A DWT-BCH code based Video Steganography by employing Variable bit length Algorithm

Shyamala A[1], Raghu K[2]

[1]Department of ECE, REVA Institute of Technology & Management, Bangalore, India
[2]School of Electronics & Communication Engineering, REVA University, Bangalore, India

Abstract— *Due to the high speed of Internet we can easily transfer video data over the Internet, but people are worried about their data being hacked by unauthorized users. Inside the host medium (text, audio, image and video) we can embed the secret message in Steganography. Video Steganography is a significant method for data hiding. In this work, a variable bit length Video Steganography algorithm is proposed. To immune the secret data, it is first encoded using BCH codes, where the message bits of length k will be converted to a codeword of length n. Depending on the wavelet coefficient values of DWT(Discrete wavelet transform), secret data are embedded into the middle and high frequencies. The results demonstrate better results than in [1].*

Keywords— Video Steganography, BCH codes, DWT, Embedding Payload, PSNR, Variable bit length algorithm.

I. INTRODUCTION

Steganography is a method of hiding a secret message within another cover medium as shown in figure (1) so that the presence of the hidden message is indiscernible. The key concept behind steganography is that the transmitted hidden message is not noticeable to the casual eye. The Steganography algorithms have to be developed in such that except for the recipients of the message no other person should suspect the hidden message. Embedding efficiency is an important attribute of any steganographic scheme which influences the security [7]. The embedding efficiency signifies tier of performance that features the visual quality, security and strength against the steganalysis tools. The embedding payload is defines as the hidden data that is being carried within a cover data.

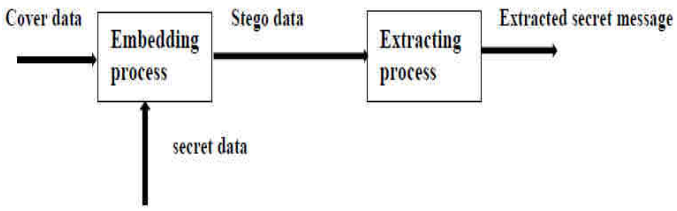

Fig. 1: General Block Diagram of Steganography

II. PROPOSED WORK

In the proposed algorithm the frames of uncompressed video are used as still pictures. First the video stream is separated into frames then every frame are going to be regenerate to YUV color space. Then DWT is applied to the three parts Y, U, and V. Second the important message is converted into one dimensional array and the message is encoded using BCH (15, 11) codes. The secret message is embedded using variable bit length algorithm into the middle and high frequencies of YUV components. By applying inverse DWT we obtain the Stego frames.

A. Discrete Wavelet Transform

Discrete Wavelet Transform is taken into account as important technique in image compression [12]. The fundamental idea of the DWT is to represent any impulsive function as a superposition of set of such basis functions. The basis functions are the scaled and shifted version of mother wavelet. In one dimensional sub band decomposition as in figure (2) the input sample is sub-divided into low pass and high pass sub bands. The Down sampled low resolution version of the input image is that the low pass sub band and residual information of the input image is that the high pass sub band.

When one dimensional sub band decomposition is carried out twice shown in figure (3), first in horizontal direction and then in vertical direction we obtain two dimensional sub band decomposition. LLi refers the low-resolution sub band which is the approximation of the original image. LHi, HLi, HHi refers the high- pass sub bands and represents the horizontal, vertical, and diagonal residual information of the original image. Where i represents the level of decomposition.

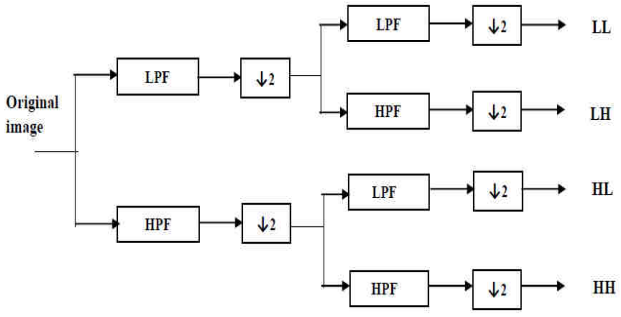

Fig. 2: One level two dimensional DWT Decomposition

The resulting one level two dimensional DWT is as shown in figure (3):

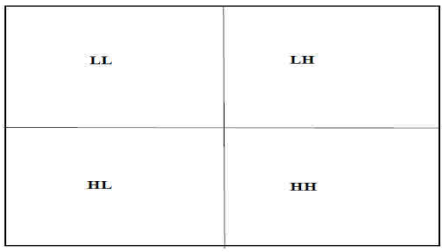

Fig. 3: First Level of the two dimensional DWT

B. BCH codes

BCH code can operate in Galois field and is considered as one of the powerful random cyclic code in detection and correction of errors [3]. BCH code are defined by two parameters that are length of code words (n) and maximum error corrected t. For any positive integer $m \geq 3$ and $t < 2^{m-1}$, a binary BCH code always exists with the parameters:

Codeword length: $n = 2^m - 1$

Message length: k

Number of error to be corrected: $n - k \leq mt$

The roots over the Galois field GF (2^m) specifies the generator polynomial of the code. For n=15 and k=11, using the property $n= 2^m -1$ we obtain the positive integer m=4. Let α be the primitive element of GF (2^4). The lowest degree polynomial over GF (2^4) is the generator polynomial. For BCH (15, 11, 1) the generator polynomial is the minimal polynomial of primitive elements α. The primitive polynomial for Galois field GF (2^4) is $1 + \alpha + \alpha^4$ which is a irreducible polynomial with m as 4. By calculating the minimal polynomial using the primitive polynomial 0, 1, α, α^2, α^3 and α^4 ($\alpha^4 = \alpha+1$) we obtain the generator polynomial g(x) as $1 + x + x^4$.

C. Data Embedding Procedure

The embedding process of secret message in figure (4) can be categorized into two levels: first the message will be encoded using the BCH codes and then the encoded message will be embedded into the cover video. The Embedding process is explained in following steps:

- Secret message is the input.
- Secret message is converted to one dimensional array.
- A BCH (15,11) encoder is used to embed the Secret message
- Load the cover video stream.
- Video sequences are converted into group of pictures.
- Frames are seperated into YUV colour space.
- To each Y, U, and V component two dimensional DWT is applied separately.
- Using variable bit length algorithm, into the middle and high frequency coefficients of Y, U, and V components the secret message is embedded.
- To each Y, U, and V component inverse two dimensional DWT is applied separately.
- Form YUV stego components and reassemble the stego frames.

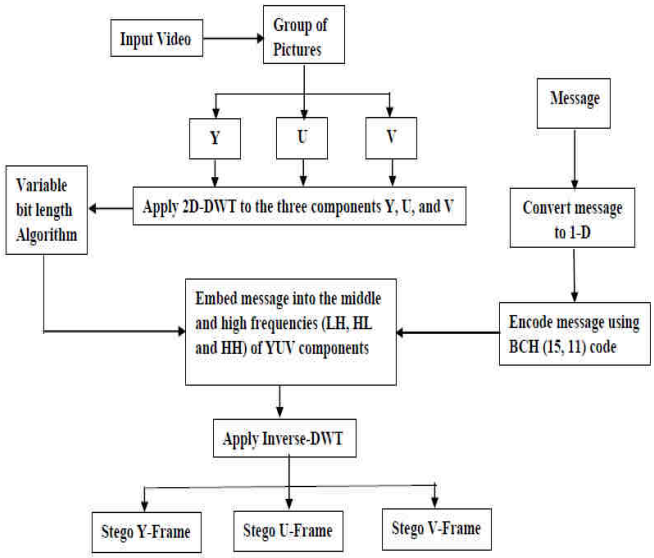

Fig. 4: A plan for the Data Embedding Process

D. Variable bit length Algorithm

The number of secret data bits to be embedded in each wavelet coefficient are determined using the Variable bit length algorithm given in equation (1).

$$BL = \begin{cases} 4, & wc \geq 2^4 \\ 3, & 2^3 \leq wc < 2^4 \\ 2, & wc < 2^3 \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where wc is wavelet coefficient, BL is number of bits to be embedded in the respective wavelet coefficient.

In this algorithm the bit length value depends upon the wavelet coefficient as shown in figure (5).

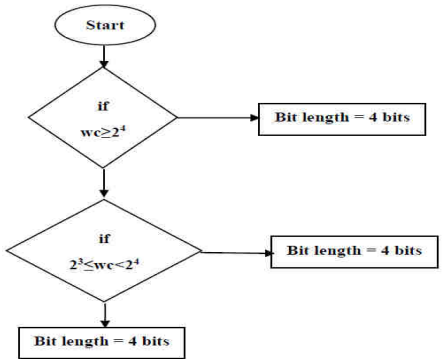

Fig. 5: Flowchart of Variable Bit Length Algorithm

E. Data Extracting Procedure

In extracting procedure the encoded message is recovered from the stego video as shown in figure (6). Using BCH

encoder the secret message will be decoded. This process can be explained by the following steps:

- Stego frames are the input.
- Frames are divided into YUV colour space.
- To each Y, U, and V component two dimensional DWT is applied separately.
- Using variable bit length algorithm the encoded message is extracted from the middle and high frequency coefficients of Y, U, and V components.
- Secret message is decoded using BCH (15,11) decoder.
- Decoded secret message is the output. Where wc is wavelet coefficient, BL is number of bits to be embedded in the respective wavelet coefficient. In this algorithm the bit length value depends upon the wavelet coefficient as shown in figure (5).

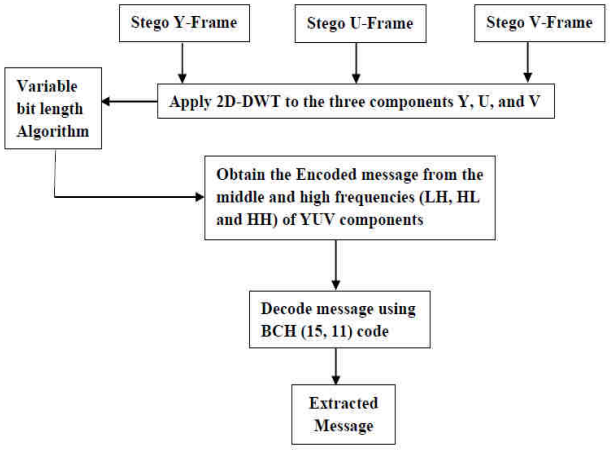

Fig. 6: A plan for the Data Extracting Process

III. RESULTS

The experimental results employs a QCIF video of 176 pixels wide and 144 pixels tall as cover data. An enormous amount of text is used as the secret data. Using BCH code of code word length 15 and message length 11 with maximum error to be corrected as 1, the secret message is encoded. Using variable bit length algorithm high PSNR value is obtained.

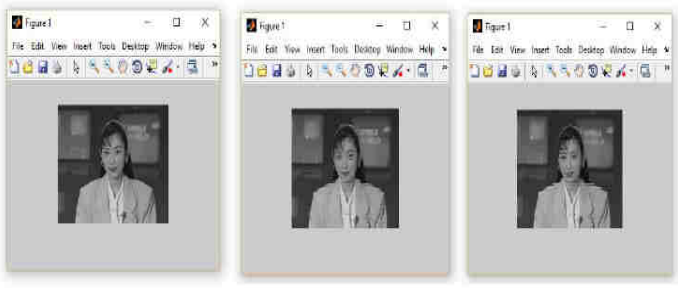

Fig. 7: (a). Original Frame, 7(b). Stego Frame of Fixed Bit Length Algorithm, 7(c). Stego Frame of Variable Bit Length Algorithm Flowchart of Variable Bit Length Algorithm

TABLE I. COMPARISON OF FIXED BIT LENGTH AND VARIABLE BIT LENGTH ALGORITHMS

Video sequences	PSNR in Fixed Bit Length Algorithm (dB)	PSNR in Variable Bit Length Algorithm (dB)
Akiyo	30.4227	30.4863
Mother-daughter	28.9314	28.9772
Bridge-close	27.6890	28.1200
Foreman	28.6142	28.8014

IV. CONCLUSION

In this paper, a DWT-BCH code based Video Steganography by employing Variable bit length algorithm has been proposed. The cover data video is decomposed into frames and then subdivided into Y, U, and V components. Using BCH (15, 11, 1) codes the secret message is encoded before Embedding process. When 2D-DWT is applied to YUV components, the secret data are embedded into middle and high frequencies. The proposed algorithm has high PSNR value. In future 2D-DWT decomposition can be used.

REFERENCES

[1] Ramadhan J. Mstafa, Khaled M. Elleithy, "A High Payload Video Steganography Algorithm in DWT Domain Based on BCH codes (15,11)," in *2015 Wireless Telecommunications Symposium (WTS)*, 2015, PP. 978-1-4-4799-6775-9.

[2] Sumanth Sakkara, Akkamahadevi D. H., K. Somashekhar, Raghu K, "Integer Wavelet Based Secret Data Hiding By Selecting Variable Bit Length," *International Journal of Computer Applications (0975-888)*, Vol 48- No-19, June 2012.

[3] Z. Rongyue, *et al.*, "An Efficient Embedder for BCH Coding for Steganography," *Information Theory, IEEE Transactions on*, vol. 58, pp. 7272-7279, 2012.

[4] I. Diop, *et al.*, "Adaptive steganography scheme based on LDPC codes," in *2014 16th International Conference on Advanced Communication Technology (ICACT)*, 2014, pp. 162-166.

[5] M. A. Alavianmehr, *et al.*, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," in *Computer and Knowledge Engineering (ICCKE), 2012 2nd International eConference on*, 2012, pp. 194-198.

[6] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes,' in *Image and Signal Processing (CISP), 2011 4th International Congress on*, 2011, pp. 1784-1787.

[7] R. J. Mstafa and K.M. Elleithy, "A highly secure video steganography using Hamming code (7,4)," *in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island*, 2014, pp. 1-6.

[8] C. Chin-Chen, *et al*., "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in *Electronic Commerce and Security, 2008 International Symposium on*, 2008, pp. 16-21

[9] L. Guangjie, *et al.*, "An Adaptive Matrix Embedding for Image Steganography," in *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, 2011, pp. 642-646.

[10] Y. Liu, *et al.*, "A Robust Data Hiding Algorithm for H. 264/ AVC Video Streams," *Journal of Systems and Software*, 2013.

[11] I. E. Richardson, *H.264 and MPEG-4 video compression: video coding for next-generation multimedia:* John Wiley & Sons, 2004.

[12] E. Prasad, "High Secure Image Steganography based on Hopfield Chaotic Neural Network and Wavelet Transforms," *International Journal of Computer Science & Network Security*, vol. 13, 2013.