International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 229-234
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

AN EFFICIENT AND SECURE HIGH CAPACITY VIDEO STEGANOGRAPHY USING BCH CODES (15, 11) IN DWT DOMAIN

Ajit Danti
Department of MCA
JNNCE, Shivamogga,
Karnataka, India

G R Manjula
Department of CSE
JNNCE, Shivamogga,
Karnataka, India

Vidhathri K N
Department of CSE
JNNCE, Shivamogga,
Karnataka, India

***Abstract*—Video data over internet is increasing nowadays. Complex structure and huge size of the video makes it suitable for efficient steganography. Embedding payload and embedding efficiency are the two factors on which the performance of any steganography algorithm relies. An efficient and secure large embedding capacity video steganography using BCH codes (15, 11) in DWT domain is proposed. Secret image is scrambled using chaos algorithm to make it unreadable and further encoded using BCH codes (15, 11) to improve the security of the algorithm. The encoded image is embedded into cover videos discrete wavelet transform (DWT) coefficients. DWT high and middle frequency regions are utilized to insert the encoded secret image as the middle and high regions are less sensitive data. The distortion between original video and stego video are calculated using PSNR and MSE metrics. Experimental results illustrates that the proposed approach is highly secure and robust since it uses multilevel security. The proposed method is suitable for communicating confidential information and secret data storing, E- commerce, protection against data alteration, media etc. As there is no trace of finding the existence of the secret image, this method is hard to break so it becomes difficult for the steganalysis to be done; hence it is very efficient and secure.**

Keywords— **Chaos, BCH, DWT, PSNR**

I. INTRODUCTION

Internet appeared in the late 1960s and 1970s out of the need to trade research information among the analysts over various colleges and furthermore to empower communication in the combat zone to pass on imperative data which could demonstrate worthwhile in the war circumstances. Since the beginning of the web, the security and the privacy of the delicate data have been of most extreme significance and top need.

Communication through internet is increasing day by day. Data of various kinds like text, images and videos are sent and received over internet on daily basis. The quick increment of data sharing between individuals has caused various security issues. New security breaches are coming on a daily basis. One of the approaches to offer security in data communication is by method of steganography. Video steganography is one among the various growing techniques to conceal the secret data inside the cover video and sending it through transmission medium. Complex structure and huge size of video makes it suitable to be used as cover medium.

The proposed algorithm utilizes the videos of various formats as cover medium. The secret data to be embedded is first scrambled using chaos algorithm to make it unreadable and then encoded using BCH codes (15, 11) to improve the security of the algorithm. Then the encoded secret data is inserted into high and middle frequencies of the Y, U and V elements of the frames. The experimental results observed show that the proposed approach gives better visual quality.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are illustrated in section III. Concluding remarks and future scope are given in section IV.

II. PROPOSED ALGORITHM

A. Chaos algorithm –

Chaos algorithm is utilized to scramble the secret picture before it is encoded using BCH codes and embedded into the cover source. Here cover source is a video into which we wish to embed the secret image. Sender of the secret image encrypts the secret image and sends the encrypted and BCH encoded secret image by embedding into the cover video. So first and foremost task is to scramble the secret picture using chaos algorithm [12]. To scramble the image bits, the algorithm utilizes logistic mapping technique. The chaotic map is defined in equation 1.

$$X_{k+1} = \mu X_k (1 - X_k) \qquad (1)$$

Here $0 < X_k < 10$ and $0 \leq \mu \leq 4$. μ denotes the control parameter. A non-convergent and non-periodic sequence $\{X_k$, k = 0,1,2,...} is generated. Initial conditions with different values are utilized to obtain uncorrelated statically logistic sequences. Utilizing different initial conditions for every part, apply chaos theory on different parts to take benefit of its sensitiveness for initial value and increase the security and provide unpredictability. The secret image is partitioned equally into 8 parts; each will have RGB components each of 8 bits. Then use the logistic map to generate a logistic chaotic sequence of N real numbers $\{X_k\}$ where k = 0, 1, 2, N-1. The initial condition considered for μ is 3.60 and initial condition considered for X is 0.65. Using initial conditions of X_k and μ the sequence is shown as below:

$\{X_k\}$ = {0.819000, 0.533660, 0.895921, 0.335687, 0.802805, 0.569913, 0.882404, 0.373563...}

The threshold T is the mean values of these real numbers. For the first part, T is utilized. If $X_k \geq T$ then $B_k = 1$ else $B_k = 0$. Therefore generated binary sequence $\{B_k\}$ for the first part is as below:

$$\{B_k\} = \{1, 0, 1, 0, 1, 0, 1, 0...\}$$

In secret image part for each 8 bit components C_k , an XOR operation is performed between each bit of C_k with single bit of B_k foe example if C_k = 10101001 and B_k = 1 then C_k = 01010110, where C_k is the encrypted component. This process is repeated until every component is encrypted. The remaining 8-1 parts of the secret data are also scrambled using the same technique using different logistic maps and different initial values.

B. Bose, Chaudhuri, and Hocquenghem (BCH) Codes

It is an expansive class of random error detecting and multiple error correcting cyclic codes. BCH codes are an astounding speculation of the Hamming code. Hamming code can be used only for single bit error correction. For any positive integer m>= 3 and $t < 2^{m-1}$, there exists a binary BCH code with the accompanying parameters:

k bits of Message
$n = 2^m - 1$ length of codeword block
Maximum number of correctable error bits: t
$d_{min} >= 2t + 1$ of minimum distance
$n - k <= mt$ number of parity-check digits

A maximum of t bits can be corrected for a binary BCH (n, k, t) with codeword of the length n ($c_0, c_1, c_2 \ldots c_{n-1}$) and message of length k ($a_0, a_1, a_2 \ldots a_{k-1}$). Messages and codewords that are encoded can both be deciphered as polynomials, where $a(x) = a_0 + a_1x^1 + \ldots + a_{k-1}x^{k-1}$ and $c(x) = c_0 + c_1x^1 + \ldots + c_{n-1}x^{n-1}$.

In the proposed technique, the BCH code (n, k, t) where n= 15, k= 11 and t=1 is utilized with the accompanying characteristics:

1. The primitive polynomial is $\alpha^4 + \alpha + 1$.
2. Primitive component of GF (2^4) is α , where m = 4 and n = 2^4-1.
3. The minimal polynomials of α, α^3, and α^5 are:
   - $M_1(x) = x^4 + x + 1$
   - $M_2(x) = x^4 + x^3 + x^2 + x + 1$
   - $M_5(x) = x^2 + x + 1$
4. For the applied BCH code (15, 11) he minimum distance chosen is greater than two.
5. The generator polynomial $g(x) = M_1(x) = 1 + x + x^4$ is used if single error correction is utilized.

C. Embedding Process

The information embedding procedure can be finished by the accompanying strides and the block diagram for the same is depicted in Fig. 1.

Step1: Secret data to be concealed is taken as input.(content or picture).
Step 2: Convert the secret information (which is a colour picture) to a 1-D array, and after that change the position of the entire picture using chaotic algorithm.
Step 3: The entire secret picture is changed to a one dimensional array.
Step 4: Utilizing the BCH (15, 11) encoder encode the picture.
Step 5: Encoded data is split to block containing 15 bits each (4 bits of parity + 11 bits of picture), and then XORed with the 15 bits of random value as key.
Step 6: The cover video stream is input.
Step 7: Number of frames are obtained from the video sequence.
Step 8: Every frame is split into the YUV colour space.
Step 9: To every Y, U, and V frame segments, 2D-DWT is applied separately.
Step10: For every U, V, and Y frame segments, embed the encoded picture into the high and middle frequency coefficients (HH, LH, and HL).

$$Y_{ij} = E\,[\text{floor}\,(Y_{ij\_bit1,\,2,\,3}),\, S] \text{ if } (Y_{ij} \geq 0)$$
$$Y_{ij} = E\,[\text{floor}\,(|Y_{ij\_bit1,\,2,\,3}|),\, S] \text{ if } (Y_{ij} < 0)$$
$$U_{ij} = E\,[\text{floor}\,(U_{ij\_bit1,\,2,\,3}),\, S] \text{ if } (U_{ij} \geq 0)$$
$$U_{ij} = E\,[\text{floor}\,(|U_{ij\_bit1,\,2,\,3}|),\, S] \text{ if } (U_{ij} < 0)$$
$$V_{ij} = E\,[\text{floor}\,(V_{ij\_bit1,\,2,\,3}),\, S] \text{ if } (V_{ij} \geq 0)$$
$$V_{ij} = E\,[\text{floor}\,(|V_{ij\_bit1,\,2,\,3}|),\, S] \text{ if } (V_{ij} < 0)$$

Where E is the embedding method, S is the encoded secret data. And U_{ij}, V_{ij} and $Y_{ij,}$ are the U, V and Y coefficients, and

Step11: I-DWT is applied on the frame elements.

Step12: YUV colour space is converted back to RGB colour space then stego frames are reconstructed.

Step13: Stego video is output

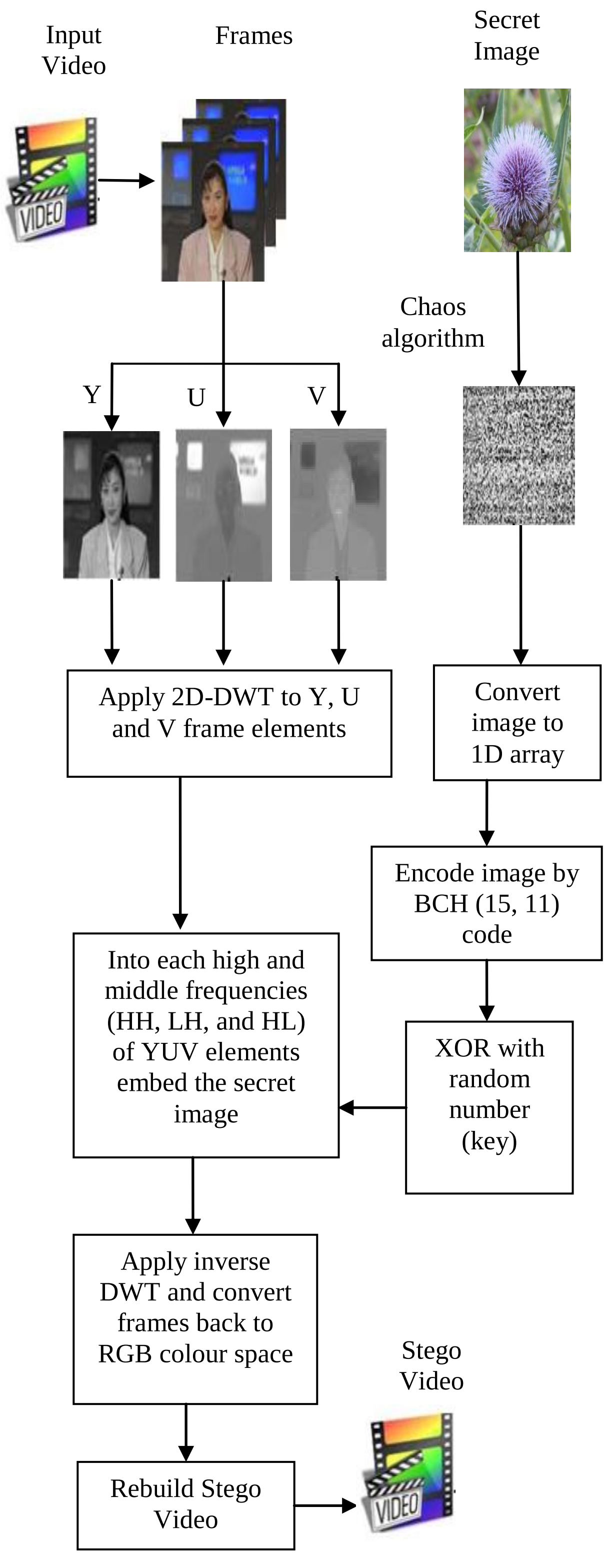

Fig. 1: Video Steganography embedding algorithm Block Diagram

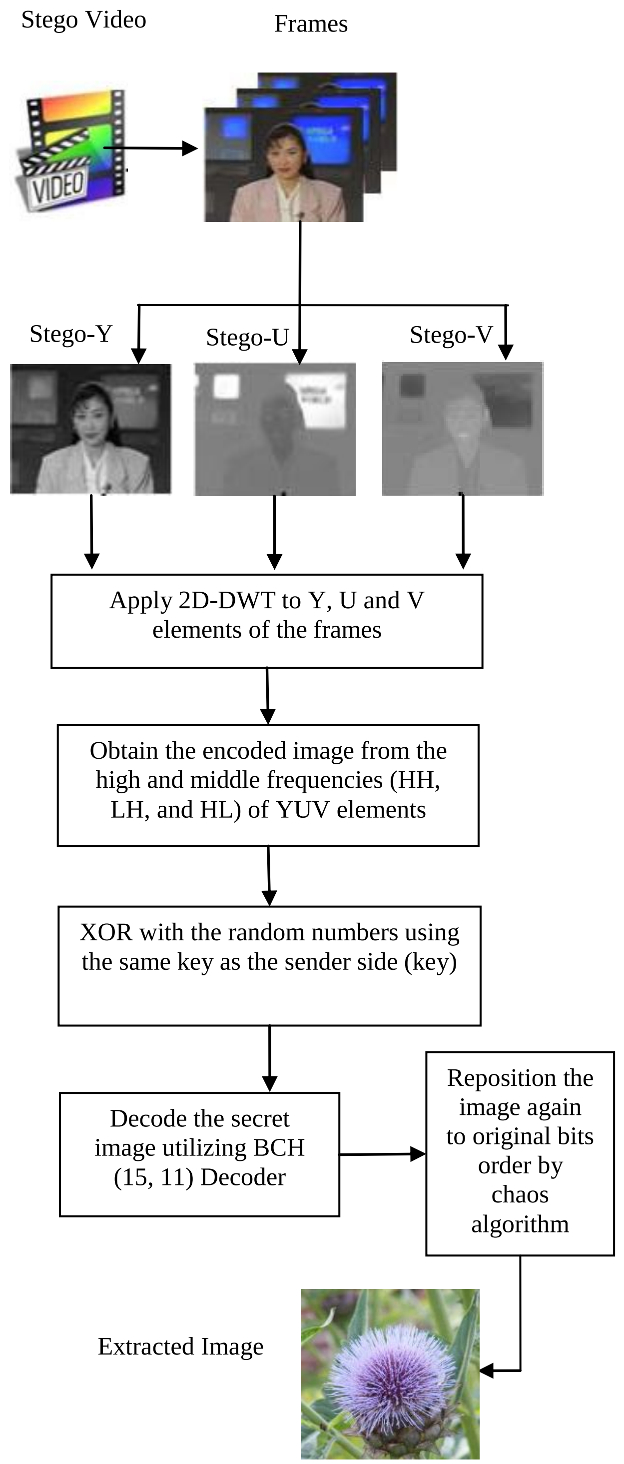

Fig. 2: Video Steganography Extraction algorithm Block Diagram

D. Extraction Process

The extraction process can be finished by the accompanying strides. The block diagram for the secret image extraction is depicted in Fig. 2

Step 1: Stego video is input.

Step 2: Number of frames are obtained from the Stego-video.

Step 3: Every frame is isolated into the YUV colour space.

Step 4: To every Y, U, and V elements 2D-DWT is applied separately.

Step 5: From the high and middle frequency coefficients (HH, LH, and HL) of every U, V and Y elements of the video frames, the encoded data is extracted.

$$S_{1,2,3} = EX\,[\text{floor}\,(Y_{ij\_bit1,2,3})] \text{ if } (Y_{ij} \geq 0)$$

$$S_{1,2,3} = EX\,[\text{floor}\,(|Y_{ij\_bit1,2,3}|)] \text{ if } (Y_{ij} < 0)$$

$$S_{1,2,3} = EX[\text{floor}\,(U_{ij\_bit1,2,3})] \text{ if } (U_{ij} \geq 0)$$

$$S_{1,2,3} = EX\,[\text{floor}\,(|\mathbf{U}_{ij\_bit1,2,3}|)] \text{ if } (U_{ij} < 0)$$

$$S_{1,2,3} = EX\,[\text{floor}\,(V_{ij\_bit1,2,3})] \text{ if } (V_{ij} \geq 0)$$

$$S_{1,2,3} = EX\,[\text{floor}\,(|V_{ij\_bit1,2,3}|)] \text{ if } (V_{ij} < 0)$$

Where, EX is the extracting procedure. S is the secret data. And U_{ij} ,V_{ij} and Y_{ij}, are the distorted U, V and Y coefficients

Step 6: Segment the entire encoded message into 15-bits groups.

Step 7: The random 15-bits number that was utilized by the sender is used to XOR each group of bits.

Step 8: The data is decoded by the BCH decoder.

Step 9: An array is obtained from the outcome groups.

Step10: The data bits are rearranged to the original bit position using chaos algorithm.

Step 11: Output the secret picture/data.

Two techniques are utilized as a part of the proposed steganography algorithm to scramble the secret picture. The strategies used are known both to the sender and receiver of the secret information. Before concealing the secret information inside the cover video, the secret image is scrambled to make it unreadable by utilizing chaos algorithm. Then the chaos encrypted secret image is encoded utilizing BCH codes. To further enhance the security of the proposed method and improve the robustness, the outcome image bits are grouped to 15 bits each and XORed with a random 15- bit number as key. To decode at the receiver side the same key has to be used and should have knowledge of the BCH codes used by the sender. Even logistic map is required to decrypt the scrambled secret image.

III. EXPERIMENTAL RESULTS

MATLAB is used to test the proposed algorithm. Various videos and secret images utilized for implementing the proposed video steganography algorithm are: Five various format videos are chosen, namely Akiyo.3gp, Carphone.mp4, Container.3gp, Rhinos.avi and Foreman.mp4 as shown in Fig. 3.

Fig. 3: Various Cover Videos (Akiyo.3gp, Carphone.mp4, Container.3gp, Rhinos.avi and Foreman.mp4)

Five different secret images chosen are: Lena.jpg, Pepper.jpg, Flower.jpg, Building.jpg and Tiger.jpg all 128 X 128 in dimension as shown in Fig. 4.

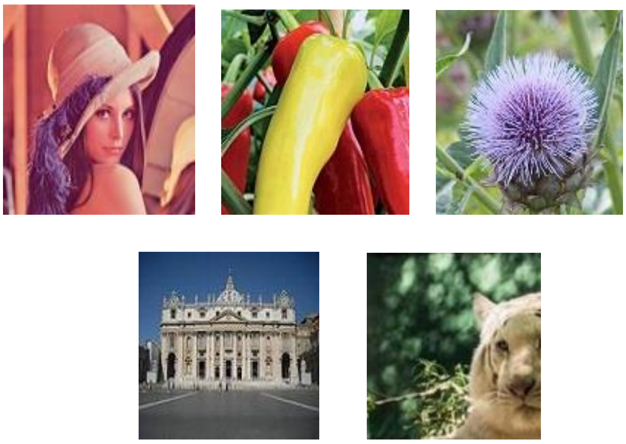

Fig. 4: Secret Images- Lena, Pepper, Flower, Building and Tiger respectively in .jpg format

The perceptual nature of stego video can be measured utilizing the equation

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

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 229-234
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

Where, m and n are the video resolution. O is original frame and S is stego frame element respectively.The distortion in the stego video is measured by Peak Signal to Noise Ratio (PSNR) utilizing the equation 3.

$$PSNR = 10 * Log_{10}\left(\frac{MAX\ {o}^2}{MSE}\right) \quad (3)$$

The experimental results are depicted in Table 1 Overall, the Rhinos.avi and Foreman.3gp video has the best visual quality with PSNR value 48.64 dB and MSE value 0.0171 for Rhinos.avi video. And the PSNR value of 48.38 dB and MSE value of 0.0067 for Foreman.3gp video is observed.

Table -1 Experiment Result

Video Sequences (.3gp, .avi, .mp4)	**Secret Images (128 x 128)**	**PSNR (Video)**	**PSNR Y**	**PSNR U**	**PSNR V**
Akiyo	Lena	44.901	40.164	61.080	61.098
Akiyo	Pepper	44.902	40.164	61.157	61.115
Akiyo	Building	44.903	40.165	61.119	61.188
Akiyo	Tiger	44.903	40.165	61.194	61.169
Akiyo	Flower	44.901	40.164	61.094	61.095
Carphone	Lena	46.027	41.384	61.933	62.093
Carphone	Pepper	46.028	41.276	65.828	65.915
Carphone	Building	46.028	41.276	65.937	65.911
Carphone	Tiger	46.028	41.275	65.892	65.914
Carphone	Flower	46.028	41.384	62.055	62.018
Container	Lena	41.729	35.925	59.029	59.029
Container	Pepper	41.729	35.925	59.051	58.975
Container	Building	41.729	36.952	62.914	62.179
Container	Tiger	41.729	36.952	62.847	62.147
Container	Flower	41.729	35.926	58.988	58.992
Rhinos	Lena	48.646	43.906	65.947	65.685
Rhinos	Pepper	48.649	43.907	65.964	65.824
Rhinos	Building	48.649	43.906	65.967	65.843
Rhinos	Tiger	48.649	43.907	65.946	65.819
Rhinos	Flower	48.647	43.906	65.922	65.781
Foreman	Lena	48.384	43.742	61.980	61.549
Foreman	Pepper	48.392	43.745	62.006	61.689
Foreman	Building	48.393	43.744	62.076	61.714
Foreman	Tiger	48.389	43.742	62.119	61.626
Foreman	Flower	48.384	43.740	61.950	61.608

The technique proposed is tested using five various secret images and five different cover videos of varying format (Akiyo.3gp, Container.mp4, Carphone.3gp, Rhinos.avi and Foreman.mp4). The cover video chosen is in AVI (Audio Visual Interleaved) format, .mp4 format (Motion Pictures Expert Group- 4 Part 14) and .3gp (Third Generation Partnership) format. The cover video, which are nothing but still pictures varies in size. The size of the secret picture taken is 128 x 128.

Table 1 show the peak signal to noise ratio of performance of our proposed method. The PSNR value for Y component ranges between 35DB to 43DB, and the PSNR value for U component is between 58DB to 65DB, and the PSNR value for V component is between 58DB to 65DB. The PSNR value of Y component is less than PSNR value of U and V component because secret data embedded in Y component is large compared to U and V component.

Fig. 5: Secret Image

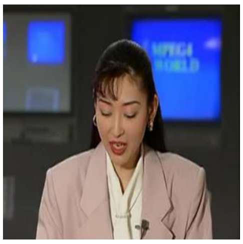

Fig. 6: Cover Video

Fig. 7: Stego Video

Fig. 8: Recovered Image

Fig. 5 illustrates the secret image to be embedded in Akiyo.3gp cover as shown in Fig. 6. The resultant stego video is depicted in Fig. 7. After extraction process the recovered image is as shown in Fig. 8. Perceptual quality of the stego video is good as difference between cover video and stego video is not noticeable to the human eyes. This algorithm is robust against attacks as the algorithm creates more confusion to the attackers. The hacker cannot understand extracted secret image from the video as the image bits are scrambled using chaos algorithm. Even if he somehow extracts the secret image, since he doesn't have the logistic map to unscramble the secret image, he can't get the secret image in its original form. One more level of security is added by encoding the encrypted image using BCH codes (15, 11) and then XORing each 15 bit block by a 15 bit random number. The very purpose of steganography is served if the perceptual quality of the stego video is good. Any hacker who is observing the transmission channel cannot predict whether the information is being transmitted over the channel or not.

IV. CONCLUSION

An efficient and large embedding capacity approach for concealing the existence of an image in cover video has been proposed. Experimentation is done utilizing cover videos of various formats like AVI, MP4 and 3GP. Obtained results are compared with base techniques which conceals text message in YUV video file. We can infer that the visual quality of the Stego video and the retrieved image is observed to be good in the proposed method. For example, Foreman.3gp video used as cover video for embedding secret image Pepper.jpg gives 48.3927 dB as PSNR value, which is better compared to existing system. In base technique[1] the PSNR value lies between 35dB to 45dB for concealing text information (small in size) inside cover video, while the proposed algorithm gives better PSNR value in the range of 35dB to 48dB for concealing colour image inside cover video. For example, using Foreman.3gp video to conceal Pepper.jpg gives PSNR value for video as 48.3927 dB, PSNR Y value of 43.7455 dB, PSNR U value of 62.0062 dB and PSNR V value of 61.6892 dB which is observed to be better compared to the base technique which conceals text file inside the same Foreman video with, PSNR Y value of 41.374 dB, PSNR U value of 41.982 dB and PSNR V value of 42.532 dB. Confusion created for the attackers is more in the proposed algorithm as both encryption and encoding techniques are utilized to conceal the secret information. So the method is robust against attacks. The proposed method is strengthened with respect to security aspect which is the major requirement in communication stream. Before embedding the image inside a video, it is encrypted using chaos algorithm and then encoded using BCH codes (15, 11). Multiple levels of security are provided through chaotic encryption and BCH encoding before embedding in high and middle frequencies of Y, U, and V elements of the video frame. So this method is more secure for information hiding. This method can be used to effectively conceal colour secret image in a cover video of any format.

This work hides an image file in a video file. In the future work it can be extended for hiding video file in a video and also different techniques of frequency domain can be utilized to enhance the payload capacity.

V. REFERENCE

[1] Mstafa, R.J. and K.M. Elleithy. A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11). in Wireless Telecommunications Symposium (WTS), 2015.

[2] Mstafa, Ramadhan J., and Khaled M. Elleithy. "An Efficient Video Steganography Algorithm Based on BCH Codes." ASEE, 2015.

[3] 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.

[4] 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.

[5] 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.

[6] W. Jyun-Jie, et al., "An embedding strategy for large payload using convolutional embedding codes," in ITS Telecommunications (ITST), 2012 12th International Conference on, 2012, pp. 365-369.

[7] R. Zhang, et al., "Fast BCH Syndrome Coding for Steganography," in Information Hiding. vol. 5806, S. Katzenbeisser and A.-R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 48-58.

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

[9] G. Prabakaran and R. Bhavani, "A modified secure digital image steganography based on Discrete Wavelet Transform," in Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference , 2012, pp. 1096-1100.

[10] L. Tse-Hua and A. H. Tewfik, "A novel high-capacity data-embedding system," Image Processing, IEEE Transactions o n, 2006, vol. 15, pp. 2431-2440.[11]

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

[12] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 3, No 1, pp. 11-22, February 2014.