A SECURE TEXT TRANSMISSION USING VIDEO CRYPTOGRAPHY & HUFFMAN CODING

Ms.Shilpa Verma[1], Mr. Omveer singh[2], Ms. Madhavi Brijwasi[3]

[1]*Department of Electronics & Communication engineering, Rajasthan Technical University, Kota (Raj.)*

[2]*Department of Computer Science & engineering, CGI, Bharatpur (Raj.)*

[3]*Department of Computer Science & engineering, CGI, Bharatpur (Raj.)* .

Abstract: The availability of versatile multimedia processing software and the far-reaching coverage of the interconnected networks have facilitated flawless copying, manipulations and distribution of the digital multimedia (digital video, audio, text, and images). The ever-advancing storage and retrieval technologies have also smoothed the way for large-scale multimedia database applications. However, abuses of these facilities and technologies pose pressing threats to multimedia security management in general, and multimedia copyright protection and content integrity verification in particular. Although cryptography has a long history of application to information and multimedia security, the undesirable characteristic of providing no protection to the media once decrypted has limited the feasibility of its widespread use. Image and video are the two most basic forms of transmitting information. With the help of Image and video encryption methods any particular set of images or videos can be transmitted without worrying about security. In the proposed research the video is distributed into the photo frames using a matlab code and all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. In the proposed work for each frame two pixels situated at the top left and the bottom right corner are modified so as to insert text in each image. After the completion of the pixel value changing all the images is placed in a sequential manner and then all the frames are cascaded for generation of the original video file with encryption. This new video is almost similar to the original video file with no changes visible to the naked eye.

Keywords: Video Encryption, Lossless Watermarking, Pixel Mapping, Stenography, Huffman coding.

I. INTRODUCTION

The objective of an information system security programme is to protect an organization s information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level. Security, integrity, non-repudiation, confidentiality, and authentication services are the most important factors in information security. While information security plays an important role in protecting the data and assets of an organization, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organizations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and business. In the advent of greater demand in digital signal transmission in recent time, the problem of huge losses from illegal data access has become a burning issue. Accordingly, the data security has become a critical and imperative issue in multimedia data transmission applications. In order to protect valuable information from undesirable users or against illegal reproduction and modifications, various types of securities are needed [1]. These security techniques are cryptography, steganography, combination of cryptography and steganography etc.

Any video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. Generally the frame rate is 25 so we can say that 25 frames are captured within one second time. For the efficient and successful implementation of this particular algorithm there is a requirement that the video needs to be segmented. For a particular case if we suppose that the video is of 5 minutes duration than this video majorly contains 7500 frames in it. These frames are vital building block for the video as well as for video encryption process. We can insert and send the text along with the frame by using various available watermarking techniques. There are various different watermarking techniques available like visual watermarking, discrete cosine transform, discrete Fourier transform and lossless watermarking method. All

the watermarking techniques recently available have certain drawbacks and also these methods are a little bit time consuming. Also the watermarking techniques can be modified using more advanced techniques for image processing. To get over the drawbacks of the watermarking techniques stenography method can be used for the encryption of the video files. Stenography is mainly useful in terms of efficient and accurate data processing for the case of the real time applications. In the proposed work also the stenography technique can be generated by using a pixel mapping algorithm. Also the stenography technique is faster and efficient in terms of time required for marking the particular set of images.

II.Cryptography

Cryptography is an art of protecting the information by transforming it into an unreadable and untraceable format known as cipher text. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is a science which is used from thousands of years. It concerns about the encryption as well as decryption of secret data in such a way that valuable information will remain safe from unauthorized users. Cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the **key.** The concept of a key is analogous to the combination for a combination lock. Although the concept of a combination lock is well known you can t open a combination lock easily without knowing the combination [2].

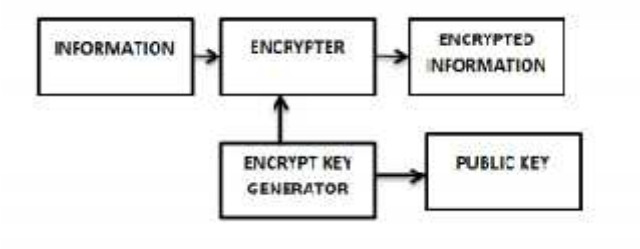

Fig 1:cryptography Encryptor

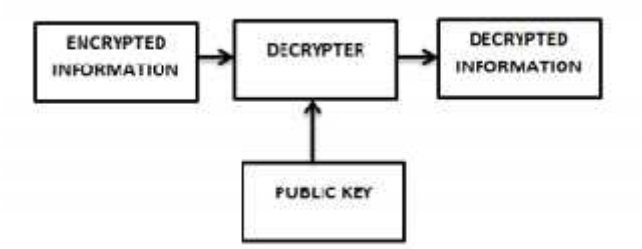

Fig 2:cryptography Decryptor

III. IMPLIMENTATION

A. Architecture of Video Cryptography

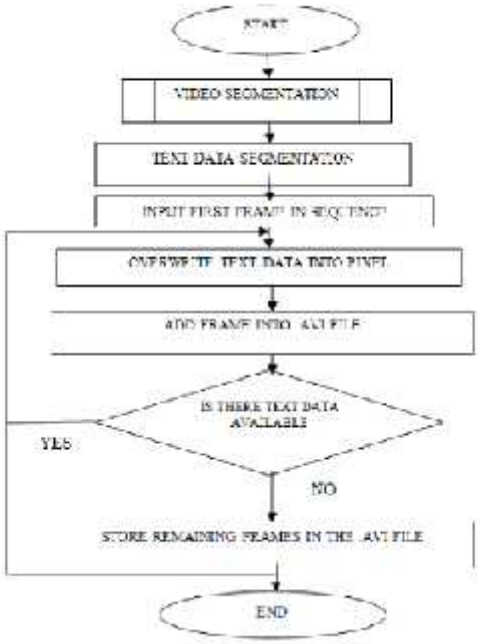

Fig. 3. Architecture of video cryptography system

Figure 3 describes the flowchart showing the sequence of steps to be executed for generating the encrypted video file for secured text data transmission. The algorithm is briefly described in terms of flowchart for the better understanding of the whole process. The complete algorithm is coded in a Matlab code showing the detailed process involved in the video encryption and the text insertion in the video file for secured transmission. As shown in the algorithm in figure 1 the complete video is segmented into number of images using a small Matlab code module and after the processing of the video by the Matlab code module the video gets divided into different frames of same size. Then the text string which is to be inserted among the images is partitioned into the group of two bits each. As we need to

modify only two pixels per image so we divide the text data into the group of two bits. Each character in the text data can be represented by a specific ASCI value so each of the character occupies 1 byte or 8 bits in an image. In this particular algorithm each of the image has to be modified by two pixel value and that also only the last two bits so each of the character in the text data to be inserted is represented by its ASCI value in line. After this each of the characters represented into the group of 8 bits is subdivided into the groups of 2 bits only. So now we have four groups for each of the character in the text data to be inserted into the images. In this algorithm to represent one particular character we require four pixels to store one particular character. As per the grassman law importance of three basic colors which are red, blue and green are different. As per grassman law the importance of the green layer is the most because it contains 59% weightage to generate any color in a particular pixel as per the requirement. Due to this in this particular algorithm only the value of the red and the blue layers are changed for processing the image so as to retain the original shade in the frame. The green layer in each of the images is unchanged. Only the blue and red layers pixels are modified in each of the image frames. Now we have frames as well as very well distributed text data available so the next step to be followed is to encode or map the text data into the pixels of individual frames till the end of the text data. In the proposed work we are going to store one character into one frame so there is a requirement of n number of frames for storing n number of characters in the text data. For a particular image frame by modifying only two pixels at top and bottom of the image file does not make any significant changes in the visual effects of the frame so

they are not visible to the human eye.

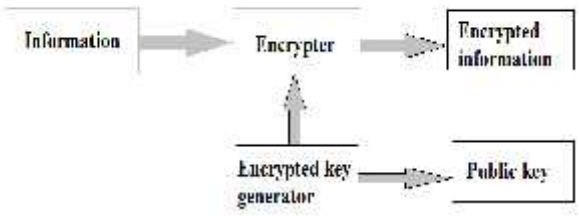

Fig 4:Encryptor

IV .Huffman Coding

Huffman coding algorithm was developed by David Huffman in 1951. Huffman coding is based on the frequency of occurance of a data item (pixel in images). The principle is to use a lower number of bits to encode the data that occurs more frequently. Codes are stored in a ***Code Book*** which may be constructed for each image or a set of images. In all cases the 8 Code book plus encoded data must be transmitted to enable decoding. Huffman coding is an entropy encoding algorithm used for lossless data compression. In this algorithm fixed length codes are replaced by variable length codes. When using variable-length code words, it is desirable to create a prefix code, avoiding the need for a separator to determine codeword boundaries. Huffman Coding uses such prefix code.

Huffman procedure works as follow:

1. Symbols with a high frequency are expressed using shorter encodings than symbols which occur less frequently.
2. The two symbols that occur least frequently will have the same length.

The Huffman algorithm uses the greedy approach i.e. at each step the algorithm chooses the best available option. A binary tree is built up from the bottom up.

There are basically two concepts in Huffman coding

1. Huffman Encoding
2. Huffman Decoding

Image compression is followed by encryption is applied on colour and grayscale image of different size and type. Here compression is performed by Huffman lossless coding algorithm which is depending on contents of data. For resultant compressed data is secured by encryption algorithm. The schematic block diagram of this proposed approach is given in Fig

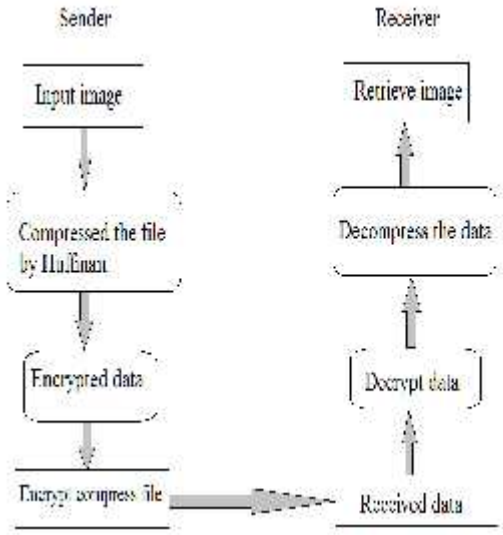

Fig 5: The schematic block diagram of proposed approach

V. RESULTS AND ANALYSIS

The figure 6.1Shows how we transfer text in a video

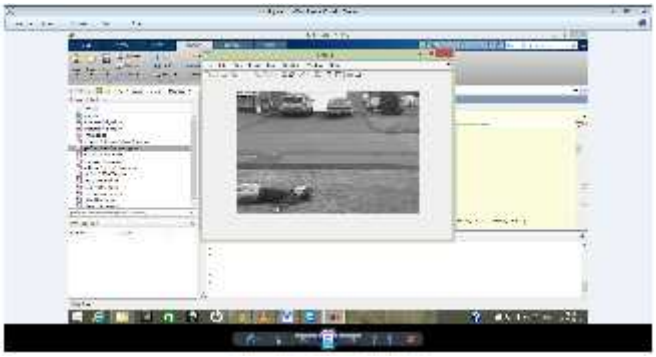

Fig. 5.1Transfer Text in a video

The figure 5.2 shows how we decrypt text from video enter the password

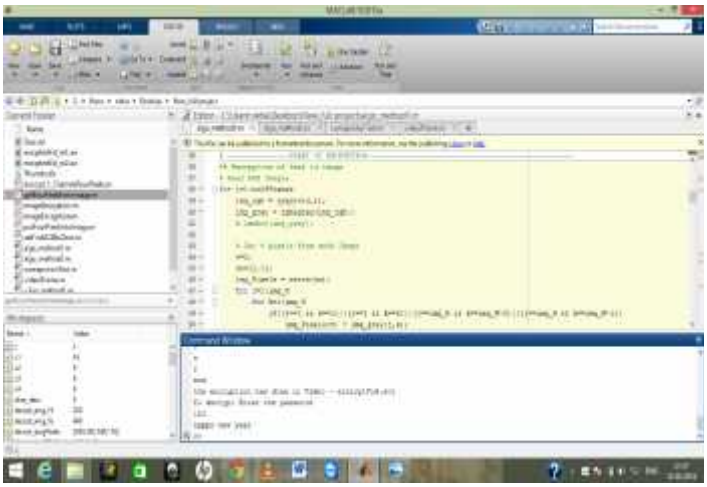

Fig 5.2 Decrypt Text from video using Password

The figure 5.3 shows How we decrypt the text and password from a video file

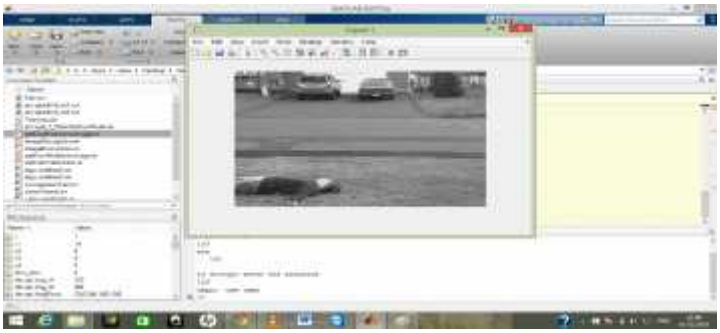

Fig 5.3 Decrypt Text using Password

The figure 5.4 shows the comparision of above two programs

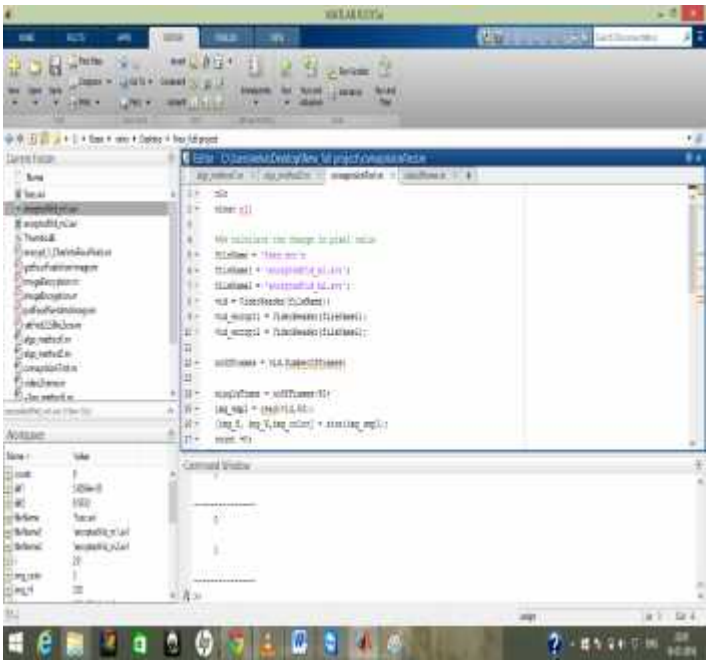

Fig 5.4 Comparision of Two Methods

VI . CONCLUSION and Future Work

In this thesis, we proposed a Secure text Transmission Using Video Cryptography. Here we use Encryption with The Password to transmit the video.

Security has become an important issue over time for large sized data. The main goal of this thesis is to find out a way of making data or messages highly secured and smaller in size than the original. To achieve this aim, it uses an existing most effective Huffman Compression Technique on data (so that it can be turned into a small sized file), with a newly developed Block of video cryptography (to make it secure). Two Private keys have been used which are known to both sender and receiver but are secret from the outside world, that is why known as Secret Key Cryptography. Whole system fulfils the goals of Cryptography and is simple but doesn t leave behind the security issues. It is not vulnerable to Brute-force attack due to large key domain.

One of the important features of the proposed work is it plays a vital role in transmitting the information mapped on an either image or a video file very effectively and efficiently. The information underlying the image or a video is not visible to the naked eye. Only the person having the private key and the rule list can identify and decode the original information into its original form. This method simplifies the task of securing the vital information from the misuse and protects it from the unwanted user.

With the use of the cryptography and stegnography combination the information security can be increased.
In future we must include this features in to audio file and other format of multimedia also.
As we know that multimedia techniques are very popular now a days so if the security features are added in to the multimedia technique then its better.

REFERENCES

[1] Anil Kumar, M. K. Ghose Information Security using Genetic Algorithm and Chaos All India Council of Technical Education (Government of India) vide their office order: F.No:8023/BOR/RID/RPS- 236/2008-09.

[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa An Overview of Video Encryption Techniques International Journal of Computer Theory and Engineering, Vol. 2, 1793-8201. 1 February, 2010.

[3] Pushpa R. Suri and MadhuGoel Ternary Tree and Memory-Efficient Huffman Decoding Algorithm IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-0814

[4] Mamta Sharma Compression Using Huffman Coding IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010.

[5] Nigam Sangwan Text Encryption with Huffman Compression International Journal of Computer Applications (0975 8887) Volume 54 No.6, September 2012.

[6]Yanqun Zhang, *Digital Watermarking Technology: A Review* 2009 ETP International Conference on Future Computer and Communication page- 250-252.

[7]Niu X.M., Lu Z.M., and Ho S.H. Digital watermarking of still images with gray-level watermark, IEEE Trans. on Consumer Electronics 46(1) (2000). p. 137-144.

[8]I. J. Cox, et al, "Digital watermarking and Steganography" (Second Edition), Morgan Kaufmann, 2008.

[9]Yanqun Zhang, *Digital Watermarking Technology: A Review* 2009 ETP International Conference on Future Computer and Communication page- 250-252.

[10]Yiwei Wang, John F. Doherty, Robert E. Van Dyck, *A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images* IEEE Transactions on Image Processing, Vol.11, NO.2 (February 2002) page 77-86.

[11]Fei C., Kundur D., and Kwong R.H. Analysis and Design of secure watermark-based authentication systems, IEEE Trans. on Information Forensics and Security **1** (1) (2006). p. 43-55.

[12]Barni M., Bartolini F., Rosa A.D. and Piva A. Capacity of full frame DCT image watermarks, IEEE Trans. On Image Processing (8) (2000). p. 1450-1455.

[13]Lu C.S. and Liao H.Y.M. Multipurpose Watermarking for image authentication and Protection, IEEE Trans. on Image Processing (10) (2001) p. 1579-1592.

[14]A. M. Eskicioglu, J. Town and E. J. Delp, Security of Digital Entertainment Content from Creation to Consumption, *Signal Processing: Image Communication, Special Issue on Image Security*, 18(4), pp. 237-262, April 2003.

[15]S.P.Mohanti Digital Watermarking : A Tutorial Review Report IISC Banglore,1999.

[16]M. S. Hsieh, D. C. Tseng, and Y. H. Huang, Hiding Digital Watermarks using Multiresolution Wavelet Transform, IEEE Trans. on Industrial Electronics 48 (2006), no. 5, 875 882.

[17]S. Rawat and B. Raman, A New Robust Watermarking Scheme For Color Images , 2010 IEEE 2nd International Advance Computing Conference, pp. 206-209, 2010.

[18]A. Nikolaidis and I. Pitas, *Region-based Image Watermarking* IEEE Transactions on Image Processing, VOL.10, NO.11 (2001) page 1726-1740.

[19]D. S. Taubman, JPEG2000: Standard for Interactive Imaging". *Proceedings of the IEEE*, vol. 90, no. 8, pp. 1336-1357, August 2002.

[20]F. Fang and S. Tan, A Robust Digital Watermarking Technique with Improved Performance under JPEG Compression, Proc. SPIE, Applications of Digital Image Processing, September 2006.

[21]A. Skodras, C. Christopoulos, and T. Ebrahimi,The JPEG 2000 Still Image Compression Standard". *IEEE Signal Processing Magazine*, vol. 18, no. 5, pp. 36-58, September 2001.

[22]D. S. Taubman and M. W. Marcellin, *JPEG 2000: Image Compression Fundamentals, Standards and Practice.* Norwell, MA: Kluwer, 2002.

[23] N. Yoshio, T. Yousuke, S. Shigeyuki, Z. Liang, and Y. Hideo, A study on video scrambling considering inter-frame prediction, vol. 105;NO.500(IE2005 127-185), 2006.

[24] NarendraK.pareek, vinodpatidar, krishanK.sud, Diffusion-subtitution based gray image encryption scheme Digital signal processing 894901,2013.

[25] Bibhudendra Acharya1, Saroj Kumar Panigrahy2, Sarat Kumar Patra3, and Ganapati Panda3, Image encryption using advanced hill cipher algorithm , ACEEE International Journal on Signal and Image Processing Vol 1, No. 1,37-41, Jan 2010.

[26] AllamMousa (1) and Ahmad Hamad, Evaluvation of the RC4 algorithm for data encryption , International

Journal of Computer Science & Application Vol. 3, No.2,44-56, June 2006.

[27] Ali B.Y.Mohammad, J.Aman, Image encryption using block based transformation", IAENG.Int.J.Comput.Sci.15-23,2008.

[28] MarwaAbd El-Wahed, SalehMesbah, and Amin Shoukr, Efficiency and Security of some image encryption algorithms , Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008,London, U.K. 978-988, July 2 - 4,2008.

[29] Guodong Ye, Image scrambling encryption algorithm of pixel bit based on chaos map ,PatternRecognit, Lett.31,pp.347-354,2011

[30] Jin-mei Liu, QiangQu,:cryptanalysis of a subtitutio-diffusion based image cipher using chaotic standard and logistic maps ,Third International Symposium on Information Processing, ,pp.67-69, 2011.

[31] Hongxing Yao, Meng Li, An approach of image hiding and encryption based on a new hyperchaotic system:,Int. J. Nonlinear Sci.7,pp.37938,2009..

[32] IsmetOzturk, Ibrahim Sogukpinar, Analysis and comparison of image encryption algorithm , Trans. Eng. Comput. Technol.,pp.38-42,2009

[33] A.Syalim,T.Nishid, and K.Sakurai, Preserving integrity and confidentiality of a directed acyclic graph model of provenance, Proc. Working Conf. Data and Applications Security and Privacy,pp.311-318,2010.

[34] E. Choo, L. Jehyun, L. Heejo, and N. Giwon. SRMT: A lightweight encryption scheme for secure real-time multimedia transmission. In Multimedia and Ubiquitous Engineering, pages 60–65, 2007

[35]T. Uehara and R. Safavi-Naini. Recovering DC coefficients in block-based DCT. In Proc. of IEEE Transactions on Image Processing, volume II, pages 3592 3596, 2012

[36] K. Ahsan, and D. Kundur, Practical Internet Steganography: Data Hiding in IP found online at <http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf>

[37] R.J. Anderson and F.A.P. Petitcolas, On the Limits of Steganography, J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474 481

[38] A. Skodras, C. Christopoulos, and T. Ebrahimi,The JPEG 2000 Still Image Compression Standard". *IEEE Signal Processing Magazine*, vol. 18, no. 5, pp. 36-58, September 2011.