DATA TRANSFER USING VISUAL CRYPTOGRAPHY

[1]M. Satish kumar ,[2]Dr.V.Sangeeta,[3]B.Mahesh, [4]R.Krishna Rao, [5] S.Radhika
[1]Assistant professor,[2] professor, [3]Assistant professor, [4] Assistant professor, [5]Associate Professor
[1]Computer science And Engineering
Raghu Institute of Technology,Visakahapatnam,India.

Abstract: Now days the secured data transmission and data integrity are the two challenging areas for research. This work describes the concept of data hiding using visual cryptography. Data transferring will secure and create need of improvement when transfer data every time. Visual cryptography with boundary steganography represents GUI (Graphical User Interface) for security improvement. Then by using invisible watermarking technique hide those two shares into the selected frames and the image is hided and finally all the frames are again converted into video using the FFMPEG tool and video is encrypted using the base64 encoder with asymmetric cryptographic technique .In the receiver system, the video was decrypted and split into frames and extracting the shares and data by selecting the frames which was watermarked.

Keywords: boundary, stego image, secrete, Data hiding, visual cryptography, base64 encoder with asymmetric cryptography.

I. INTRODUCTION

In present days, with the development of computer technology and Internet technology, multimedia data are used more and more widely, such as images, videos or audios. In order to keep secure, some sensitive videos need to be protected before transmission. For this data hiding technique is used along with visual cryptography. Data hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

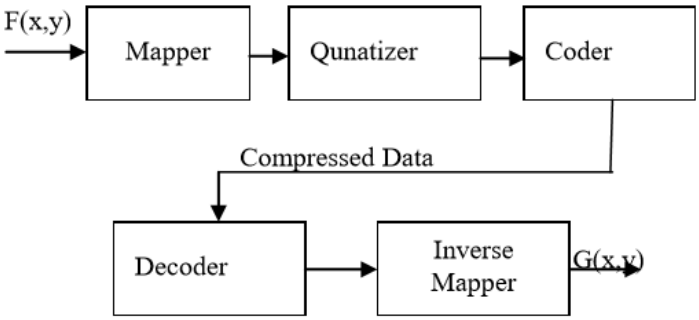
The advantage of steganography over cryptography is the practice of protecting the contents of a message alone, while steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. In this paper, we propose a data hiding technique to embed a secret message along with the secret image in a multiple number of frames. Here encoding and decoding is done with the help of asymmetric cryptography technique along with the base64 encoder. Base64 is commonly used in a number of applications, including email via MIME, and storing complex data in XML. The paper is organized as follows: Section2 describes the techniques used, Section3 summarizes other works related to data hiding with other encryption algorithms, Section 4 describes the proposed system model we consider, and finally Section 5 draws the conclusion.

II. VISUAL SHARING MECHANISM

The visual secret sharing (VSS) scheme, is a type of secret sharing scheme which can split the secret information into n shares and recover them by superimposing the shares. In VSS, the secret to be hidden is a black and white image and each share is comprised of groups of black and white sub pixels used to recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque so that superimposing shares can result in recovering the secret image. An advantage of VSS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations.

A. Image compression Techniques

Image compression systems are composed of two distinct structural blocks: an encoder and a decoder. As shown in the fig 1, the encoder is responsible for reducing the coding, inter pixel and psycho visual redundancies of input image. In first stage, the mapper transforms the input image into a format designed to reduce inter pixel redundancies. The second stage, qunatizer block reduces the accuracy of mapper's output in accordance with a predefined criterion. In third and final stage, a symbol decoder creates a code for quantizer output and maps the output in accordance with the code. These blocks perform, in reverse order, the inverse operations of the encoder's symbol coder and mapper block. As quantization is irreversible, an inverse quantization is not included.



B.

C. Fig.1 Compression System

When the data is embedded into the image then the required memory is created into the covering media. But if some additional data is required, it is embedded into image then the process of image compression is done. When it is desired to transmit repeated data over bandwidth- constrained channel, it is important to first compress the data and then encode it. i.e., first encoding and then compressing. Mark Johnson and et.al has examined the possibility of first encrypting a data and then compressing it, such that the compressor does not have knowledge of the key for encryption. The encrypted data can be compacted using dispersed source coding ethics, as the key will be available at the decoder.

B. Data Hiding Key

This key is present at the data hiding center as well as receiver side the data hider can embed some auxiliary data into the encrypted image according to the data hiding key. The receiver may be the content owner himself or can be unauthorized party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to encryption key.

C. Watermark Embedding

Since the [2] encryption algorithm is with additive privacy homomorphism property, any robust additive watermarking scheme can be used. Use of spread spectrum technique for this purpose. For watermarking, the cipheredbytes from the less significant bit planes of the middle resolutions were considered, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent. Also, the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, modifying which leads to loss of quality. The impact on quality of watermarking in the compressed-encrypted domain was studied. It was also experienced that how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much.

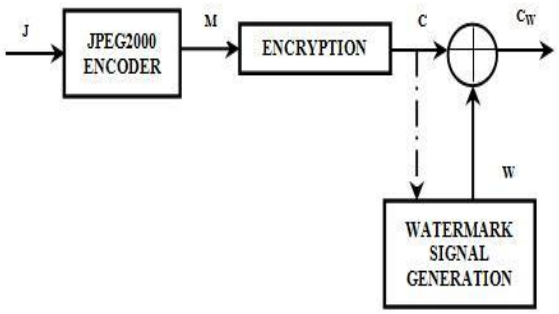


FIGURE 2 – ARCHITECTURE FOR JPG CONVERTER

III. PROPOSED SYSTEM

In this proposed system when we want to transfer any text data or a visual data from source to destination. We need to hide the data inside the video after splitting it into different number of frames. The secret image is also used in order to hide the data so that the safe transmission of data is possible which provides more security to the data. A [1] Visual Cryptography scheme is needed to split the image into shares. If the attacker attacks the image he can able to see only the secret image not the shares. Thus to improve

the safe transmission over the network we proposed this data hiding using multiple frames. In [8], a robust watermarking algorithm is proposed to embed watermark into compressed and encrypted JPEG2000 images.

A. Frame Selection

Select the video file to hide the Secret image and Data. By using the FFMPEG tool, Video was split into 3 different formats. First the video will divide into audio and video separately. Then the video part will be converting into n number of frames. In future these frames are used to hide the image and the data.

B. Data hiding using Visual Cryptography

We are selecting any two frames from n number of frames. Selecting the Secret image and converting this image into Grey scale image and further converted into Binary image. By using the Visual Cryptography scheme, the binary image is split up into two shares. To hide data into the share, the data is encrypted using Paillier Cryptosystem [9] and by using the Steganography technique the cipher text is embedded into the two shares. The Invisible watermarking scheme is used to hide two shares into the selected frames and after the image is hided, then all frames are converted into video and mix up with audio and finally video was encrypted using the Base 64 Encoder.

The paper is organized as follows: Section2 describes the techniques used, Section3 summarizes other works related to data hiding with other encryption algorithms is reported in [3]-[7], Section 4 describes the proposed system model we consider, and finally Section 5 draws the conclusion.

IV. CONCLUSION

In this paper we have proposed the data hiding technique with the help of multiple frames for the safer transmission of data over the network. A visual cryptography technique along with the steganography technique provides more security. A hierarchial encryption is used with the paillier cryptosystem in [2] will encrypt the data. A ciphertext is also inserted inside the binary image so that any attacker tries to hack will able to see only the secret image not the share and the data.

V. ACKNOWLEDGMENT

I would like to thanks my project guide Prof. K. Naga lakshmi (Computer Science & Engineering) continuous guidance and motivation helped me to achieve greater heights.

REFERENCES

1. E. R. Verheul, H. C. A. Van Tilborg,"Constructions and properties of k out of n visual secret sharing schemes", Designs, Codes, Cryptog, Vol. 11, No. 2, pp. 179–196, 1997
2. L.N.Pandey and Neeraj Shukla, "Visual cryptography schemes using compressed random shares," in Proc. IJARCSMS Int. Conf. Sep 2013.
3. P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking," in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.
4. W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.
5. X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
6. W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process.Lett., vol. 19, no. 4, pp. 199– 202, Apr. 2012.
7. X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2,pp. 826–832, Apr. 2012.
8. K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.
9. C.Wolf,S.Lucks,P P.W.Yau."Publicly Verifiable,Secret Sharing from Paillier's cryptosystem" IEEE Trans. Inf. (Eds.): WEWoRC2005,LNIP-74,pp.98–108,2005
10. A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703–716, Jun.201