ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

A Framework of Robust Video-Object Steganographic Mechanism over Wireless Networks using Arnold Transform

P SOWMIYA[1] , W T CHEMBIAN[2*] M.E, M.I.E.T.E, (Ph.D.) AND S Aravindh[3] M.Tech., M.B.A.,

[1]Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.
[2]Head of the Department, Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.
[3]Associate Professor, Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.
*Corresponding author: W. T. CHEMBIAN (csehod@gojaneducation.com)

ABSTRACT

To protect the resources from unauthorized users, the remote user authentication have become an essential part in the communication network. With the development of information security, the traditional image encryption algorithm has been far from to ensuring the security of images in the transmission process. The main objective of the proposed work is to get the permission for accessing element through remote authentication by hiding encrypted biometric signal within image of the user. The biometric signal is encrypted using symmetric key image encryption technique that first scramble the locations of the pixels using four 8-bit sub keys and then encrypt the pixel values by XOR the selected 8-bit key. The scrambling operation is done using Arnold Transform Algorithm and hided into the cover image with Qualified Significant Wavelet Tree (QSWT). The Compressed cover image gets transmitted over wireless channel for remote authentication. The Inverse Wavelet Transform is used to separate encrypted signal and the cover image. The biometric signal gets decrypted by XOR operation and inverse Arnold transformation algorithm. The Arnold transform algorithm increases the Normalized Cross Correlation (NCC) value for normalizing the image in order to improve the quality of reconstructed image. Hence, the XOR operation then change the pixel values making the image very meaningless. And so the error is minimized in the proposed system compared to the existing techniques. The problems identified in the existing systems such as data loss, complexity and accuracy in biometric signal has been overcome by the proposed system. The proposed system can be used in military purposes for sharing confidential data. The data can be accessed over remote areas in secured manner.

INDEX TERMS: Arnold Transform, Scrambling, XOR Operation, Remote Authentication, Biometric Signal, QSWT, Steganographic Video Object.

1. INTRODUCTION

The development of Internet has revolutionized the lifestyle of the people. In the recent time, more and more traditional day-to-day affairs, like access to information, entertainment, financial services, and product purchase are carried out through the Internet. The exchange of personal information through insecure channel is forcing

people to be concerned with Internet security. Authentication of any remote user, based on their identity, is a part of essence in Internet security. The authentication is used to confirm the identity or originality of the person by ensuring the details which are given by that person. There are two types of authentication namely positive authentication and negative authentication. In this the positive authentication is already implemented in the existing systems. In order to detect and eliminate the cyber-attack the negative authentication is implemented. The examples are given below to show the difference between positive authentication and negative authentication. In the example there is a system based on password based authentication. The system contains positive authentication with a set of limited passwords for each and every user which was saved in a separate file. If the intruders crack the file the may enter into the users account. Whereas in the negative authentication, there is a anti-password space which contains the string that is not present in the password file. Here if the intruders get into the anti-password file also it is difficult to find the original password of the user. So that the negative authentication technique provides more security features than the existing positive authentication technique.

The positive authentication system is used in the proposed scheme and at least two or three of the following factor should be true for security reasons:

- The Person who is going to authenticate should have identity card, mobile phone, security token etc. These are ownership factor.
- The Person who is going to authenticate should know password, PIN number, pattern etc. These are knowledge factor.
- The Person who is going to authenticate should undergo fingerprint, retinal pattern, facial reorganization, DNA sequence, other biometric identifier etc. These are inherence factor.

According to the report in[7], the 12.6 million customers affected in US by fraud Identity and $4.6 billion loss for them. In overall 5.3% is the probability of people who affected in the fraud identity. In order to overcome the fraud identity the robust remote human authentication technique is introduced in many literatures[4–6]. In that many people suggest password and smart card for remote

authentication. By referring advantages and disadvantages of the remote authentication technique the biometric signal is found to be best technique for authenticating purposes.

The biometric signals are already used in the existing system. For submitting as password in the smart cards alone the biometric signal is used. Biometrics has already been incorporated in remote authentication but only as password substitution in smart cards. In order to investigate their full potentiality, biometrics can be incorporated in hybrid crypto-Steganographic schemes. In particular, cryptographic algorithms can scramble biometric signals so that they cannot be understood, then hide the scrambled image from the intruders steganographic technique is implemented to hide the scrambled biometric signal into the cover image that is the image of the person. In the proposed system we implemented some methods and technique to overcome the problem which has been faced in the existing remote authentication system. Here the head-and-body detector is used to extract the face and body of the person from the image that is Video Object (VO).

1.1 Remote Authentication

The one-way hash function technique was implemented in the remote password authentication scheme which was proposed by Lamport[3]. In that system the user id and the passwords are maintained in separate verification table. It is difficult to maintain the verification table in the remote server. The attackers can modify the variables that are passwords by cracking the verification table. In order to overcome the weakness in this remote authentication technique Diffie-Hellman Key agreement protocol is reported by Liao et al.[8]. In this report, the session key is used to encrypt and decrypt the message which have been communicated by using the symmetric encrypt system. In that the random cryptographic keys are generated, so that it is difficult to memorize that password as well as it is difficult to store random password in the table. Whereas

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

the passwords which are used here is simple and can be easily guessed by attackers. Some users will use same password for all applications. In such case if the attacker finds the password of the user in a single application means they can easily access the other applications of the same user. The remote authentication scheme in smart cards using dynamic user's identity[8-9] is another technique which is proposed to overcome defects in the

previous technique. The use of static password in smartcards through wireless channels may leak the details about the user. In order to overcome the difficulties by using the static password that is constant password for the smart cards in the proposed scheme they are using dynamic passwords that is the n password can be changed for each and every transactions. So there is no chance for intruders (or) attackers to guess the password, but the drawback here is (a) users should always have their smart cards with them in order to do transactions, (b) if a user loses his/her smart card, he/she will not be able to do any transactions and should wait for the reissuing of the card (sometimes several days), (c) smart cards cost money and effort each time they are (re)issued, (d) due to low power they cannot perform very complex computations. Many of the aforementioned password-based authentication problems can be confronted using biometrics[10]. Biometrics are inherently more reliable, since biometric traits cannot be lost or forgotten, they are more difficult to forge, copy, share, and distribute.

1.2 Steganographic Methods

The main purpose of Steganography, which means 'writing in hiding' is to hide data in a cover media so that others will not be able to notice it (Figure 1). While cryptography is about protecting the content of messages, steganography is about concealing their very existence[11]. Many compression techniques[12] are used in the literature for steganography. The Qualified Significant Wavelet Trees (QSWTs) is used in this technique to hide the image into the cover image. Discrete Wavelet Transform (DWT) are used for compression of the images which is in JPEG, MPEG formats etc. By using this methods the lossy messages are send through wireless channels without any loss during transmission and it will protect the hided data from attacks. Even though the process will protect the data loss, the loss of data will occur in some minute area.

There are two components used in steganography of the image namely soft-authenticator watermark and chrominance watermark. The soft-authenticator watermark is used for authentication purposes to avoid image tampering. The chrominance watermark is used to enhance the compression efficiency of the image. The DWT and Integer Wavelet Transform (IWT) is combined

and proposed by Hemalatha et al.[13]. In that the encrypted key and the secret image is hided into the cover image. But it is quite complex to implement the embedding algorithm.

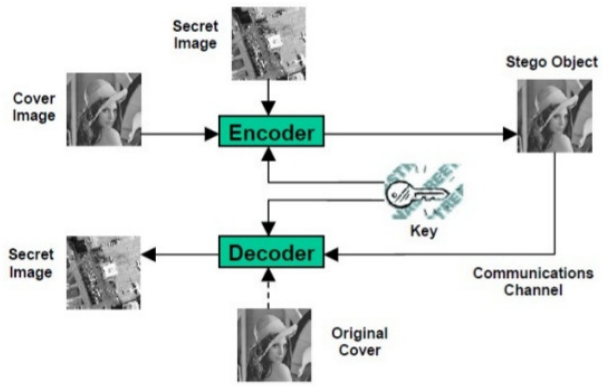


Figure 1. Steganography Process.

For the minutiae embedding of the image wavelet-based steganographic method is useful. The hided information can be easily found when the attacker knows the embedding algorithm. A last category of approaches involves data hiding within image or video objects of the cover image. Object-oriented data hiding is more secure

and robust against deciphering attacks but it usually creates visually sensitive artifacts.

2. PROPOSED REMOTE SERVICE ACCESS USING BIOMETRICS

2.1 Encryption using Arnold Scrambling Algorithm and XOR Operation

There are many types of methods available that can do Image Encryption[14-16], and the majority of them are scrambling algorithms based on pixel shuffling. In 2011 Zhang et al. proposed an image encryption method based on total shuffling scheme[3]. Pixels shuffling based image encryption techniques have one problem that it cannot change the histogram of an image. Hence, their security performances are not good. The encryption method that combines the pixel exchanging and gray level changing can handles reach a good chaotic effect. Our proposed

method do this job. The process of transforming a digital image into another meaningless image by scrambling the original image is known as Arnold scrambling algorithm. By this algorithm the digital image gets preprocessed before hiding the image into the cover image. This process is also called as information disguise. The non-password technique can be followed by scrambling and hiding image into another image. So there is no need to memorize user id and password. This technique provides confidential and secure data transmission. To change the distribution of error bit in the image some watermarking techniques implies image scrambling method before hiding the image into another image. Many digital watermarking techniques uses Arnold transformation algorithm before it gets processed. This transformation algorithm undergoes images with $(N^{*}N)$ pixels shows in the Equation (1).

The Figure 2 shows the coordinates for the image as (x,y), by implementing Arnold Transformation technique the coordinated (x,y) gets transformed to another point (x',y') is represented as,

[x';y']= [1 1 ; 1 2] * [x ; y] mod(N) ….....(1)

x, y ∈ {0,1,..., N - 1}, (x, y) and (x′, y′) are the coordinates of the pixels before - and - after scrambling.

The transformation specified here is two-dimensional Arnold Scrambling. The right side is the coordinates of input image. Then the left side is the coordinates of output scrambled image. The iterative process should be done for n successive nodes. Equations for encryption and decryption is given below:

Encryption:

p = [1 1 ; 1 2] * [x ; y];

out(mod(p(2), m)+1, mod(p(1), m)+1) = in(y+1, x+1)

x=row; y=column, out=encrypted image, in=input image

Decryption:

p = [2 -1 ; -1 1] * [x ; y];

out(mod(p(2), m)+1, mod(p(1), m)+1) = in(y+1, x+1);

Where n denotes the number of iterations, n = 1,2,3… the iteration process will continues until all the pixel in the given image gets transformed. Where cycles undergoes

transformation is denoted as *T* whereas size of the image is represented by N.

The Arnold Transform algorithm shows the transformation of original image into scrambled one. So that the intruders can't get the original image even though they hack the data while transmitting over wireless channels. Because after scrambling the image gets vectorized that is the original image is not visible to others. The sender and the receiver alone knows the rounds which was undergone while generating chaotic map.

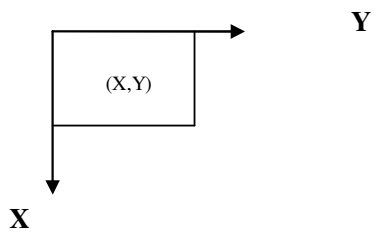


Figure 2. Image coordinates.

The key which was used to generate the chaotic map is very simple while comparing with other encryption technique. Then the original image will not get revealed in the wireless transmission. Therefore the Arnold transformation algorithm plays a major role in the overall encryption techniques. In this system before hiding image

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

into another image the secrete image gets encrypted by the Arnold transformation algorithm that is given in Figure 3.

Block Level XOR Operation

The input gray scale image denoted as X. For additional security, after the completion of Arnold transform use the Scrambled image X_S as the input for block level XOR operation and encrypt it using equation below to generate the final encrypted image X_C. The Scrambled image X_S is divided into 2 pixels × 2 pixels blocks. The image pixel contained by every block $P_{i,j}$ of XT is encrypted using block level XOR operation by four eight bit sub key K1 K2 K3 and K4. As given below respectively.

$$P'_{1.1} = P_{1.1} \oplus K1$$
$$P'_{1.2} = P_{1.2} \oplus K2$$
$$P'_{2.1} = P_{2.1} \oplus K3$$
$$P'_{2.2} = P_{2.2} \oplus K4$$

Where $P_{i,j}$ is the pixel value at i^{th} and j^{th} location in block inside pixel of image .the encrypted image by using the XOR operation is called by cipher image X_C and it is ready to be sent to receiver site. The total size of key in our algorithm is 32 bit long which proves to be strong enough.

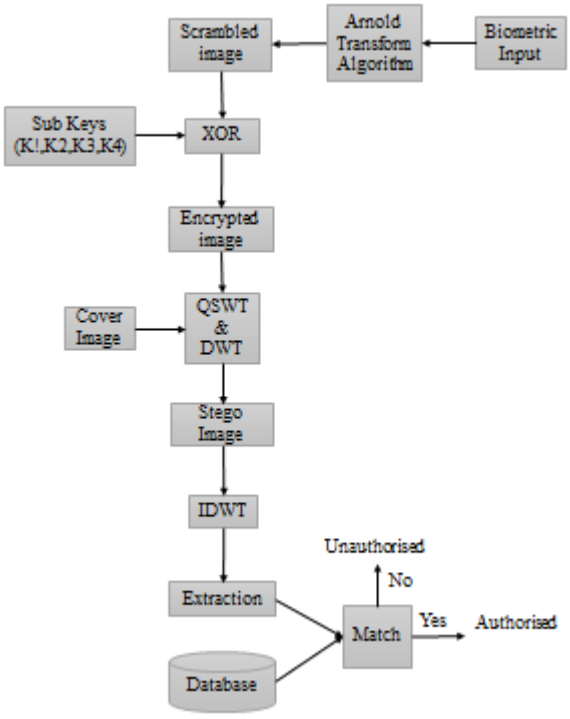


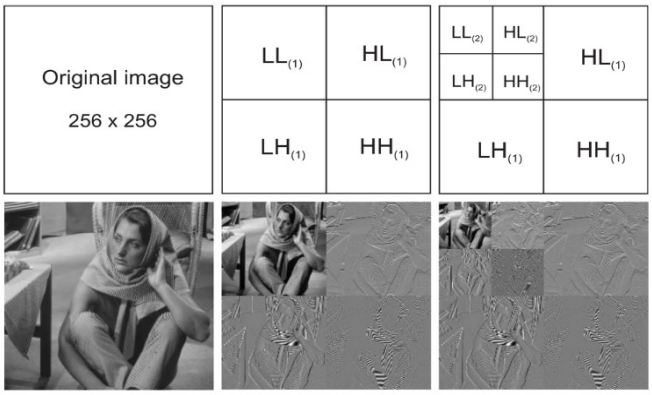
Figure 3. Block diagram for remote authentication.

2.2 Discrete Wavelet Transform

Discrete wavelets transform is a signal analysis theory. It is a time and frequency domain analysis method which can localize time and frequency domain, and has widely used in many fields. The basic idea of DWT is the detailed frequency separation on signal, namely multi-resolution decomposition. The host graph is decomposed to four sub-graphs in size of one quarter: one low frequency approximation graph and three medium and high frequency detail sub-graphs in horizontal, vertical and diagonal direction. The human visual system (HVS) is more sensitive to image modifications in smooth areas

(low frequency components) than texture and edges areas (high frequency components).

The Discrete Wavelet Transform is used to hide information like text, audio, video, images etc., into cover image. The steganographic technique is implemented in the discrete wavelet transform. In this technique the cover image is divided into four equal parts with respect to the resolution of the image that is (128*128) bits. The four parts is represented as low, middle and high frequencies that is represented as LL, HL, LH and HH. There are two operation which undergoes in DWT namely Horizontal operation and vertical operation.



(a)

(b)

Figure 4. Image decomposition. **(a)** One level. **(b)** Two level.

First step undergoes horizontal operation that is the analysis done in horizontal direction the pixels from left to right and then stores the addition of the nearby pixels in the left side. The subtraction of the neighboring pixels is done and the difference value is stored into the right side. In the original image left side that is sum denotes Low frequency part (L) and the right side that is the product denotes High frequency part (H). The host video object is decomposed into two levels using the discrete wavelet transform (DWT)[17]. Then the image undergoes two level of decomposition that is given in the Figure 4.
Vertical operation is done in second step. The pixels are analyzed in vertical direction that is from top to bottom. The addition of the nearby pixels is performed and on the top the sum valued gets stored. Then the subtraction of

the neighboring pixel is performed and on the bottom the difference value gets stored. Then LL, LH, HL, HH are the four sub-bands will generated after this process. The original image is same as the low frequency band in sub-bands. The higher level DWT is obtained after decomposing the LL sub-bands. The vertical, horizontal, diagonal sub-bands are represented as LH, HL and HH respectively. The DWT is the process of hiding image into another image. Then the image is divided into four different parts with respect to the pixels (240*240 pixels). Then the image is inserted to the parts with low frequency level. The horizontal operation and the vertical operation is given in the below diagram.

3. EXPERIMENTAL EVALUATION

The experimental values are examined to compare the efficiency, robustness, effectiveness and accuracy of the proposed system with the existing system. The experiment for our proposed system is done with 100 biometric signals and 100 images. The analysis starts with the Encryption of the image. Here the encryption of the image is done with the Arnold Transform algorithm along with XOR operation which consist of the cover image as well as the secret image.

4. CONCLUSION

The proposed method provides confidentiality and security for the remote data authentication. The Arnold algorithm along with XOR operation is used in the proposed system in order to reduce the complexity and minimize time consumption for scrambling the image. Then QSWT and DWT provides high level of robustness in compression standards and the image quality is also maintained after decompression. Finger print is used here as a biometric input for improving accuracy and to eliminate fraud access.

5. REFERENCES

1. Klimis Ntalianis, Member, IEEE, and Nicolas Tsapatsoulis, Member, IEEE, “Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Network,” *IEEE transactions on emerging topics in computing*, Mar. 2016.

2. Areepongsa .S, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao,(2000) “Steganography for a low bit-rate wavelet based image coder,” in Proceedings of the *IEEE*

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Conference on Image Processing, vol. 1. IEEE, 2 pp. 597–600.

3. G. Zhang, and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Opt. Commun.* vol. 284, pp. 2775-2780, 2011.

4. Chun-Ta Li and Cheng-Chi Lee, "A Robust Remote User Authentication Scheme Using Smart Card," vol. 40, no. 3, pp. 236-245, 2011.

5. Hongfeng Zhu, Man Jiang, Xin Hao and Yan Zhang, "Robust Biometrics-Based Key Agreement Scheme With Smart Cards Towards A New Architecture," *Journal of Information Hiding and Multimedia Signal Processing*., vol. 6, no. 1, Jan 2015.

6. Khanjan Ch. Baruah, Subhasish Banerjee, Manash P. Dutta and Chandan T. Bhunia, "An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card," *International Journal of Security and Its Applications*, Vol.9, No.1 (2015), pp.397-408.

7. A. Pascual and S. Miller, "Identity fraud report: Data breaches becoming a treasure trove for fraudsters," *Javelin Strategy Res*., pleasanton, CA, USA, Tech. Rep. 1/2013, 2013.

8. E.-J. Yoon, S.-H. Kim, and K.-Y. Yoo, "A security enhanced remote user authentication scheme using smart cards," *Int. J. Innovative Comput., Inf. Control*, vol. 8, no. 5(B), pp. 3661-3675, May 2012.

9. Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Comput. Commun.*, vol. 32, no. 4, pp. 583-585, Mar. 2009.

10. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4-20, Jan. 2004.

11. Stefan Katzenbeiser and Fabien A.P.Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House, Computer Security series, Boston, London, 1999.

12. C.P. Sumathi , T. Santanam and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *International Journal of Computer Science & Engineering Survey (IJCSES)* Vol.4, No.6, Dec 2013.

13. S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure color image steganography in transform domain," *Int. J. Cryptography Inf. Secur.*, vol. 3, no. 1, pp. 17_24, Mar. 2013.

14. X. Li, J. Knipe, and H. Cheng, "Image Compression and Encryption Using Tree Structures," *Pattern Recognition Letters*, Vol. 18, No. 8, pp. 2439 2451, 1997.

15. X. Wang, and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," *Opt. Commun*. vol. 284, pp. 5804-5807, 2011.

16. Y. Zhang, J. Xia, P. Cai, and B. Chen, "Plaintext related two-level secret key image encryption scheme," TELKOMNIKA. vol. 10, pp. 1254-1262, 2012.

17. S. Li and W. Li, ``Shape-adaptive discrete wavelet transforms for arbitrarily shaped visual object coding," *IEEE Trans. Circuits Syst. Video Technol*., vol. 10, no. 5, pp. 725_743, Aug. 2000.