Data Hiding Technique in Video Stegnography using BCH Codes in DWT Domain

Miss. Nehali Pawar[1] Prof. Kishor Pandyaji[2]
[1]M.E. Student [2]Associate Professor
[1,2]Department of Electronics Engineering
[1,2]PVPIT, Budhgaon, Maharashtra, India

Abstract— Stegnography is a method of hiding data in cover file which may be in the form of an image, audio or video. The video stegnography is one of the best method for secret data hiding that reduces the chance of secret message hacking. Data embedding is a process where secret message is embedded in video file. The video stegnography techniques are useful in high security requirements. This paper presents, the high capacity video stegnography based on BCH code in DWT domain is used for data hiding. This proposed system encoded the secret message by BCH encoder. The encoded message hides under the video in DWT domain. This proposed system basically divides in two parts namely data embedding and data extraction. In this paper data embedding process is discussed in detail and also the results of data embedding on the basis of parameters like visual quality, embedding payload. The paper also provides detailed information and results of data embedding process. The proposed video stegnography technique may give better result than the existing techniques.

Key words: Video Stegnography, Stego Video, Security, LSB Method, Hamming Code, BCH Code, Embedding Payload, Visual Quality, PSNR

I. INTRODUCTION

Video stegnography is an art of hiding data in video media. The secrete message may be text, image, audio, video. The best technique is to hide the secret data without reducing the quality of the cover video, so that it cannot be detected by naked eyes. The embedded video is known as the "stego" video which is sent to the receiver side by the sender. Block diagram of video stegnography is shown in fallowing diagram:

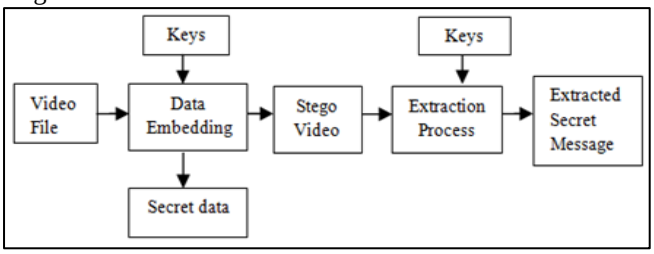

Fig. 1: Block Diagram of Video Stegnography

Video based stegnographic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, data are transformed to frequency components by using FFT, DCT and then embedded in some or all of the transformed coefficients. In spatial domain, the bits of data can be embedded in intensity pixels of the LSB positions of the video. Video stegnography used various types of algorithms for data encoding. Algorithms are based on LSB methods, error detecting and correcting codes etc. Efficiency of particular algorithm is decided by its performance parameters.

II. RELATED WORK

In 2009, Eltahir, L. M. Kaih, and B.B. Zaidan proposed a high rate video stegnography system based on least significant bit method. The idea of suggested method is by using 3-3-2 approach. This 3-3-2 approach actually uses least significant bits of RGB (Red, Green and Blue) in 24 bits image. The 3-3-2 approach is efficient because stego video is almost the same as the original video. The result was found to be good and the size of the data was substantial. It is about 33.3% from the size of image. [1]

In 2014, R. Shanthakumari and Dr. S. Mallinga presented a paper on Video Stegnography using LSB matching revisited algorithm. In their project they used a video file of AVI format as a cover file. This proposed method there was two problems which are low embedding rate and lack of security. LSBMR algorithm has a low replacement rate and hence the Mean Square Error (MSE) is low, as a result of which LSBMR is more secured than the LSB algorithm for data hiding.[2]

In 2013, Hemant Gupta, Dr. Setu Chaturvedi presented a video stegnography through LSB based hybrid approach. This method is used in AVI videos. Data hiding is done in ost video by using single bit, two bit, three bit LSB substitution and after that Advanced Encryption Standard (AES) Algorithm is applied. They have found the PSNR and correlation factor between Original and embedded image for 1 bit LSB & 2 bit LSB & 3 bit LSB Substitution and AES method. [3]

In the year 2011 ShengDun Hu, KinTak U presented a video stegnography system based on non-uniform rectangular partition. This technique can hide an uncompressed secret video in a host video stream. But we have to make sure that both the secret as well as the cover file should be of almost the same size. Each frame of secret video is partitioned in to non-uniform rectangular part which is encoded. Results of using this technique showed no distortion. All the PSNR values of the frames were larger than 28dB. [4]

Ramadhan J. Mstafa and khaled M. Elleithy, Senior Member, IEEE, Department of Computer science and Engineering, University of Bridgeport, proposed a highly secured method of video stegnography by using Hamming Code (7, 4). In their project they propose a secure video stegnography algorithm based on linear block code. The visual quality of the system is decided by the Pick Signal to Noise Ratio (PSNR) of stego videos are above 51 dB, which is close to the original video quality. The embedding payload is also acceptable, where in each video frame we can embed 16 Kbits and it can go up to 90 Kbits without degrading of the stego videos quality. [5]

Ramadhan J. Mstafa and khaled M. Elleithy, Senior Member, IEEE in Department of Computer Science and Engineering University of Bridgeport Bridgeport, proposed a video stegnography technique, "A High Payload Video Stegnography Algorithm in DWT Domain Based on BCH Codes (15, 11)." For encoding secret message BCH encoder is used. The encoded secret message embedded in video in DWT domain. The experimental results for this technique are better than above techniques.[9]

III. METHODOLOGY

The proposed system is high capacity video stegnography based on BCH code in DWT domain. This system gives idea about data hiding. The proposed system is enclosed by the two processes that are data embedding process and data extracting process.

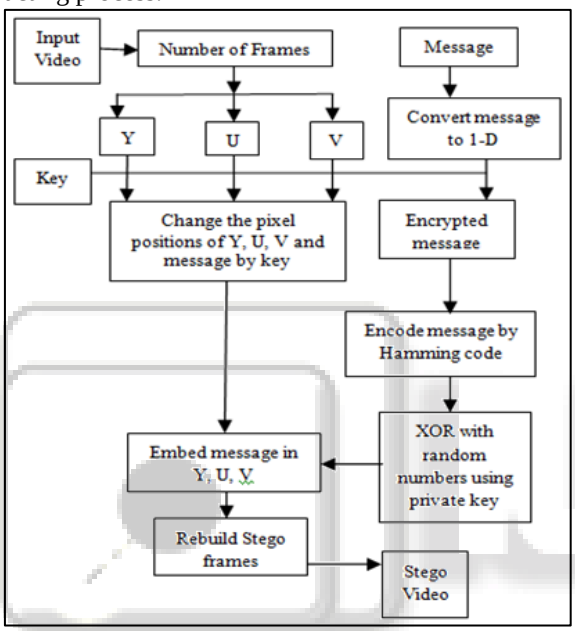

Fig. 2: Data embedding process

Secret message is text file which is embedded in to video. Change the bits positions of secret message by key1. That secret message is converted in to one dimensional array. Encoding is takes place with the help of BCH encoder. XOR the encoded data by using key2. Finally encoded secret message is ready for embedding in video.

Input video is converted in to number of frames and further each frame is converted in to Y, U, V components of image. 2D-DWT is applied on Y, U, V components of image which divided it in to LL, HL, LH, HH frequency components. DWT is well known method of converting time signal in to frequency signal. It gives detailed frequency coefficients than DCT and FFT. After that apply inverse DWT to all this LL, HL, LH, HH and rebuilt the stego frames. At last stego frames combined to form Stego Video.

IV. PERFORMANCE PARAMETERS

A. Visual Quality

1) Mean Square Error

MSE measures the average of the squares of the 'Error'. It is the average squared difference between a cover image and stego image.

$$\text{MSE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{h}[C(i,j,k)-S(i,j,k)]^2}{m*n*h} \qquad (1)$$

Where, C and S are refer as cover image and stego image respectively. In addition, m and n are defined as video resolutions and h indicates the R, G and B color channels (k=1, 2 and 3).

2) Peak Signal to Noise Ratio (PSNR)

PSNR ratio is used to find out the visual quality of the proposed video stegnography method. PSNR is an objective quality measurement used to calculate the difference between the original and the stego video frames. PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined through the mean squared error (MSE). It is expressed by,

$$\text{PSNR} = 10 * \log_{10}\left(\frac{{\text{MAX}_0}^2}{\text{MSE}}\right) \qquad (2)$$

Where, MAX_0 is maximum intensity of image. Typical value for the PSNR is 30 to 50 dB, where higher value of PSNR is always better.

B. Embedding Payload

Embedding payload is the maximum amount of data can be embedded into the cover file without losing the quality of the original file. Embedding payload of any video stegnography technique is decided by Hiding Ratio (HR).

Hiding Ratio (HR) is expressed by,

$$\text{HR} = \frac{\text{Size of embedded message}}{\text{Video size}} * 100\% \qquad (3)$$

V. RESULTS

The results for data hiding in video1.AVI video and prpol-rerender2. AVI video are shown in fallowing fig 3 and fig 4 respectively.

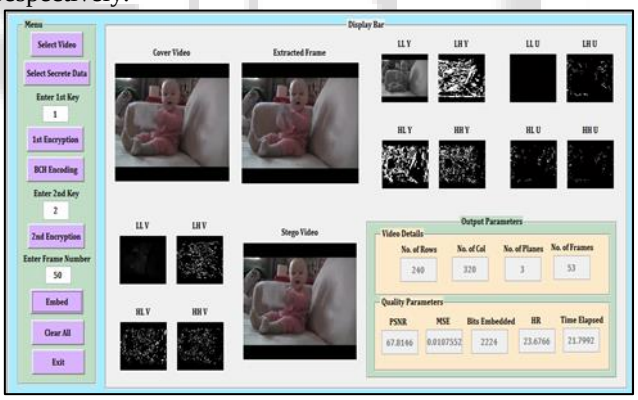

Fig. 3: Result for the data hiding in Video1.AVI video.

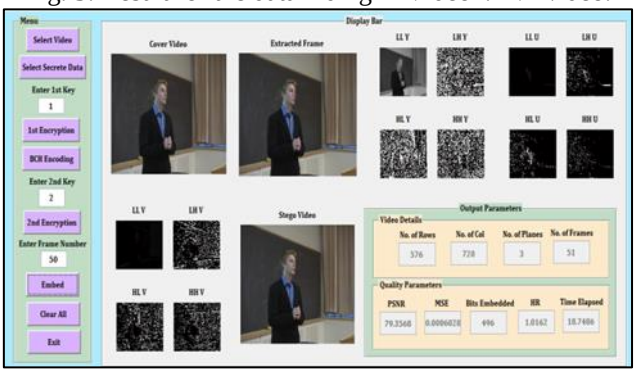

Fig. 4: Result for the data hiding in prpol-rerender2.AVI video.

Technique	Cover video	Video Resolution	No. of Frames	MSE	PSNR (dB)	Embedding payload	Hiding Ratio
Data Hiding Technique in Video Stegnography Using BCH Codes in DWT Domain	Video1. AVI	240*320	53	0.0107	67.81	2224 Bits	23.67%
	prpol: rerender2. AVI	576*720	51	0.0006	79.35	496 Bits	1.01%
	Flame.AVI	240*256	53	0.0038	72.28	496 Bits	6.60%
	Toy Plane_ Liftoff.AVI	480*640	53	0.0030	72.96	2224 Bits	5.91%

Table 1: Results of data hiding technique for different AVI videos.

The results for data embedding are calculated on the basis of parameters like embedding payload and visual quality. Embedding payload means embedding capacity of cover video. This embedding payload is used to calculate the embedding efficiency of video. The visual quality is another important parameter which depends upon mean square value and PSNR value. The PSNR should be between 30 to 50 dB, where higher value is always better. The results for data hiding in different cover videos are shown in Table1.

The four different types of AVI videos are taken as a cover video for data hiding as shown in above table. The PSNR value is between 67-79 dB and shows different hiding ratios depends on embedding payload.

VI. Conclusion

The data hiding by video stegnography based on BCH code in DWT domain technique is discussed in detail. The results for data hiding are discussed on the basis of parameters like embedding payload, visual quality and hiding ratio. The results for four different AVI video samples are discussed in above table. This data hiding technique may give better results than other data hiding technique.

References

[1] M. E. Eltahir, L. M. Kiah, and B. B Zaidan, "High Rate Video Streaming Steganography", in Information Management and engineering, 2009. ICIME '09. International conference on, 2009, pp. 550-553.
[2] R. Shanthakumari and Dr.s. Malliga, "Video Steganography Using LSB Matching Revisited Algorithm", in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV (Nov-Dec. 2014), pp 01-06.
[3] Hemant Gupta and Dr. Setu Chaturvedi, "Video Stegnography through LSB based hybrid approach", in International Journal of Engineering Research and Development, Volume 6, Issue 12 (May 2013), pp. 32-42.
[4] ShengDun Hu, KinTak U, "A Novel Video Stegnography based on Non-uniform Rectangular Partition", in International Conference on Computational Science and Engineering, pp 57-61, Aug.2011
[5] R. J. Mstafa and K. M. Elleithy, " A highly secure video stegnography using Hamming code (7, 4)" in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp. 1-6
[6] Ms. Pooja Vilas Shinde and Dr. Tasneem Bano Rehman, "A Survey: Video Stegnography techniques" in International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015 ISSN 2091-2730.
[7] Syeda Musfia Nasreen,et al.,"A Study on Video Stegnography Techniques" in International Journal of Computational Engineering Research (IJCER), Vol 05, Issue 10, October – 2015, ISSN (e): 2250 – 3005.
[8] K. Parvathi Divya, et al., "Various Techniques in Video Stegnography – A Review", in International Journal of computer and Organization Trends Volume-5, February-2014, ISSN: 2249-2593
[9] Ramadhan J. Mstafa and khaled M. Elleithy, Senior Member, IEEE, "A High Payload Video Stegnography Algorithm in DWT Domain Based on BCH Codes (15, 11)" in Department of Computer Science and Engineering University of Bridgeport Bridgeport, CT 06604, USA

