A Robust Video-Object Steganographic Mechanism for Remote Authentication

Souparnika M P[1], Preethy Mol B[2], Saritha K[3]

[1]*M. Tech. Student,* [2,3]*Asst. Prof.*

Dept. of Computer Science and Engineering, Nehru college of Engineering and Research Centre, Thrissur, Kerala, India

Abstract - Many sensitive information are usually transmitted over wireless network for remote authentication. These information can be identification numbers, biometric signals, passwords, etc. Since these kind of information are highly sensitive we have to give high security to these while sending over wireless networks. Many kind of techniques are used for providing security and authentication like watermarking, steganography etc. But watermarking is a kind of old method while steganography is popular and effective. Steganography is a process of hiding a secret message (can be a password, biometric signal, etc.) in to a cover media like image audio, video, etc. Here we are using a biometric signal like finger print, and encrypt it by using chaotic encryption then hide in a video object. This video object is partitioned and shuffled before hiding by using QSWT. This module will send over the wireless network which give high robustness to the attacks and a high security level.

Keywords: Steganography, Video object, Biometric signal.

I. INTRODUCTION

Steganography is a practice of hiding a file, video, audio, image, message within another file, message, video, audio, image. The word steganography combines the greek word ‘steganos’ meaning covered, concealed or protected and ‘Graphein’ meaning writing. Wireless transmission of sensitive information like passwords, id numbers, biometric signals etc are common. Usually in the case of online inter views, video conferencing remote authentication is an in evitable part. Sice remote authentication include sending some kind of authentication information which is very sensitive over wireless networks, we have to provide high degree of efficient Security. Especially in the case of video conference we appearing in a whole manner to the other party so it must be highly secure and the other party must be authorized ensuring security. In old days water marking is dependable but today it become an old technology. Steganography is mainly used for hiding sensitive information while sending over wireless networks. Steganography is popular and effective. Steganography is a process of hiding a secret message (can be a password, biometric signal, etc.) in to a cover media like image audio, video, etc. Different effective techniques are used for steganography over years. DCT(Discrete cosine transform)[2], DWT(Discrete wavelet transform)[3], IWT(Integer wavelet transform)[4], and some techniques uses dual domains. All these techniques have many advantages and disadvantages. QSWT[1] algorithm is another important technique or method for steganography which is dominating in terms of security since it is adding some more conditions to the previous technologies.

In this paper we are proposing a new technique for improving the security of the stego object or the hiding module. Here we extract the video object and then partition it in to several parts. Then we rearrange these partitions for hiding the encrypted biometric signal using QSWT. After hiding we again rearrange the partition in the right order then send it over the receiver. At the receiver side if we want to get the encrypted biometric signal we have to correctly rearrange the video object as we arranged it in the sender side which is only known by the receiver.

II. SYSTEM MODEL

Remote authentication includes hiding a secret information into a text, audio, image, video etc, and send it over the wireless network to the receiver side. Since the information sending through wireless network , it is exposed to several attacks like brute force attack.

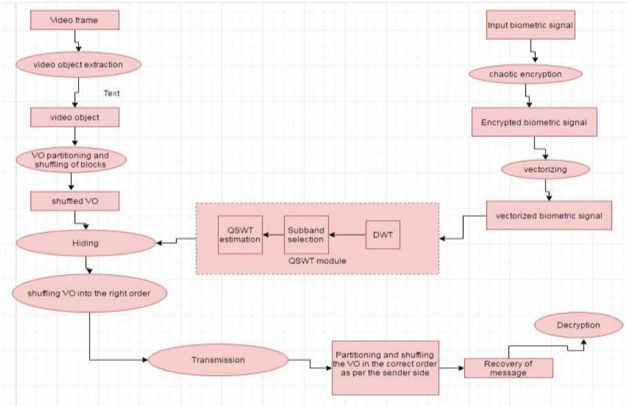

Fig. 2.1 Flow diagram of proposed system

So we have to concentrate on the security of hiding module. The proposed system mainly have six modules. Firstly it extract the video object form a video frame. Then this video object should decompose in to several blocks and shuffle these blocks according to a password known by only sender and receiver. A biometric signal will take separately and encrypt it by using chaotic encryption. This encrypted biometric signal will hide inside the shuffled video object using QSWT. Then again this video object will shuffled to the right order. Finally this module will compress and send it over wireless network to the receiver. At the receiver side it will reshuffle according to the password and them recover the message by using IDWT. The flow diagram of the system is shown in the Fig. 2.1.

III. PREVIOUS WORK

1.DCT (Discrete cosine transform) [2]

DCTis a steganographic mechanism which utilizing the LSB (least significant bit) for hiding. An image is a set of pixels, its is a matrix. DCT converts the pixels of an image into special frequencies.ie, DCT is a technique which is performed or which sees an image as a special domain.DCT converts the pixels of an image into special frequencies. Since an image is a matrix and a matrix is a two dimensional object we use 2D-DCT[1]. The two dimensional DCT is applied on blocks of 8x8 pixels then this pixels are transformed into 64 DCT co-efficients[2]. After this quantization the LSB of the quantized co-efficients are selected. The secret messages that we want to hide is embedded in these LSB bits for security.

The main advantages and disadvantages of this technique are described below.

ADVANTAGES

- Less complicated compared to other techniques
- Selection of LSB bits for hiding less time taking process
- LSB technique has been used to accommodate maximum payload

DISADVANTAGES

- During quantization less important frequencies are discarded
- Only most important frequencies reach at the receiver which used for reconstruction of the image
- Reconstructed image may become distorted

2. DWT (Discrete wavelet transform) [3]

DWT is one of the most popular and effective steganographic technique. It embeds the secret message in a frequency domain unlike the DCT. In DCT the message embeds in a spatial domain while DWT embeds in frequency domain. In DWT it divides the frequency domain in to four different frequency bands (HH,HL,LH,LL). Out of these the secret message is embed in to high frequency co-efficients. The low frequency co-efficients are preserved unaltered for improving image quality[3].

ADVANTAGES

- Providing a fair amount of security
- Frequency domain is more easy to handle than spatial domain
- It is difficult to retrieve the message for a third party

DISADVANTAGES

- Complex compared to DCT
- In terms of remote authentication security can be improved by more decomposition and by applying more conditions to hiding strategy

3.DCT-DWT dual domain [4]

Both DCT and DWT are two efficient technologies for steganography. But as we discussed above there some disadvantages for both of these. So in some cases the orthogonality[3] of two domains are used for perform high performance. It is an approach for combined image authentication and colour image compression. In these type of domain it making use of both watermarking and data hiding framework. Orthogonality of different domains are used for designing multipurpose watermarking[4].Different domains are used for authentication , colour decomposition , and watermarking insertion. These kind of approaches are implemented as a DCT-DWT dual domain algorithm. It mainly employs 8x8 Discrete cosine transform(DCT) and Discrete wavelet transform (DWT) as dual domains.

Since the dual domain making the use of orthogonality of two domains it can achieve the advantages of both domains. The Discrete cosine transform (DCT) is mainly used for watermak generation by maping special domain to frequency domain while Discrete wavelet transform (DWT) is mainly used for embedding process. The embedding process in DWT is taking place in a frequency domain. It partitions the frequency domain in to four frequency bands and the high frequency bands are used for embedding while low frequency bands are preserved unchanged for retrieving image quality.

ADVANTAGES

- We can make the use of orthogonality of two domains say DCT and DWT
- Each domain is in charge of different process so complexity in one domain decreases

DISADVANTAGES

- Inconvenience of using two domains
- We must have a thorough knowledge of each domain

4.DWT-IWT [5]

IWT stands for Integer wavelet transform. Wavelet domain hide data in regions that human visual system cannot see, like high frequency bands (HL, LH and HH). Hiding data in those regions which increases the robustness and also provide fair visual quality. Integer wavelet transform maps integer to integer ie ,one integer data set into another. In DWT, the wavelet filters uses floating point coefficients so hiding data must be more careful. Any truncations of the floating point value causes the loss of the secret information may also lead to the failure of the data hiding system. To avoid problems of floating point precision, in IWT it maps integer dataset to only another integer data set.

ADVANTAGES

The main advantages described below,

- Make the use of orthogonality of two domains
- IWT can ensure lossless compression

DISADVANTAGES

- Inconvenience of using two domains
- While using two domains it must be complicated

5.DCT-SVD [6]

DCT-SVD dual domain is mainly used digital rights management area. As we know when we upload an image mainly sensitive images like biometric signals it must have to be protected. Violation of digital right images are common so protection of copy rights of digital images must be strong enough so that no one can break it. To protect digital rights many techniques are used. Fingerprint technique is common. biometric features of finger print is used to generate the watermark. The most important minutia points are extracted from the fingerprint. Then the coordinates of these minutiae points are represented as matrix and utilizes as watermark. Then the embedding and extraction of watermark is done in DCT-SVD[6] domain.

DISADVANTAGE

- Not tested under lossless compression

IV. PROPOSED METHODOLOGY

Video conferences , online interviews , online tests , online id,ect are inevitable part of our day to day life. In these kind of of situations. Passwords ,pin numbers, identification information ,biometric signals any kind of information can be send over wireless network for remote authentication. Here the security of these kind of information must be ensure. Steganography is used to hide these kind of information before send over the wireless networks. There are many kind of steganography mechanisms as we discussed in previous session. All those technologies have advantages and disadvantages. But when we focusing on security, we have add some more conditions to the existing techniques. QSWT[1] (Qualified significant wavelet transform) is one of such technique which increases the level of security.

In this approach the security level of steganography is increased by adding an encryption module to the secret message and also some special conditions for selecting the region for hiding. Here we decompose the video object before hiding the secret message and arrange it correctly before sending .The modules are described below,

1.VIDEO OBJECT EXTRACTION

2.DECOMPOSITION AND REARRANGING OF VIDEO OBJECT

3.CHAOTIC ENCRYPTION

4.HIDING USING QSWT

5.REARRANGING OF VO

6.RECOVERING OF MESSAGE

1.VIDEO OBJECT EXTRACTION

Video object is the most important or prominent frame of a video with only semantically meaningful region. For example if we have a frame with the face of a man with a beautiful background, then the background is not semantically meaningful in that frame, only the face is meaningful. So a video frame extract the background from the face. It is done by using several morphological operations.

2. DECOMPOSITION AND REARRANGING OF VIDEO OBJECT

Here we decompose the video object in to several blocks by using block division of image in matlab. Then rearrange these blocks according to a given order. Then the secret message will hide in this shuffled video object. After hiding it will again shuffled to the right order then it will send it over to the receiver side.

3.CHAOTIC ENCRYPTION[1]

Chaotic encryption is used for encrypting the secret message so that the security of entire stego module will increase. It mainly has two parts. One is encryption keys generation and other one is encryption itself. Encryption key’s generation is done by a C-PRBG[1] (chaotic pseudo random bit generator).PRBG is based on three chaotic system ie it generate keys from three independent chaotic orbits and then mix it.

The encryption mechanism avoids iterations and also maintaining high security standards. It combines three chaotic ciphers by using s-box mechanism. It first perform the s-box operation using plain text and then xor it with the key. Then this result will undergo s-box operation again. Then the final product will give the cipher text. This method provide high security.

4.HIDING USING QSWT

QSWT stands for qualified significant wavelet transform. Qswt is a set of conditions for improving the regions for hiding the secret data. Here QSWT[1] utilizes the DWT[2] algorithm. We can also use IWT for improving the performance. First the QSWT take the input frame and partition it into four frequency bands say HH,HL,LH,LL by using DWT in first level. Then select a low frequency band either LL or LH to perform next level of decomposition. In next level the LH is again decomposed into LL1,LH1,HL1,HH1.In this level also the low frequency bands are selected and we can further decompose. The low frequency band contain the original image so when decomposing the quality of image is preserved. Then we select the highest energy pair among LH2LH3,HL2HL3,HH2HH3.In the existing work we hide the message in highest energy pair which resulting the recovering fingerprint image is not clear for matching. So here we hide the message only in one highest energy band not in the pair which resulting the high resolution image of the fingerprint at the receiver side. Although we are hide in only one band not the pair, we are not compromising the security level. So that we added an additional module which decompose and shuffle the blocks of the video object before hiding. After this the significant co-efficient selection[1] is taking place.

ALGORITHM

1.Start procedure QSWT

2.Define I,S,L(I=input frame ,S=sub band selection,

L=subband level)

3.Defining T1,T2 (threshold values)

4.Apply DWT according to different levels

5.check whether the subband is innode

6.check whether it is greater than T1

7.repeat till T2

ADVANTAGES OF QSWT

- Efficient algorithm which facilitate robust hiding
- The information that is embedded is difficult to detect by human visual system
- Best known technology for retrieval of hidden message

5.REARRANGING OF VO

After the hiding of encrypted biometric signal in to the shuffled VO ,the VO will reshuffle in to the original order. Only after this reshuffling , the stego object become ready to send. The ready to send stego object will send to the receiver side over wireless network. If a third party is happened to get the image he cannot detect any secret message. Even if he try to detect the message it does not going to work until he correctly shuffle the stego object. So we can say the increase of the security level become high compared to the previous works.

6.RECOVERY OF MESSAGE

After getting the stego object at the receiver side , the receiver will shuffle the image in the correct order(only the sender and receiver knows the shuffling order).Then IDWT will apply on the shuffled image for recovering the encrypted biometric signal and then decrypt it using the primitive values of the chaotic encryption.

V. SIMULATION/EXPERIMENTAL RESULTS

The system is implemented by using the tool Matlab2014 and the results are promising.The main problem of previous work was the quality of the output image which is very low and cannot perform the fingerprint matching. Since here we hiding the message in only one band not the pair, we get a better quality image output. In terms of security and robustness the proposed work gives a better result compared to the previous work.

Image Quality

The image quality of stego object and the extracted output(Decrypted biometric signal) are determined in terms of PSNR and MSE values. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to comparing the squared error between the original image and the reconstructed image. PSNR and MSE are inversely proposed. So if PSNR value is high then the quality of image is also high.

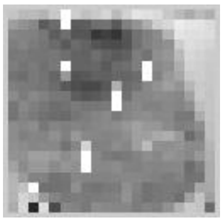

Fig 5.1 Existing system output

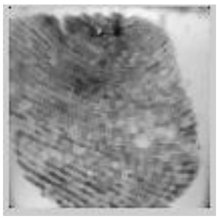

Fig 5.2 Proposed system output

To compute the PSNR, we have to first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

M and *N* are the number of rows and columns in the input images, respectively. Now PSNR will be computed using the following equation:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

R is the maximum fluctuation in the input image data type. Ie, *R* is 1, if there is a double-precision floating-point data type. *R* is 255 If there is an 8-bit unsigned integer data type, etc.

Given below two graphs showing the PSNR value of the existing and proposed work (Fig.5.3) and MSE value of output image of the existing and proposed system (Fig.5.4).

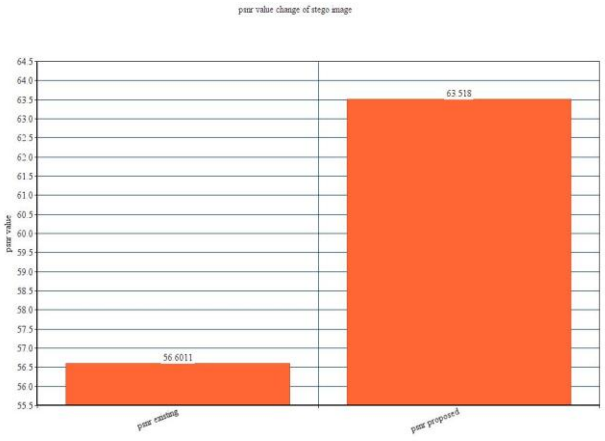

Fig.5.3 Psnr value change of stego object

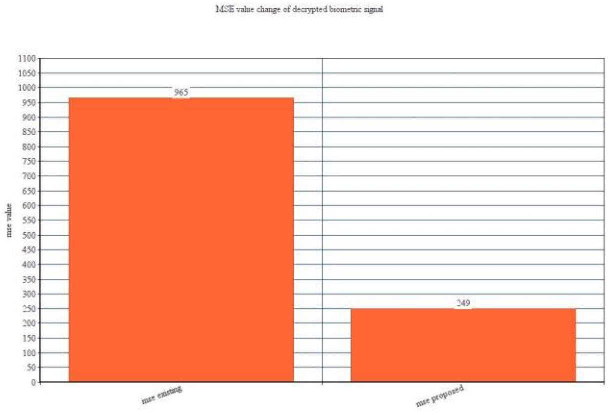

Fig.5.4 MSE value change of decrypted biometric signal

VI. CONCLUSION

Video conferencing, online interviews, online identification process etc are inevitable part of our educational, society life which require remote authentication. Steganography provide security for secret message which may be pass words, numbers ,biometric signals etc. In this paper we propose a new system which is mainly used for remote authentication. The system is seems to be providing more clear image of the biometric signal at the time of recovering of message and also the security level of the stego object is seems to be higher than the existing system. Although we are focusing on the security , the complexity of the system is relatively high. In future we can work on this problem.

VII. FUTURE SCOPES

Although the proposed system providing a high level of security , the complexity of the system is a bit tiring. Also before starting the process there are some initial conditions needed such as , the video object , the password for shuffling the video object should be shared before the system starts. If we use only one video object and one password it may be threatening. So more video objects and passwords need to be shared which is a kind of inconvenience. These limitations and open issues, which should be further, investigated in future research.

REFERENCES

[1] KlimisNtalianis, and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks ," *in Proceedings of the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING* , FEBRUARY 2016.

[2] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DC Tand Compression Techniques on Raw Images" *IEEE Trans. Image Process.*, vol. 13, no. 9, pp. 1200–1212, Sep. 2004.

[3] P.-Y. Chen and H.-J. Lin, "A DWT based approach for image steganography,"*Int. J. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 275290, 2006.

[4] S. Areepongsa, Y. F. Syed, N. Kaewkamnerd, and K. R. Rao, "Steganography for a low bit-rate wavelet based image coder," *in Proc. IEEE Int. Conf. Image Process.*, vol. 1. Sep. 2000, pp. 597600.

[5] D. Kundur, Y. Zhao, and P. Campisi, "A stenographic framework for dual authentication and compression of high resolution imagery," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 2. May 2004, pp. 14.

[6] 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. 1724, Mar. 2013.