ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Hybrid Technique for Hiding Data Inside Video Using Combined Cryptography and Steganography

Divya Prasannan [1], Renjith Thomas [2]

P.G. Student, Department of ECE, GISAT Engineering College, Payyapady, Kerala, India[1]

Assistant Professor, Department of ECE, GISAT Engineering College, Payyapady, Kerala, India[2]

Abstract: In this article, a hybrid technique for hiding data inside image using combined cryptography and steganography is proposed in which data is hidden inside an encoded video file. In the system, video file is separated into individual frames and encoded separately. Any one encoded frame is selected for hiding secret data. Before hiding, secret data is encrypted using chaos encryption which provides improved security compared to conventional techniques. Encrypted secret data is hided inside the encoded bit stream by comparing the bit values. An index value is created which is used for correctly decoding the hided secret data. The system provides good security and the video after recovering the secret data is similar to the original one. The quality of the video is analyzed using PSNR values and correlation values

KEYWORDS: Chaos encryption, video encoding, Index value

I. INTRODUCTION

In this digital world there is a need for transmitting our data in a secure way. Steganography and cryptography are the two commonly used techniques for making our data secure. Now a day's most of the information transfer is by using multimedia files. Traditional cryptographic techniques are not suitable for multimedia applications. Here comes the importance of Steganography which can be used for multimedia applications.

Steganography is an art of hiding secret data inside unremarkable places such as documents, images, videos etc so that eavesdropper's will not guess the existence of secret inside. Steganographic techniques mainly identify the redundant contents of the medium and replace it with the secret data bits without losing the integrity of the medium used. One of the simplest spatial domains embedding technique used in Steganography is the LSB technique. This method is based on removing the redundant bits and substituting that position with most significant bits of secret message

Cryptography converts data into cipher text which is unreadable to the unauthorized person. Cryptographic algorithms take plain text and key as input and convert plaintext to unreadable format called cipher text. It mainly applies some transformations on the plain text to produce the cipher text.

The work in this paper is divided in three stages. 1) Frame separation 2) Data hiding 3) Combining frames. . A video file is a collection of n number of frames. For hiding the secret data any one of the frame is selected and then encrypted data is hided in the frame. The video file is encoded using any of the encoding schemes frame by frame. From that any one of the encoded frames is selected for hiding our secret data. The hided frame is combined with other frames to get the stego video.

This paper is divided into four sections, first section is the introduction. Section II gives a brief idea about existing systems. The proposed data hiding technique is presented in section III. Finally, Analysis in session IV and conclusions are drawn in section V.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

II. LITERATURE REVIEW

In 'Application of image hiding in Mp4-video using Steganography technique' by S.Sangaeswari et.al [1] a hiding procedure for high resolution Mp4 videos is proposed. In this work Mp4 video frames are transformed using DCT and embed secret information in high order coefficients. For decoding inverse DCT is performed over the received stego video.

In 'Secure video data hiding' by Kumbhar Shraddha et.al [2] input video and secret data are encoded by using a security key and hide secret data inside video to get stego video. Decoding is done using the same secret key. DCT method is used for data hiding purpose.

In 'Secure data hiding technique using video Steganography and watermarking' by Shivani Khosla [3] a system with large hiding capacity and also limits the perceivable distortions that might occur while processing is proposed. In this work LSB technique is used for data hiding. It uses a secret password for improved security.

In 'An approach to hide data in video using steganography' by Deepak Kumar et.al[4] a new video steganographic algorithm using hash function technique is proposed. A double hash function is used to select pixel from row and column for purpose of hiding.

In 'Data hiding using video Steganography' by P.R.Deshmukh [5] a hash based LSB technique for video Steganography is proposed. Hash function is used to select the pixel position to hide the data. System is analyzed using PSNR and MSE values. The system obtained a PSNR of approximately 55% and MSE of 0.05.

In "A DWT Based Approach For Image Steganography" by Po-Yueh Chen [6] a frequency domain technique to hide data is proposed. In this, algorithm is divided into 2 modes and 5 cases. DWT of image is taken and message is embedded in the high frequency coefficients. Low frequency coefficients are kept as same to preserve the quality of image. Mathematical operations are performed on image before embedding. There operation make the message secret.

In "High Capacity And Security Steganography using discrete wavelet transform" by Manjunatha Reddy [7], discrete wavelet transform based Steganography is proposed with high capacity. In this, coefficients obtained from DWT of both cover image and data are combined to get the Stego image. In this system capacity and security increased by maintaining a good PSNR value.

In " A Novel Technique For Image Stegenography Based On DWT And Huffman Encoding" by Amitava Nag[8], proposed an image Steganography technique based on DWT. DWT of image is taken and date is coded using Huffman coding. Then each code of Huffman code is embedded in the DWT high frequency coefficients. Low frequency band is preserved to maintain the quality of the image. This algorithm also has a good capacity and a better PSNR value is obtained.

In "A Secure Color Image Steganography In Transform Domain" by Hemalatha S [9] a new scheme of hiding an image and key in the cover image was proposed. In this both DWT and IWT (integer wavelet transform) are used. High PSNR value is obtained for Stego image and cover image,that is no visual difference between them. In this paper secret image is in gray scale and cover image is a color image. To get confidentially a key is generated and the key is encrypted and using IWT encrypted key is hidden in cover image.

In "A High Secure And Robert Image Steganography Using Dual Wavelet Blending Model" by Prabakaran Ganesan [10] a gray secret image is hided in a gray cover image using DWT and IWT. Using Arnold transform secret image values are scrambled and then DWT/IWT is applied to both images. Blending is applied to the image. By using different combination of DWT/IWT high security and robustness is achieved.

III. PROPOSED SYSTEM

In the proposed technique of secret data hiding, both cryptography and Steganography are utilized to improve the security of secret data. In this technique a video file is used to hide the secret data. A video file is a collection of n number of frames. For hiding the secret data any one of the frame is selected and then encrypted data is hided in the frame using bit substitution technique. First the secret data is encrypted using chaotic encryption. Resulting sequence is converted to bit stream. The video file is encoded using any of the encoding schemes frame by frame. From that any of the encoded frames is selected for hiding our secret data. The hided frame is combined with other frames to get the stego video. The resulting video file will not be similar to the initial video file.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

The block diagram of the proposed system is shown in Fig.1. The system has three inputs. They are input video, secret data and secret key. The encoded video with hided data is given as output from the system. In the block diagram five processes are shown. They are separating video frames, encoding, and chaos encryption using key, data hiding and frame combining.

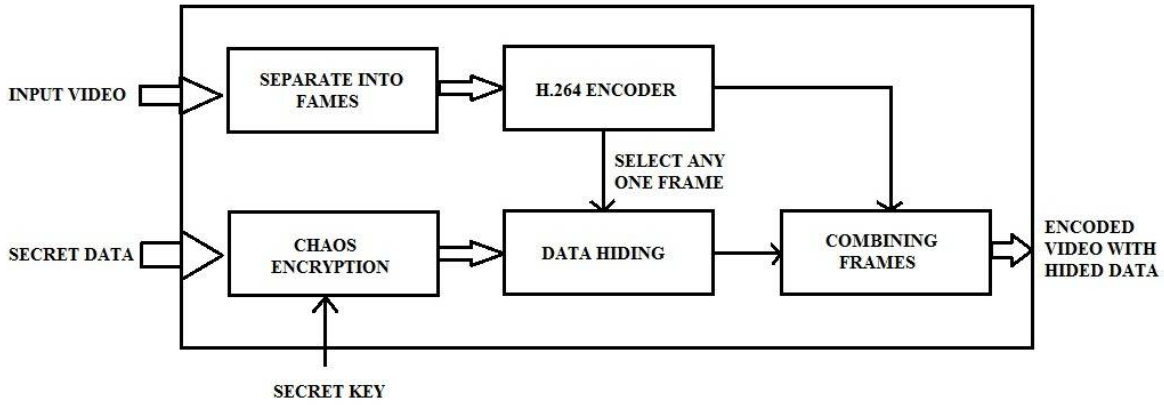

Fig.1 Block diagram of proposed system

In the block diagram first the input video is separated into frames and each frame is individually encoded using H.264 encoding. H.264 encoding is a commonly used encryption format which has mainly three processes. Initially the encoder makes a prediction about the current block based on the previously encoded blocks. This prediction is subtracted from the current block to get a residual. This residual is quantized and encoded using any of the variable length coding technique to get the encoded output. Using this encoder all frames are encoded and out of that one encoded frame is selected for data hiding.

Secret data to be hided is encrypted using chaos encryption. For chaos encryption, initially choose a key (r, x) input as the secret key. Map all symbol set (A, B, C…) to a range between 0 and 1. For e.g. .49<T<.51. Then choose first symbol to send (e.g. T) and iterate formula x = r*x*(1-x) 'n' times until x enters T space (.49<T<.51). Then number of iterations 'n' is send as coded version of symbol. Using this entire secret data is encrypted.

The encrypted secret data is hided inside the selected encoded frame. The process of hiding is shown in Fig.2. First matrix indicate the encrypted data bit stream, second matrix indicate the encoded frame's bit stream and third matrix indicate the bit stream after data hiding. For hiding purpose, both encrypted secret data bit stream and encoded frame bit stream are compared bit by bit. Based on the bit values a new bit stream is created instead of encoded bit stream.

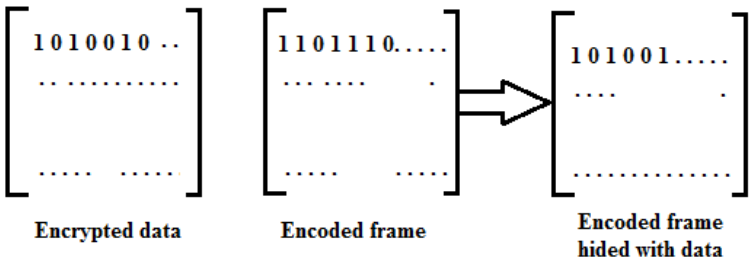

Fig.2 Secret data hiding

If both bits are one, we make an entry one in the new stream and mark 'E' in the index term. If (0, 1) then we make an entry 0 in the new bit stream and mark 'L' in the index term. If (1, 0), we make an entry 1 in the new bit stream and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

mark 'H' in the index term. Continuing like this entire bit stream is created. This bit stream is combined with the other encoded frames to get the encoded video file. This stego video is transmitted through the medium. During the hiding process an index term is created which is used at the time of extraction.
Extraction process is the reverse of hiding process which is shown in Fig 3. First matrix in figure indicates the encoded frame after data extraction, second matrix is the received bit stream and third matrix is the encrypted data extracted from received bit stream. Based on the index value data is extracted out.

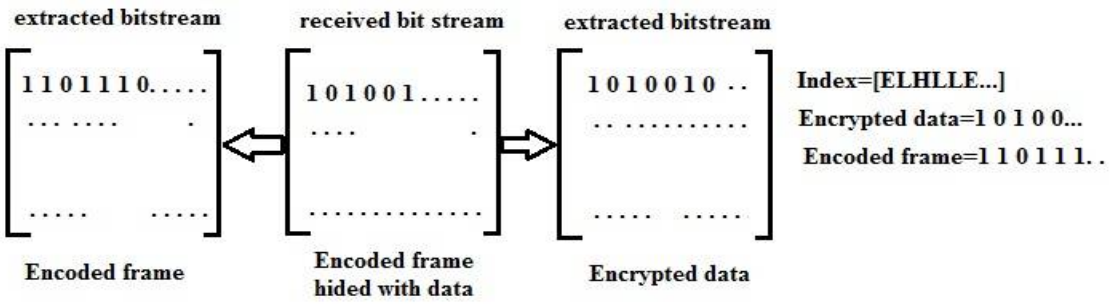

Fig.3 secret data extraction

Since we are hiding data inside any one of the frame, eavesdropper will not guess the existence of secret data inside that. Thus we can provide higher security to the secret data. Using this technique both video/audio file and a huge amount of data can be securely transmitted through insecure medium.

IV ANALYSIS

Some simulations and analysis are carried out to prove the efficiency of the proposed system. The work is simulated in MATLAB 2012. The system GUI working window is shown in Fig.4. Model created using GUI has two sessions, Transmitter session and Receiver session. Transmitter section carries out the encryption, compression and hiding. Receiver session carries out the decryption, extraction of secret data and analysis.

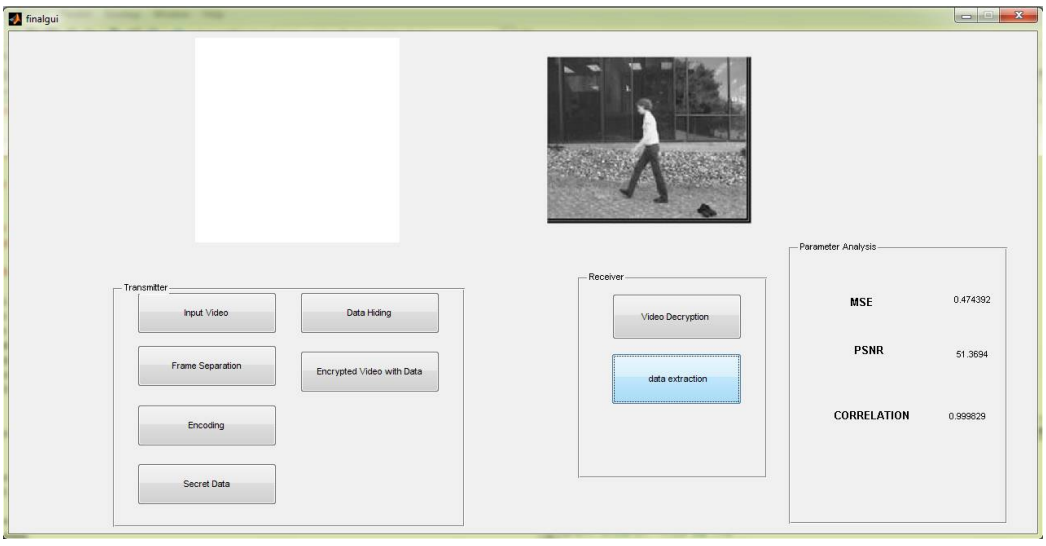

Fig.4 Proposed system implementation

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Efficiency of the proposed algorithm can be verified using two parameters, peak signal to noise ratio (PSNR) and correlation. The stego video formed is visually similar to that of input video and the retrieved video has only minute distortion from the original video. The hided secret data is extracted correctly without error.

By analyzing the proposed system the PSNR value obtained for the video is approximately 52%. The correlation obtained is 99%. The decrypted video is visually similar to the original one. Also the hided data is correctly decoded out from the frames.

V. CONCLUSION

In this paper a new technique for secure data communication is proposed. The technique use a combination of both cryptographic and steganographic techniques. A video file is used to hide the secret data. The encoded frames are selected for hiding the secret data. Chaos encrypted secret is hided inside video frame. By using this system we can obtain good security to video file and the secret data hided. The system obtained a high PSNR value and the secret data is extracted correctly.

REFERENCES

[1] Sangareswari.S., Aruna.V.,"Application of image hiding in mp4-video using steganography technique", International Journal of Electrical, Computing Engineering and Communication, Vol.1, Issue.2, pp.25-27, 2015.
[2] Kumbhar Shraddha, Rokade Varsha, Sukre Mayuri,"Secure Video Data Hiding", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 12, pp.736-738, 2014.
[3] Shivani Khosla, Paramjeet Kaur "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications ,Vol.95,Issue.20, pp.7-12, 2014 .
[4] Deepak Kumar Sharma1, AsthaGautam, "An Approach To Hide Data In Video Using Steganography", International Journal of Research in Engineering and Technology, Vol .3, Issue 4, pp.164-168, 2014.
[5] Deshmukh.P.R., Bhagyashri Rahangdale, "Data Hiding using Video Steganography", International Journal of Engineering Research & Technology, Vol.3,Issue 4, pp.856-860, 2014.
[6] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, Vol.4, Issue 3, pp.275-290, 2007.
[7] H.S.Manjunatha Reddy, Raja.K.B, "High capacity and security Steganography using discrete wavelet transform", International Journal of Computer Science and Security,Vol.3, Issue 6, pp.273-280, 2007.
[8] Amitava Nag, Sushanta Biswas, Debasree Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, Vol.4, Issue 6, pp.348-356, 2006.
[9] Hemalatha S, Dinesh Acharya, Renuka.A, Priya Kamath, "A secure color Image Steganography in transform domain", International Journal on Cryptography and Information Security, Vol.3, Issue 5, pp.567-570, 2005.
[10] Prabakaran Ganesan and R.Bhavani, "A high secure and robust Image Steganography using dual wavelet blending model", Journal of Computer Science,Vol.9, Issue.3, pp. 277-284, 2013.