWT operations: The encrypted biometric signal is hidden in the host video object. This makes a stego-video object that would ensure its shrouded message regardless of the possibility that there are instances of compression or lossy transmission. The QSWT (Qualified Significant Wavelet Tree) plays such a role to data recovery even if a several signal manipulations takes place. By using SA-DWTs once to a range of subjective shape, 4 sections of low, middle and high frequencies ie., LL1, HL1, LH1, HH1 are produced. LH1 includes low & high frequency parts both in horizontal and vertical directions. Sub-band LL1 can be further subdivided into four different subbands. ie., LL2, HL2, LH2 & HH2. The highest coefficient is called parent and others are called children. In this work, video object steganography scheme coefficients with local information are selected as target coefficients for casting the encrypted biometric signal.

DWT Compression: The DWT compression is done to lower redundancy of the image data so as to store/ transmit that data in efficient form.

Decryption: This module gets at its info, a vector of encoded samples, the underlying control parameters and starting conditions for secure force algorithm which produces a similar one time pad used during encryption. However, now it is utilized for decoding process. This procedure is ended after the last sample is decrypted and all the decoded samples are re-ordered to provide the underlying biometrics signal .

Implementation of algorithm used: Steganography is the process of hiding one image into another. Here the entire matlab coding required in this project can be divided into four categories:

Firstly we can take a frame from a host video at any point of time as matlab also acts as a video to frame converter.

Secondly we have taken a biometric image (fingerprint) and encrypted it using a 64-bit secure force algorithm. The reason for utilization of the secure force encryption over other encryption techniques is its high security and the similar mechanism of its encryption and decryption procedures.

Next we hide the biometric input into the original image using DWT domain. After the hiding module the original image is selected for QSWT domain thus creating a embedded stego image.

Finally the biometric image can easily be restored back from the original image when required. As the encryption and decryption mechanism of the secure force algorithm is almost the same, so it becomes easy for us to decrypt the required biometric image.

3. RESULTS AND DISCUSSSION

A. Result

In this project we have used the 64 bit secure force algorithm for the code implementation of the encryption and decryption process and DWT & QSWT coding for the hiding module. The complete screenshots of the encrypted image, vectored input, hiding module, encoded and decoded image outputs, the embedded stego image and the final decrypted image along with the histograms of all the above are mentioned in this section.

The program after video to frame conversion is shown in Figure 6. After the video has been converted into a single frame matlab will store that frame for further use and will ask for the required biometric input. At this point after we select the image the encryption procedure will begin. The encryption process and the output image after that process is discussed in section-II and the resulting image is shown in Figure 5. The secure force encryption takes about 10-15 minutes to process and we get the output as seen in that figure. This is the most important step in this entire algorithm.

In Figure 7 we can have the comparison of the histogram of original and encrypted and images. We can clearly see the difference in the histograms of the original and the encrypted image. The original image has more light tones, a little mid tone and almost No. dark tones. But the encrypted image has uniform light, mid and dark tones, which confuses an attacker and reduces the chances of a possible MIM (man in middle) attack.

The encrypted biometric image is converted into a vector using matlab so as to make it easy and more secure when embedding it within the original image. The vectored biometric image is shown in Figure 8. The hiding module contains the DWT domain and the output of this section is shown in Figure 9.

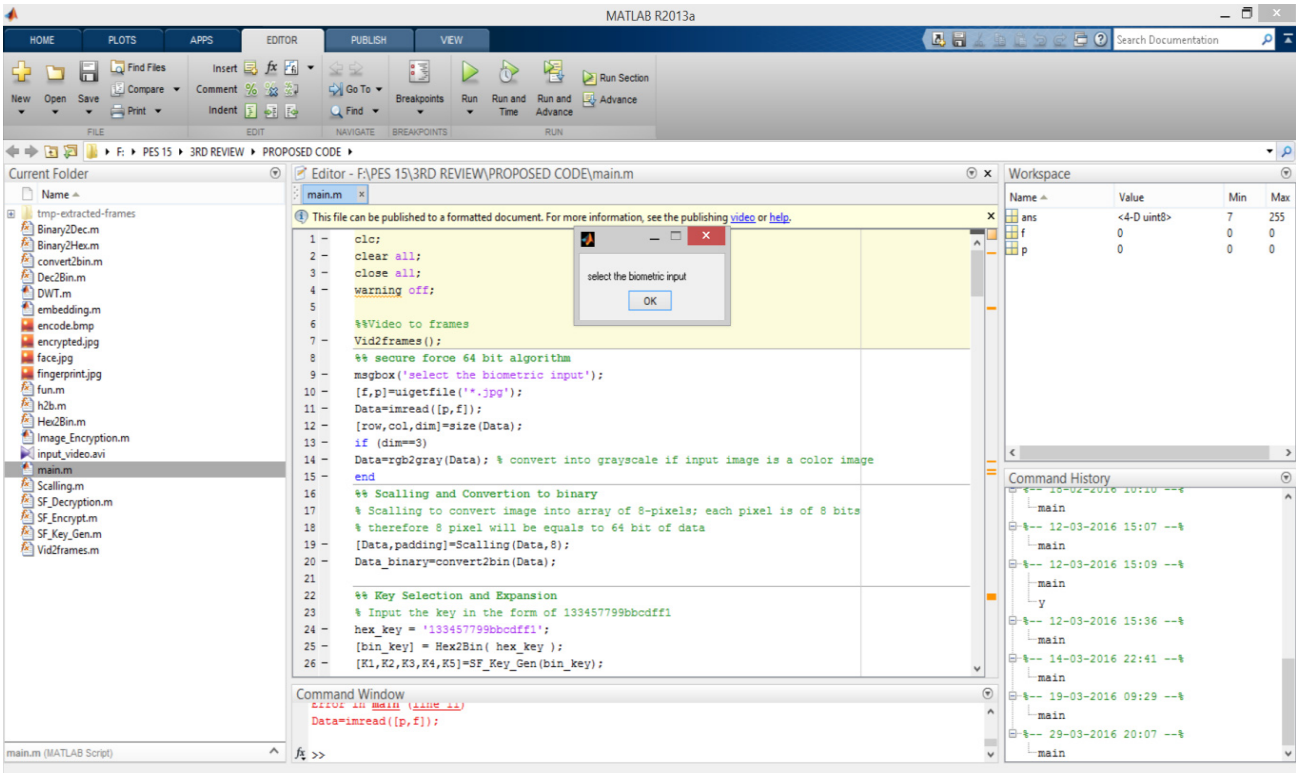

Figure: 6: Program after video to frame conversion

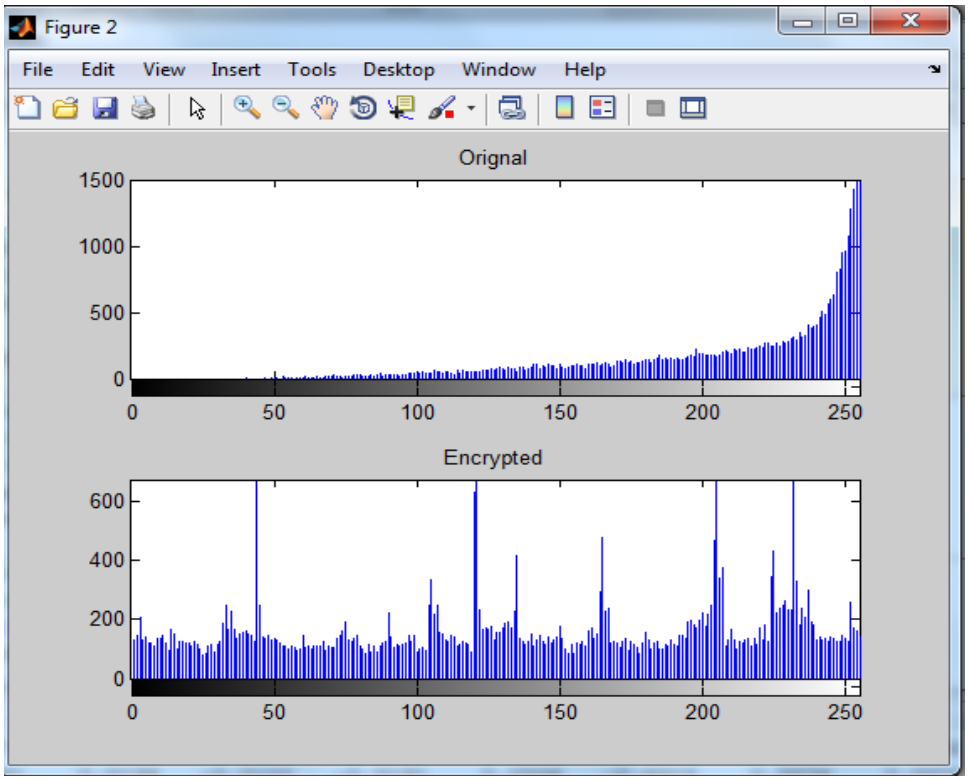

Figure 7: Comparison of original image and encrypted image

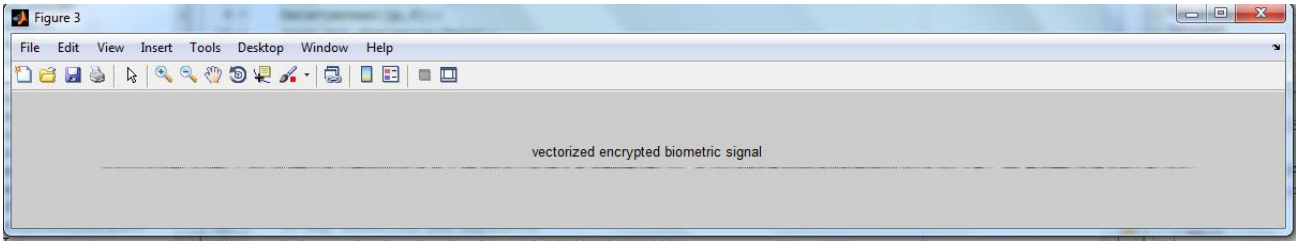

Figure 8: Vectored encrypted biometric signal

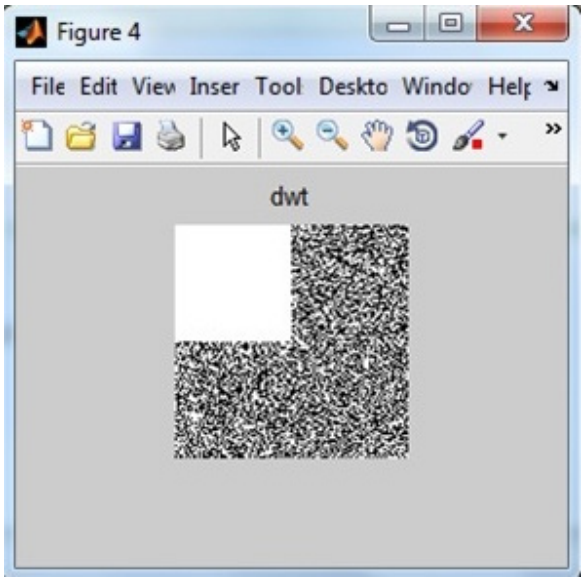

Figure 9: The hiding module containing DWT domain

The QSWT encoding process is now activated and the input image fed is given as shown below.

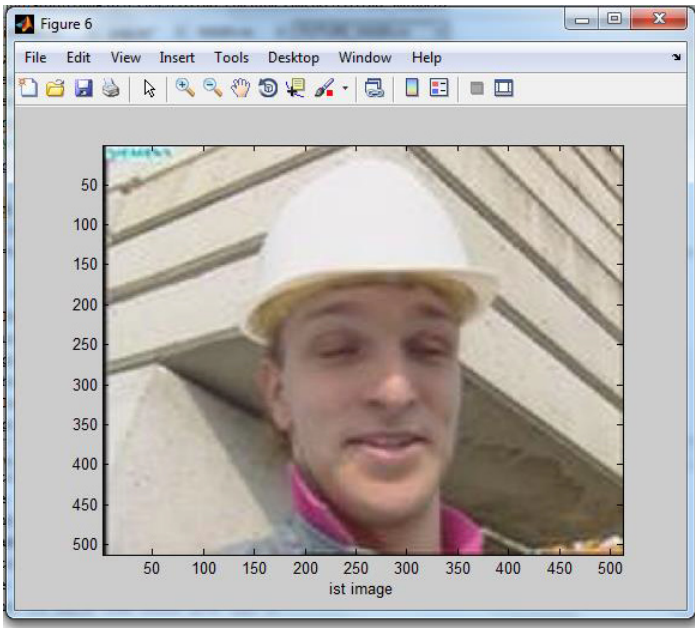

Figure 10: Original image input for QSWT encoding

After the DWT domains matlab will ask for the input required for QSWT encoding. The input image is QSWT encoded and it takes some time to complete.

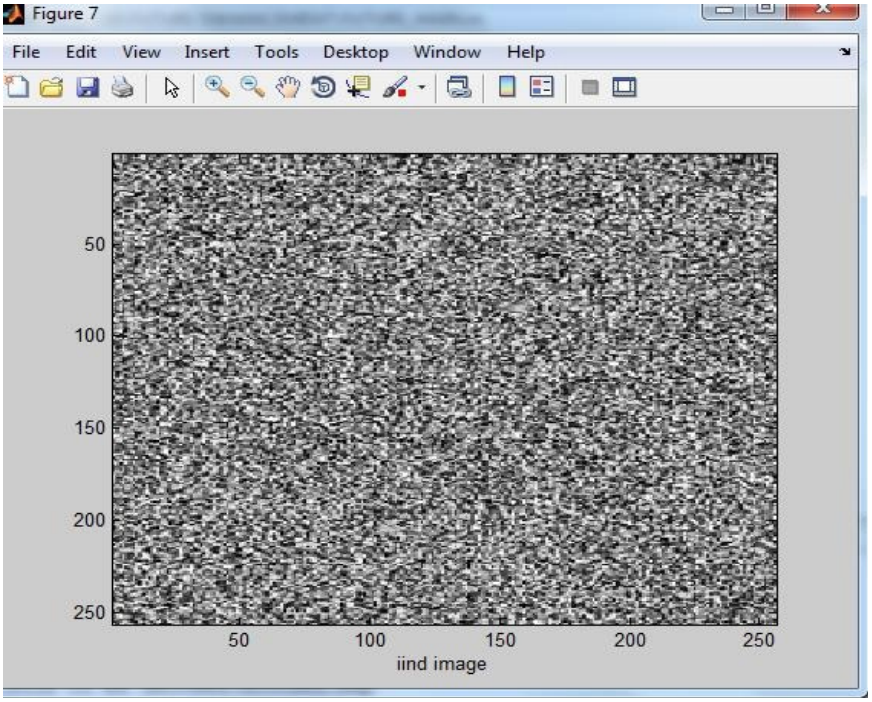

Figure 11: Biometric image input for QSWT encoding

Creating the data embedded stego image is the second major step in this whole program. Here the biometric image encrypted and converted into a vector signal has been embedded within the original image thus creating a stego image which is shown in the Figure 12.

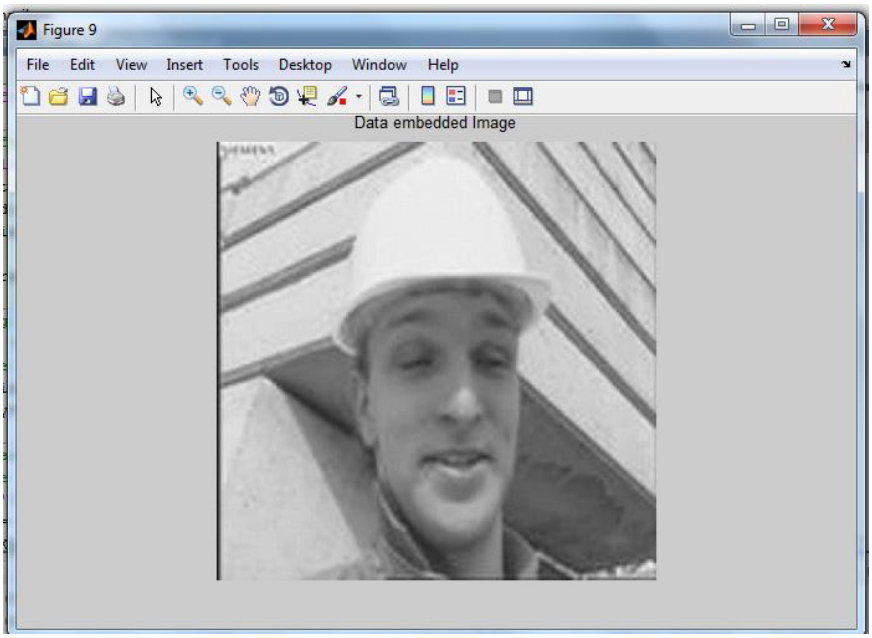

Figure 12: Data embedded Stego image

After the stego image has been created successfully, we get the histogram for the input and the embedded image as seen in the Figure 13. Here we can see very less or No. difference in the two histograms. So an attacker will have less chances of finding out that a biometric image is hidden within the original image.

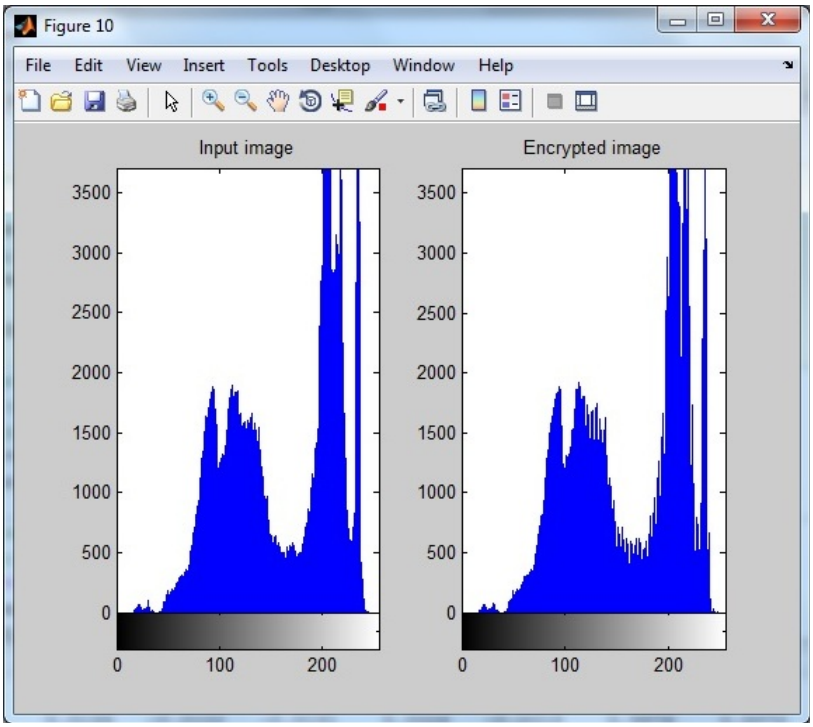

Figure 13: Histogram for the input and embedded image

The embedded stego image can be decoded very easily whenever required. After decoding the restored image obtained is shown below:

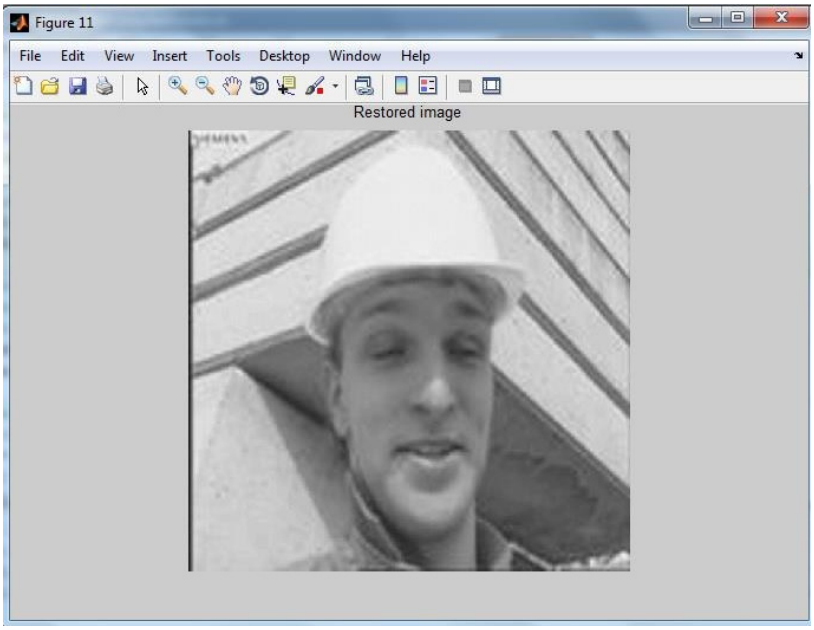

Figure 14: Image obtained after decoding

When we analyse the histogram of input and restored (decoded) image, there is No. much difference which makes the whole algorithm more secure. This is shown in Figure 14.

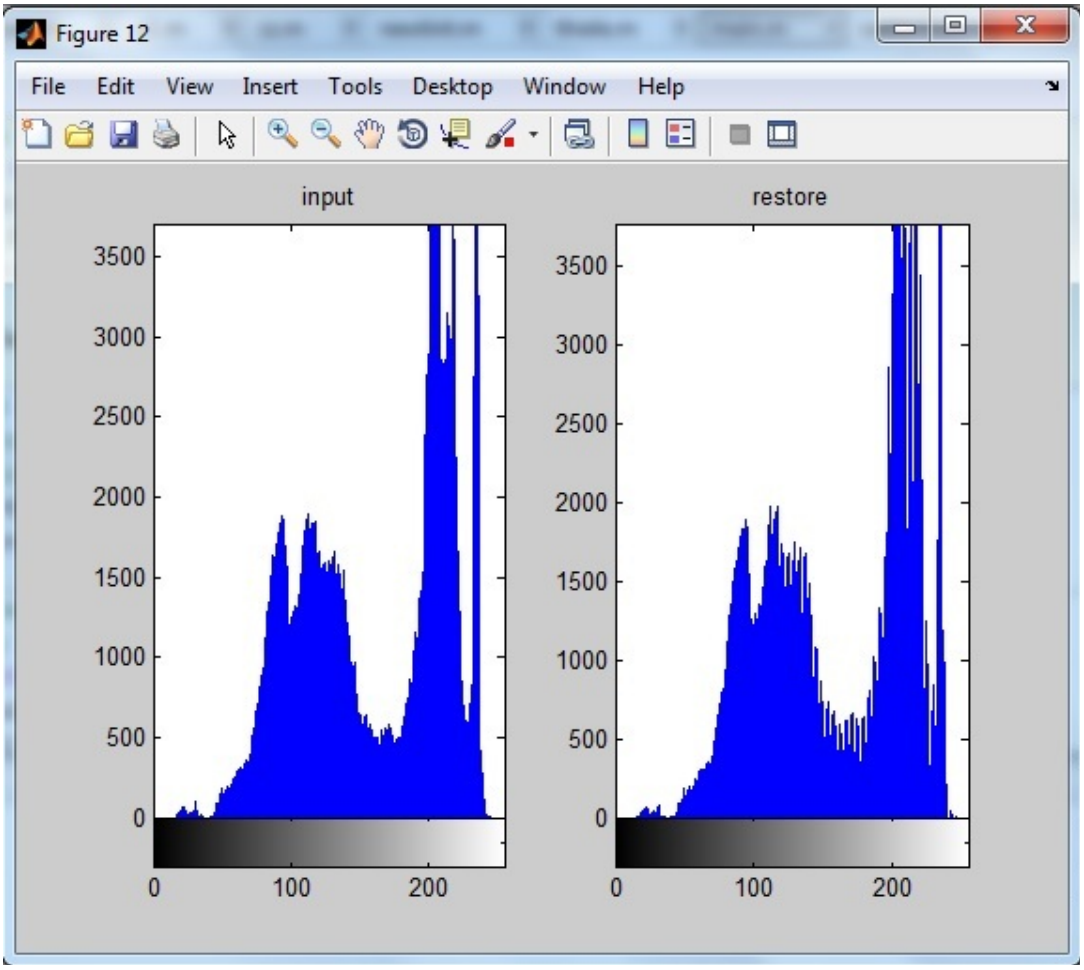

Figure 15: Histogram of input and restored image

The original biometric image can be easily decrypted to its original form (Figure 16) easily and the decryption mechanism using secure force algorithm is almost the same. The histogram of the image which we obtain after the decryption is complete (Figure 17) and it is same as the histogram of the original biometric image (Figure 7).

B. Conclusion and Future Work

Biometric signal authentication plays a vital role in todays life especially in government activities, military establishments where crucial procedures are undertaken. As steganography on its own does not ensure security, it is combined with chaotic encryption mechanism. The methodology adopted here apart from providing results that is barely indistinguishable to human vision it also provides a stego-object that can avoid various signal deformations and steganalytic attacks.

Future efforts may include compression and mobile transmission of other biometric signals like voice, iris can be investigated. As there are lot of biometric data loss that are encountered nowadays, attempts can be done to perform verification of missing parts i.e., parts that don't contain significant data.

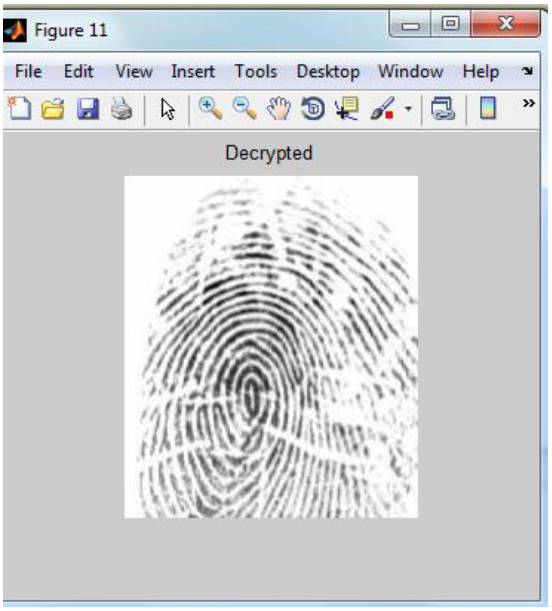

Figure 16: Obtained decrypted biometric image

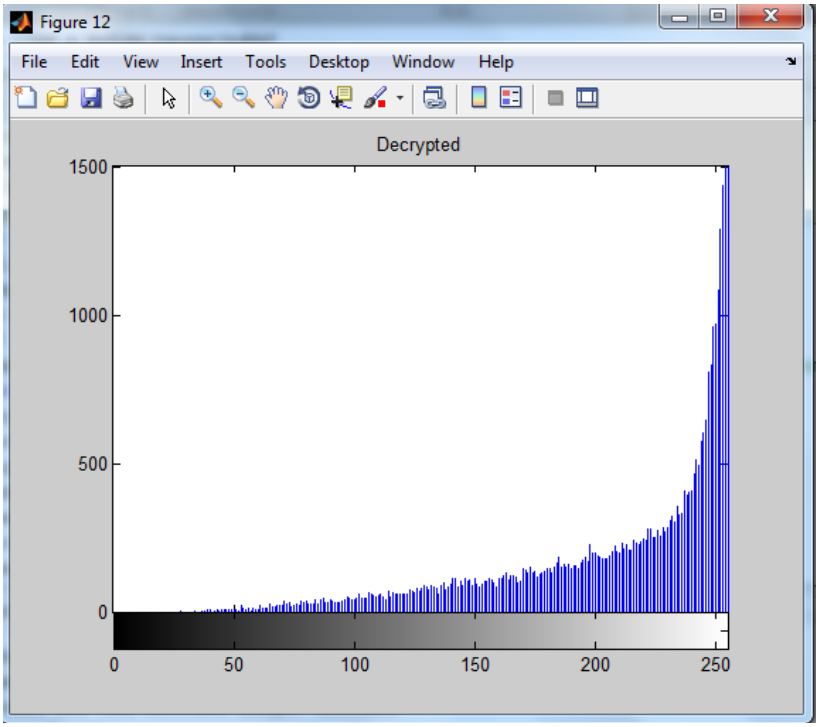

Figure 17: Histogram of decrypted image

REFERENCES

[1] Chuang, M.C., & Chen, M.C. (2014). "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics." *Expert Systems with Applications*, *41*(4), 1411-1418.

[2] Jain, A.K., Ross, A., & Prabhakar, S. (2004). "An introduction to biometric recognition." *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4-20.

[3] Ramkumar, M., & Akansu, A.N. (2001). "Capacity estimates for data hiding in compressed images." *IEEE Transactions on Image Processing*, *10*(8), 1252-1263.

[4] Madhusudhan, R., & Mittal, R.C. (2012). "Dynamic ID-based remote user password authentication schemes using smart cards: A review." *Journal of Network and Computer Applications*, *35*(4), 1235-1248.

[5] Li, S., Mou, X., & Cai, Y. (2001). "Improving security of a chaotic encryption approach." *Physics Letters A*, *290*(3), 127-133.

[6] Khan, S., Ibrahim, M. S., Ebrahim, M., & Amjad, H. (2015). "Security Analysis of Secure Force Algorithm for Wireless Sensor Networks." *arXiv preprint arXiv:1509.00981*.

[7] Pandian, R. (2015, February). "Evaluation of image compression algorithms." In *Underwater Technology (UT), 2015 IEEE* (pp. 1-3). IEEE.

[8] Provos, N., & Honeyman, P. (2003). "Hide and seek: An introduction to steganography." *IEEE Security & Privacy*, *1*(3), 32-44.

[9] Rao, N.N., Thrimurthy, P., & Babu, B.R. (2009). "A novel scheme for digital rights management of images using biometrics." *International Journal of Computer Science and Network Security*, *9*(3), 157-167.

[10] Khan, S., Ibrahim, M.S., Ebrahim, M., & Amjad, H. (2015). "Security Analysis of Secure Force Algorithm for Wireless Sensor Networks." *arXiv preprint arXiv:1509.00981*.

[11] Carminati, B., Ferrari, E., & Perego, A. (2010). "A decentralized security framework for web-based social networks." *Pervasive Information Security and Privacy Developments: Trends and Advancements: Trends and Advancements*, 356.

[12] Wang, Y.Y., Liu, J.Y., Xiao, F.X., & Dan, J. (2009). "A more efficient and secure dynamic ID-based remote user authentication scheme." *Computer communications*, *32*(4), 583-585.

[13] Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010, October). "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* (pp. 162-175). ACM.

[14] Zebbiche, K., Ghouti, L., Khelifi, F., & Bouridane, A. (2006, June). "Protecting fingerprint data using watermarking." In *First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06)* (pp. 451-456). IEEE.

[15] Madero, A. (2013). "*Password secured systems and negative authentication"* (Doctoral dissertation, Massachusetts Institute of Technology).

[16] Liao, I.E., Lee, C.C., & Hwang, M.S. (2006). "A password authentication scheme over insecure networks." *Journal of Computer and System Sciences*, *72*(4), 727-740.

[17] Kumar, A., & Tiwari, M.N. (2012). "Effective implementation and avalanche effect of AES." *International Journal of Security, Privacy and Trust Management (IJSPTM)*, *1*(3/4), 31-35.

[18] Ntalianis, K., & Tsapatsoulis, N. (2016). "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks." *IEEE Transactions on Emerging Topics in Computing*, *4*(1), 156-174.

[19] Joe, B. (2015). "A Dual Face Detection Water Marking System Using Sf For Verifying Security." *International Journal of Applied Engineering Research*, Vol. 10, Issue 5, pp. 11599-11609.

[20] Jakobsson, M., & Dhiman, M. (2013). "The benefits of understanding passwords in Mobile Authentication" (pp. 5-24). Springer New York.

[21] Hoang, T., Tran, D., & Sharma, D. (2008, December). "Remote multimodal biometric authentication using bit priority-based fragile watermarking in Pattern Recognition." *ICPR 2008. 19th International Conference on* (pp. 1-4). IEEE.

[22] He, D., & Wang, D. (2015). "Robust biometrics-based authentication scheme for multiserver environment." *IEEE Systems Journal*, *9*(3), 816-823.

[23] Das, A.K. (2011). "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards." *IET Information Security*, *5*(3), 145-151.