International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(4), pp.094-100
DOI: http://dx.doi.org/10.21172/1.84.13
e-ISSN:2278-621X

A SYSTEMATIC APPROACH TO HIDE TEXT IN VIDEO USING HAAR WAVELET TRANSFORM AND BCH CODES

Jaspreet kaur[1] and Jagroop Kaur[2]

Abstract- **It is essential to broadcast data in secure manner over an internet.To hide data in any files such as Image, Audio, and Video carrier files the Steganographic techniques are required. The earlier steganographic techniques are not sufficed due to some capacity problem. And, Video steganography is one solution to overcome this capacity problem because the data can be hidden in any frame of video. The presented work describes the implementation of hiding text in video files with the help of haar wavelet transform in selected frame or image and BCH codes. BCH codes are used for the encryption of information. Any frame from the video is selected to embed information. Apply Haar wavelet transform on that selected frame to get the low frequency sub-band in an image. The frequency sub-bands are LL, LH, HL and HH. Select any sub-band to hide information. To check the robustness of proposed algorithm the extracted message is compared with original one by applying various operations on stego image such as crop, copy, Zoom in and Zoom out. It is observed that the good quality of the extracted message after applying operations is achieved. Video steganography is a procedure to conceal information in video files in protected mode to broadcast over the internet.Performace of the video steganographic algorithm is measured with the help of PSNR and other paremeters such as MSE,Standard Deviation,Variance.The video frame having highest value of PSNR will chosen for embedding data. PSNR increases the efficiency of proposed algorithm.**

Keywords: Video, Steganography, PSNR, MSE.

I. INTRODUCTION

Video Steganography plays a vital task in real life where the subscribers wants to keep the information secret and needs to hide more and more information. Every time the large amount of information is requisite to store then the video steganography is the best method. Information is basically the heart of computer communication and till now, a variety of techniques have been implemented and formed to achieve the objective of using steganography to hide information.

The difficulty occurs when Traditional Text and Image Based Steganography techniques are not be adequate .They are used to hold only tiny quantity of information in files. So to carry large amount of information there is no technique to hide message. Here, the need of Video Steganography comes into existence. The use of video file as a carrier media for the protected information is overcame the capacity problem. To hide information, two or more frames can also be in use as a cover medium. Video files have a huge Capacity than audio and image files to store information. To expand the security aspects the Steganography can be joint with the cryptography techniques for further powerful systems for securely transmitting information.

A. BCH Codes

Secret message can be encrypted with the aid of BCH codes.BCH (Bose – Chaudhuri - Hocquenghem) Codes outline a huge class of multiple random error-correcting codes. They were first exposed by A. Hocquenghem in 1959. BCH codes are cyclic codes. The unique applications of BCH codes were secret to binary codes of length 2 − 1 m for some integer m. These were extensive later by Gorenstein and Zieler (1961) to the nonbinary codes with symbols from Galois field GF (q). For BCH codes three parameter are required (n, k, t).Where, n is the block

[1] *Department of Computer Engineering Punjabi University, Patiala*
[2] *Department of Computer Engineering Punjabi University, Patiala*

codeword length, k is the message length, t is the maximum correctable error bits.There will be a binary BCH codes with the following properties:
Block codeword length: $n = 2 m - 1$
Message length : k
Maximum correctable error bits: t
Minimum distance: $dmin > = 2t + 1$
Parity check bits: $n - k <= mt$
The inventors of BCH codes decided that the generator polynomial will be the polynomial of the lowest degree in the Galois field GF (2).

II. Literature Survey

In this paper, the author proposed a novel video steganography algorithm based on the KLT tracking algorithm and BCH codes in the wavelet domain. The proposed algorithm encompasses four distinct steps. First, in the encryption process the secret message is preprocessed, and secret message is encoded by applying BCH codes (n, k, t). Second, to identify the facial regions of interest, face detection and face tracking algorithms are applied on the cover videos. Third, In the Embedding process embeds the encoded secret message into the high and middle frequency wavelet coefficients of all facial regions are achieved. Forth, In the extraction process, extracting the secret message from the high and middle frequency wavelet coefficients for each RGB components of all facial regions is accomplished. Experimental results of the proposed video steganography algorithm have demonstrated a more embedding efficiency and a more embedding payload. [1]

In this paper, based on BCH coding the author proposed a huge embedding payload of video steganography algorithm .The secret information is firstly encrypted with the help of BCH (n, k, and t) codes to increase the security of an algorithm. Then, apply DWT on video frames and embeds secret information into video frames. During DWT the middle and high frequency sub-bands are examined to be less perceptive data, the secret information is enclosed only into the middle and high frequency sub-bands. The planned algorithm is proved with two kinds of videos that have fast and slow motion objects. The experimental results of this algorithm are compared with both the Least Significant Bit and other algorithms. The results depict good performance for the proposed algorithm rather than for the other algorithms. The evaluated hiding ratio of the planned algorithm is around 28%, which is calculated as a huge embedding payload with a minimum agreement of visual quality and the robustness of this algorithm is checked by performing various attacks on this proposed algorithm. [2]

Due to very quick development of internet and multimedia technologies, the Information concealing has received much concentration where privacy of information is played a vital role. This is resolved by Steganography, which is the process of hiding information into other information, so that attacker cannot detect the presence of hidden information smoothly. Here, so many techniques to hide information within an image, text, audio/video etc. From all other techniques image steganography is a very enticing research area. The main goal is to transfer information inside a stego-image by reducing the number of bit flips. In this research paper, The author developed a new steganography method with the help of Graphical codes and also make a correlation with another steganographic method using BCH codes has been prepared. [3]

The main intention of steganography are depends upon characteristics like Undetectability, robustness and capacity of the covered data, these characteristics that detached it from linked techniques like cryptography and watermarking. This research paper gives a review on digital images steganography and covers its basic concepts. Approaches for rising steganographic security are outlined and important research advancements are also examined. The growth of image steganographic techniques in spatial domain, in jpeg format and also depict the recent growth in the field of image steganography. [6]

The objective of this review paper is to learn the techniques of steganography by using the video file as a carrier file. The steganography is the process of hiding something with the help of embedding process in cover carrier i.e. in video file. In the video steganography only one video file can be used along with distinct frames and audio files. More information can be stored in video file rather than any other file, After all, the use of the video based steganography can be more suitable than other multimedia files. Therefore, in this paper the video steganography has been explained and the benefits of using the video file as a carrier medium for steganography have been projected. [7]

III. Proposed Algorithm

The proposed algorithm consists Encryption & Embedding Process and Extraction Process.

B. Encryption & Embedding Process

The flowchat of encryption and embedding process is as follows:-

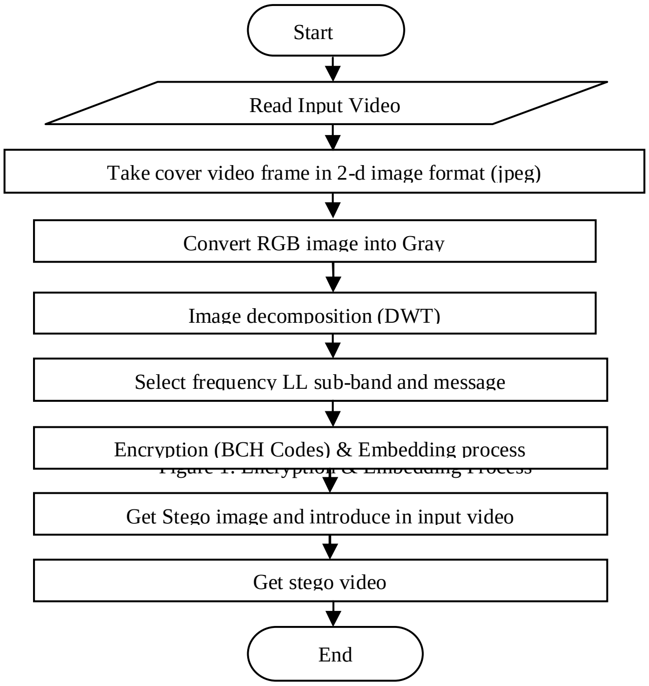
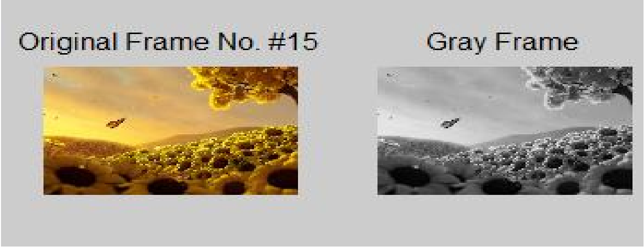

Start
Read Input Video
Take cover video frame in 2-d image format (jpeg)
Convert RGB image into Gray
Image decomposition (DWT)
Select frequency LL sub-band and message
Encryption (BCH Codes) & Embedding process
Get Stego image and introduce in input video
Get stego video
End

Figure 1: Encryption & Embedding Process

The steps for an algorithm are as follows:-

Step 1. Read Input Cover Video

For embedding process takes a cover video frame and secret text message as the inputs. Then convert cover video frame into gray frame to reduce the color complexity of pixels.Further, choose gray frame for image decomposition.



.

Figure 2: Conversion of RGB frame into Gray frame

Step 2. Image Decomposition (DWT)

Apply Discrete Haar Wavelet Transform to the gray cover video frame to decompose into different frequency sub-bands such as LL sub-Band, LH sub-Band, HL sub-Band and HH sub-Band image.LL sub-Band contains actual information of the video cover frame and other sub-bands contains the information of edges and noise.

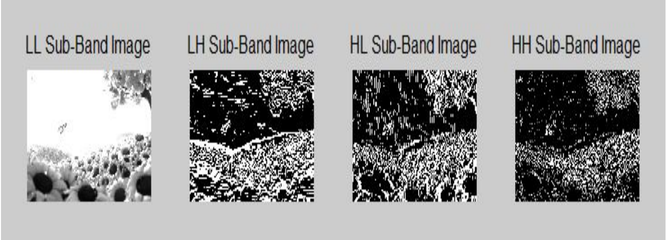
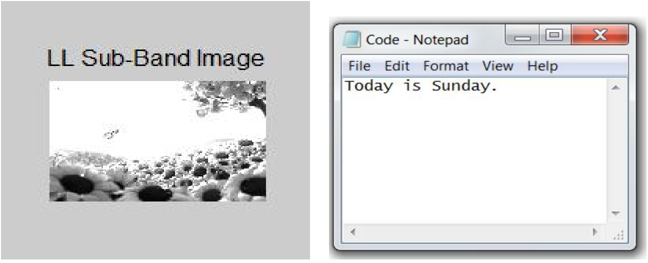


Figure 3: Haar wavelet Transform

Step 3. Select frequency sub-band and secret message

Select LL sub-band to hide secret text message. Load a secret text message which embeds into the video cover frame.Before embedding secret text into video cover frame its very essential to encrypt secret text message to increase the security.

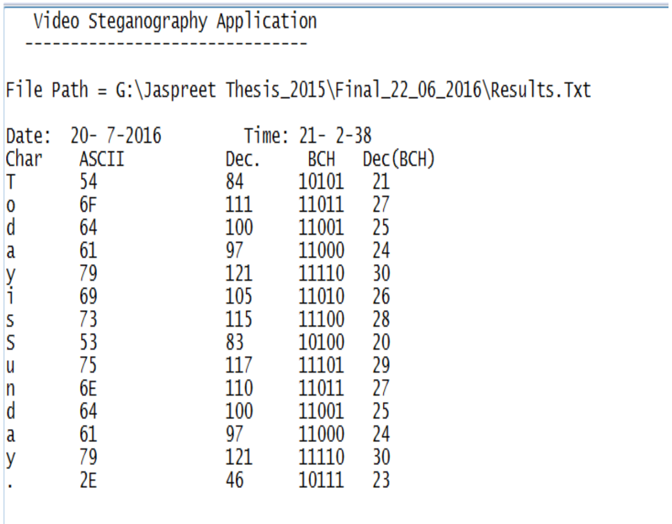


Today is Sunday.

Figure 4: Selected LL sub-band & Secret text message

Step 4. Encryption (BCH Codes) & Embedding Process

The secret text message is encrypted using BCH codes for more security. Apply the steganography algorithm to embed secret message.BCH code values are embedded into video cover frame instead of original text message to make a stego image.



```
    Video Steganography Application
   -------------------------------

File Path = G:\Jaspreet Thesis_2015\Final_22_06_2016\Results.Txt

Date:  20- 7-2016        Time: 21- 2-38
Char     ASCII           Dec.     BCH   Dec(BCH)
T        54              84      10101   21
o        6F              111     11011   27
d        64              100     11001   25
a        61              97      11000   24
y        79              121     11110   30
i        69              105     11010   26
s        73              115     11100   28
S        53              83      10100   20
u        75              117     11101   29
n        6E              110     11011   27
d        64              100     11001   25
a        61              97      11000   24
y        79              121     11110   30
.        2E              46      10111   23
```

Figure 5: Encryption of Secret Text Message

Step 5 . Replacement of Stego Image with Original Video

Get the resultant stego image and then replace this stego image with a frame of original video. Now convert gray stego image into RGB color image for replacement and to make stego video.

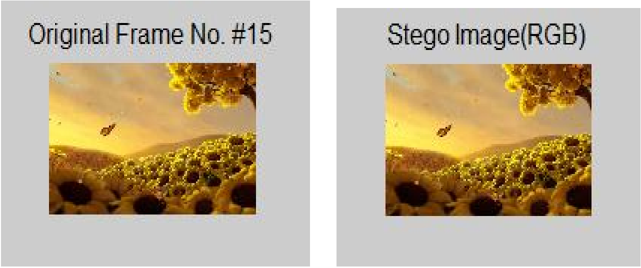


Figure 6: Comparision between Original & Stego Image

Step 6 . Get the resultant stego video

C. Extraction Process

The extraction process is totally the reverse process of the embedding process to retrieve the secret text message. To retrieve the hidden secret text message the following steps are considered:

The flowchart of extraction process is as follows:-

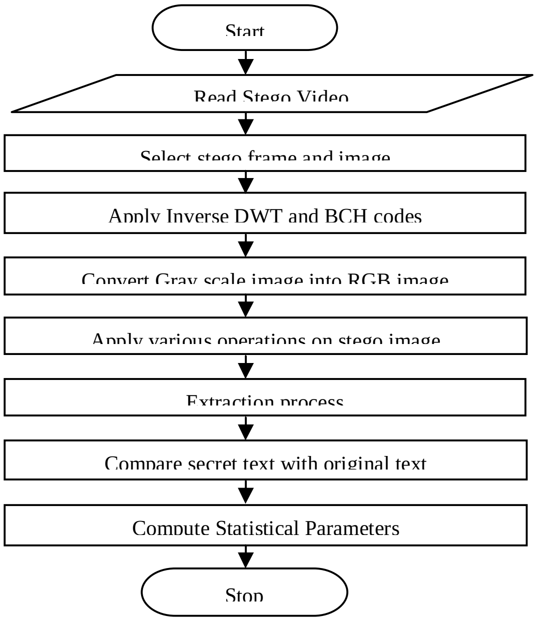

Start
Read Stego Video
Select stego frame and image
Apply Inverse DWT and BCH codes
Convert Gray scale image into RGB image
Apply various operations on stego image
Extraction process
Compare secret text with original text
Compute Statistical Parameters
Stop

Figure 7: Extraction Process

The steps for an algorithm are as follows:-

Step 1: Acquire the Stego video

Acquire stego video to take out the secret message hidden with the help of embedding process.Select stego frame to extract secret text message.

Step 2: Apply Inverse DWT and BCH codes

Apply the method to extract secret text message to the cover video frame and apply inverse haar wavelet transform on gray level image and BCH Decoder algorithm to recover the secret text message.

Step 3. Convert resultant Gray stego image to RGB Stego image.

After applying inverse Haar wavelet transform on gray level image.Convert gray level stego image into RGB stego image for message extraction.

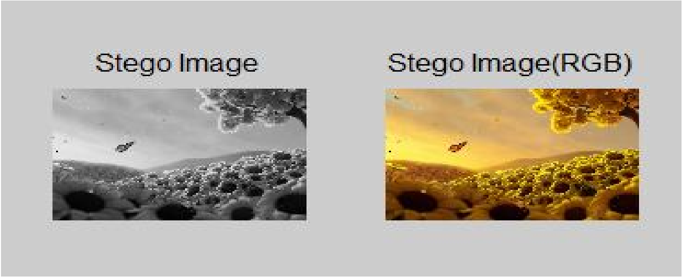


Figure 8: Conversion of Gray image to RGB

Step 4. Apply Various Operations on Stego Image

Apply various operations on RGB Stego image such as Crop, Zoom in, Zoom out and copy image to evaluate the robustness of video steganography algorithm.Secret text message can be extracted from Cropped image,Zoom In Image,Zoom Out Image and also from Copy Image.

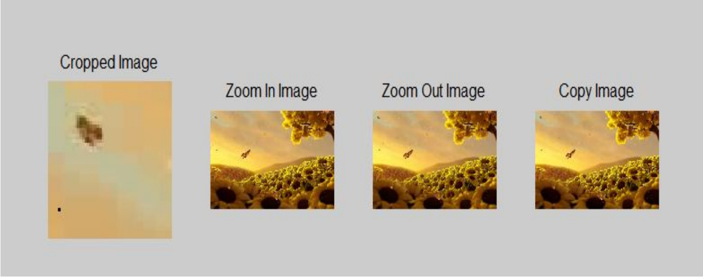
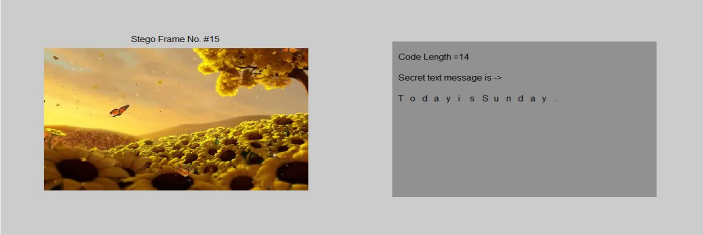


Figure 9: Operations performed on Stego image

Step 5: Compare secret text with original text

The secret text message is compared with the original text message. The extracted message of good quality is obtained either the message is extracted from cropped image, Zoom-in image, Zoom-out Image and from copy Image and increase the robustness of an algorithm.



Code Length =14

Secret text message is ->

Today is Sunday .

Figure 10: Message Extracted from Original Stego frame

Step 6: Compute Statistical Parameters

Compute statistical parameters like PSNR, MSE, SD and Variance for three different videos to check an algorithm's efficiency and robustness.

IV. EXPERIMENTAL RESULTS

A dataset of three dissimilar videos (Video 1, Video 2 and Video3) with the extension of Audio Video Interleave (.AVI) is used. Investigational results are accomplished by using the R2012a version of MATLAB software. To prepare results take each cover video's 50 frames. To check efficiency, visual quality or PSNR of the proposed algorithm is calculated. The frame number having highest value of PSNR is selected for embedding information. To check the robustness of this algorithm various attacks has been performed on stego image to achieve the good quality of secret message.The main purpose of Peak Signal to Noise Ratio (PSNR) metric is to measure the differentiation between the original and the hazy videos. The peak-signal to noise ratio (PSNR) was used to calculate the reconstructed image quality. The PSNR is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{N\times N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(f(i,j)-\hat{f}(i,j)\right)^2}dB,$$

Where N × N is the size of the original image and f(i,j) and ˆf(i,j) are the gray-level pixel values of the original and reconstructed images, respectively.

The PSNR parameter of Video 3 has improved the visual quality of all three stego videos enhanced than the other two Videos. On the whole, due to the high values of PSNR the proposed algorithm has superb visual qualities for stego videos.

Analysis of embedding and extraction process has been successfully implemented and results are delivered. The PSNR of video1, video2 and video3 are also compared. From the results it is observed that as PSNR in video3 is the best.

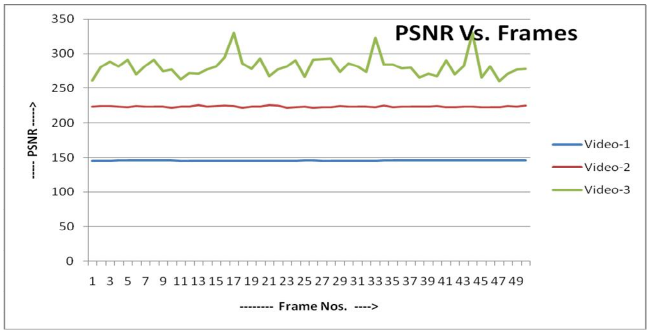


Figure 11: PSNR of three different Videos

So, It is observed that the frame number 41 from video 1(Water video) depicts the highest PSNR value, frame number 21 from the video 2 (Flowers video)and frame number 44 from the video 3(Candle video) will be selected for embedding and will give better visual qualities of stego videos while selecting the above mentioned frame numbers.

TABLE I Results of the proposed Algorithm

PARAMETERS	Water Video	Flowers Video	Candle Video
PSNR	145.833	226.303	330.118
MSE	44.712	0.802	0.004
SD	3.554	8.559	24.083
Variance	46.212	102.197	136.45

The performance of the proposed algorithm is determined with the help of above mentioned parameters.The quality of the proposed algorithm is checked with these statistical parameters. The lowest the value of MSE, SD and variance of an algorithm depicts the highest visual qualities of stego videos.

On the basis of analysis of experimental procedures of the proposed algorithm it is observed that the extracted information that is embedded through embedding process achieved the good quality and is compared with the original secret text message or information.

V. CONCLUSION AND FUTURE SCOPE

This work presents the video steganographic algorithm using haar wavelet and BCH codes. Secret message is embedded and extracted of any length; however, the processing time issue may arise if message length is more.So, the experimental results have demonstrated that the proposed algorithm has the highest embedding effieicncy or PSNR. The Robustness of this algorithm is verified against attacks. Attacks have been performed on stego image to achieve the good quality of secret message. The algorithm is tested rigorously in copy-paste, cut-paste, cropped Image, zoom-in and zoom-out image manipulation cases. The secret text message and original text message is compared in all four manipulated stego images.

The security, robustness and efficiency of this proposed steganography algorithm is enhanced by computing statistical parameters such as psnr,mse,standard deviation and variance that are applied to check the efficiency or visual quality of the stego videos.

In future, processing time dependency over the message length may be resolved by using appropriate algorithm,Investigation of embedding secret information in audio in future because video contains both images and audio & the future work can also be done on other video formats like .mpeg, .3gp etc.

REFERENCES

[1] Bharti Chandel1, Dr.Shaily Jain2. “Video Steganography: A Survey. Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17.
[2] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes." Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015.
[3] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)."Wireless Telecommunications Symposium (WTS), 2015. IEEE, 2015.
[4] Sensarma, Debajit, and Samar Sen Sarma. "Data Hiding using Graphical Code based Steganography Technique." arXivpreprintarXiv:1509.08743(2015)
[5] Singh, Kamred Udham. "A Survey on Image Steganography Techniques."International Journal of Computer Applications 97.18 (2014).
[6] Al-Frajat, A. K., et al. "Hiding data in video file: An overview." J. Appl. Sci10.15 (2010): 1644-1649