Comprehensive Study of Video Stegnography Algorithms  
Nehali Pawar¹, Kishor Pandyaji²  
M.E. Student¹, Associate Professor²  
Department of Electronics Engineering  
PVPIT, Budhgaon, Maharashtra, India

Abstract:
Video stegnography is an efficient method of data hiding in video file. The video stegnography techniques are useful in high security requirements. Secure video stegnography is a challenging task of sending the embedded information to the receiver without being detected. For hiding secret information in the video, there are many stegnographic techniques which are explained in this paper. The techniques such as video stegnography by LSB method, LSB revisited algorithm, LSB hybrid approach, non-uniform rectangular partition method and hamming code. The results of all this techniques are compared on the basis of parameters like visual quality, embedding payload, robustness. This paper provides effective review of existing video stegnography techniques and proposed the video stegnography based on BCH code in DWT domain may give better result than existing techniques.

Keywords: BCH code, Embedding payload, Hamming code, LSB method, security, Stego video, Video Stegnography.

I. INTRODUCTION
Stegnography is a Greek word which means the covered writing. Video stegnography is an art of hiding data in video media. The secret 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. Basic concept of video stegnography is shown in following diagram:

![Basic concept of Video Stegnography](image)

Several new techniques have been proposed for video stegnography. In this paper, some of the most well-known techniques have been discussed. 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 or DWT and then embedded in some or all of the transformed coefficients. Likewise 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
A. Video Stegnography using LSB matching revisited algorithm
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. First that cover video is splitted into the frames. Now, the secret message can be embedded into multiple frames. Then all stego frames are collected to form a stego video. In extraction process the original message get at receiver side. [2]
This proposed method in this paper was found 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. The PSNR value decreases on increase of the embedding unit [2].

B. Video Steganography through LSB based hybrid approach

In 2013, Hemant Gupta, Dr. Setu Chaturvedi presented a video steganography through LSB based hybrid approach. This method is used in AVI videos. The video is converted into 20 equal grayscale images. Data hiding is done in host video by using single bit, two bit, three bit LSB substitution and after that Advanced Encryption Standard (AES) Algorithm is applied. After processing the source video by using the data hiding procedures, the encrypted AVI Video is sent by the sender and decryption is performed by the receiver. They have found the PSNR for 1 bit LSB & 2 bit LSB & 3 bit LSB Substitution and AES method which discussed in comparative study of results. [3]

C. A highly secured method of video steganography by using hamming code (7, 4)

Ramadhan J. Mstafa and Khaled M. Elleithy, Senior Member, IEEE, Department of Computer science and Engineering, University of Bridgepor, proposed a highly secured method of video steganography by using Hamming Code (7, 4). In their project they propose a secure video steganography algorithm based on linear block code. Nine uncompressed video sequences are used as cover data and binary image logo as a secret message. At first, convert video stream in to number of frames and then separate each frame into Y, U and V components. Then by using a special key all pixels’s positions both cover video and secret message are randomly ordered. A binary image is used as secret image which was converted into 1-Dimentional array and the position of message is changed by a key. Now, 4 bits of message is encoded using Hamming Code (7, 4) encoding technique. Now, the encoded data is XORed with random values and result is added in Y, U and V components. The pixels are then reordered in their original position and final stego video is rebuilt from the stego frames. Exact opposite process is takes place in extraction process to get original message. [5] The data embedding and data extraction is shown in the following figures 5 and 6 respectively.
Likewise, the algorithm has high embedding efficiency as given by experimental results in this project. The visual quality of the system is decided by the Peak 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]

III. 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.

\[
MSE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} \sum_{k=1}^{K} (C(m,n,k) - S(m,n,k))^2}{MNK}
\]  

(1) [9]

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,

\[
PSNR = 10 \times \log_{10} \left( \frac{MAX_0^2}{MSE} \right)
\]  

(2) [9]

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,

\[
HR = \frac{\text{size of embedded message}}{\text{Video size}} \times 100\%
\]  

(3) [9]

C. Robustness

To evaluate the performance of video stegnographic algorithm for correctly retrieving the secret message, two objective metrics have been used: 1) the Similarity Function (SF) and 2) the Bit Error Rate (BER). Both parameters are used to test whether the extracted secret message has been corrupted during the communication. To achieve the robustness of the algorithm, the higher SF and the lower BER must be obtained. [9]

IV. COMPARATIVE STUDY

TABLE 1. COMPARATIVE STUDY BETWEEN EXISTING TECHNIQUES

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Video File</th>
<th>No. of Frames</th>
<th>Embedding Payload</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Stegno graphic using LSB matching revisited algorithm</td>
<td>Rhines.avi</td>
<td>105</td>
<td>136 bits</td>
<td>80 dB</td>
</tr>
<tr>
<td>Video Stegno graphic through LSB based hybrid approach</td>
<td>AVI video</td>
<td>20</td>
<td>set 1, set 2, set 3 each set contain 20</td>
<td></td>
</tr>
<tr>
<td>A Novel Video Stegno graphic based on Non-uniform Rectangular Partition</td>
<td>Uncompressed video in AVI format</td>
<td>150</td>
<td>Uncompressed video of 137 frames (15 frames/sec)</td>
<td>&lt;28 dB</td>
</tr>
<tr>
<td>A highly secured method of video stegnography by using hamming code (7,4)</td>
<td>Foreman.avi</td>
<td>300</td>
<td>16 Kbits</td>
<td>51-52.5 dB</td>
</tr>
</tbody>
</table>

V. CONTRIBUTION AND DISCUSSION

The results for various existing techniques are discussed above on the basis of two parameters like embedding payload and visual quality of the stego video. The visual quality of stego video is depends upon the PSNR value. For better visual quality it should be above 50 dB. The embedding payload is depends upon the size of the cover video or number of frames in video. The video stegnography technique is being implemented based on BCH code in DWT domain. In the transmitter section, secret message is get triple protection through encryption by key1, key2 and BCH encoding. The secret message is difficult to identify by unauthorized user. Therefore, system would be more robust than other proposed systems. The implemented transmitter section gave stego video which gives its visual quality and embedding payload. The PSNR value for this system is 65.28 dB for 53 frames. The value for MSE is 0.01924. The embedding payload for this is 3256 bits.

VI. CONCLUSION

In this paper, many video stegnographic techniques are discussed mainly: LSB matching revisited algorithm, LSB hybrid approach and video stegnography by hamming code. Also they compared on the basis of parameters such as visual quality of stego video and embedding payload in terms of hiding ratio. The proposed system is video stegnography by BCH code in DWT domain may give better result than existing techniques.

VII. REFERENCES


[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.