Video Steganography Using Pixel Intensity Value and LSB Technique

Dr.ManishShrivastava
Head of Department(CSE)
Institute of Technology,GGV
Bilaspur,CG,IndiaBilaspur,CG,India
email:manbsp@gmail.com

Richa Ranjanand, SushmitaKumari
B.Tech (Department of CSE)
Institute of Technology, GGV
richaranjan1193@gmail.com,
sushmitakumari363@gmail.com

***Abstract*—** Video Steganography is a method of hiding secret message inside video file. In this paper, LSB (least significant bit) technique has been used in order to conceal secret message in video file. LSB is a spatial domain technique. In this paper, we have proposed a new technique of embedding secret message on the basis of color intensity value of the RGB pixel of cover file. Color intensity is used because of the fact that low color intensity has less effect on the human eyes and is difficult to be detected. Secret message bits are embedded in alternate pixel in order to have less effect on the over quality of cover video file.

***Keywords**-components;Cover video; Dynamic LSB; secret video; Steganography; Video Steganography*

*****

I. INTRODUCTION

Steganography is hiding private or secret data within a carrier in invisible manner. It derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing) [1]. The medium where the secret data is hidden is called as cover medium, this can be text, image, video or an audio file. This method is same to digital signature and water marking techniques in few respects. [2], [3]anystego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By using lossless steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files.

Video based steganogrpahic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWTand then messages are embedded in some or all of the transformed coefficients.

Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack as described in [4] and [5]. This makes research fraternity interested in designing new methods.

In this paper, we propose a new technique for embedding secret message in video file. Color intensity value of the RGB pixel in the cover file is used to embed data. This is used due to the fact that lower intensity color has less effect on the human eyes and any modification made to it can easily go undetectable to the human eyes. Alternate pixel is used to embed secret message bits in order to have less distortion of the cover file.

The paper has following organization. Already done works in field of video steganography are kept in section 2. New proposed steganography is given in section 3. Evaluations of the proposed technique is done in section 4. Section 5 contain the performance evaluation of the technique. The paper ends with the conclusion and future scope in the field of the proposed technique.

II. RELATED WORK

This section gives a brief overview on the related work done on the video steganography using various different technologies.

A. Hiding Messages Using Motion Vector Technique In Video Steganography[6]:

In this paper, we proposed a new technique using the motion vector, to hide the data in the moving objects.The data is hided in the horizontal and the vertical components of the moving objects.

B. *Dynamic least significant bit technique for video steganography [7]:*

A dynamic LSB is a spatial domain technique where the secret information such as images, or video is embedded in the LSB of the cover movie (i.e. frames) by selecting number of bits to be embedded. The idea of the proposed method is take away the least significant pixels from one image (frame) which is in cover movie and uses them to store most significant pixels of second image (frame) which is in hidden movie. The hidden image's (frame's) values are stored in the result frame's least significant bits so they don't add greatly to the resulting combined video (movie).

C. *A Novel Image Steganographic Method UsingTri-way Pixel-Value Differencing [8]*:

To enlarge the capacity of the hidden secret information and to provide an imperceptible stego image for human vision, a novel steganographic approach using tri-way pixel-value differencing (TPVD) was proposed.To upgrade the hiding capacity of original PVD method referring to only one direction, three different directional edges are considered and effectively adopted to design the scheme of tri-way pixel-value differencing.

III. PROPOSED STEGANOGRAPHY TECHNIQUE

In order to increase the efficiency of our proposed video steganography technique, we first encrypt the secret message to be embedded so that it become nearly impossible for the third party to detect the original message.

A. *Bit Exchange method (Encryption)*

Simple bit exchange method is used here for encrypting our secret message. The following are the steps for encryption method.

- Step-1: One by one byte is read from the secret message and it is converted into its equivalent 8-bit value. Then each bit is shifted one bit right in order to get the new pattern for the secret message bits.
- Step-2: We then read 8 bits at a time and divide it into two blocks 4 bits each and then perform the XOR operations with 4-bits on the left side and 4 bits on the right side and substitute the new bits in right 4-bit positions. The same thing repeated for all bytes.
- Step-3: Repeat step-1 and step-2 until the entire secret message pixels have been encrypted successfully.

B. *Selection of pixels on the basis of intensity*

The basic idea behind this proposed method of video steganography is that the pixel whose color intensity value is low has less effect on the overall appearance of the picture in comparison of the high intensity color valued pixel.[9] One more advantage is that we can embed more no. of secret message bits in low color intensity valued pixel.

C. *Algorithm of LSB technique*

The proposed algorithm is given in this section. Embedding technique is given below:

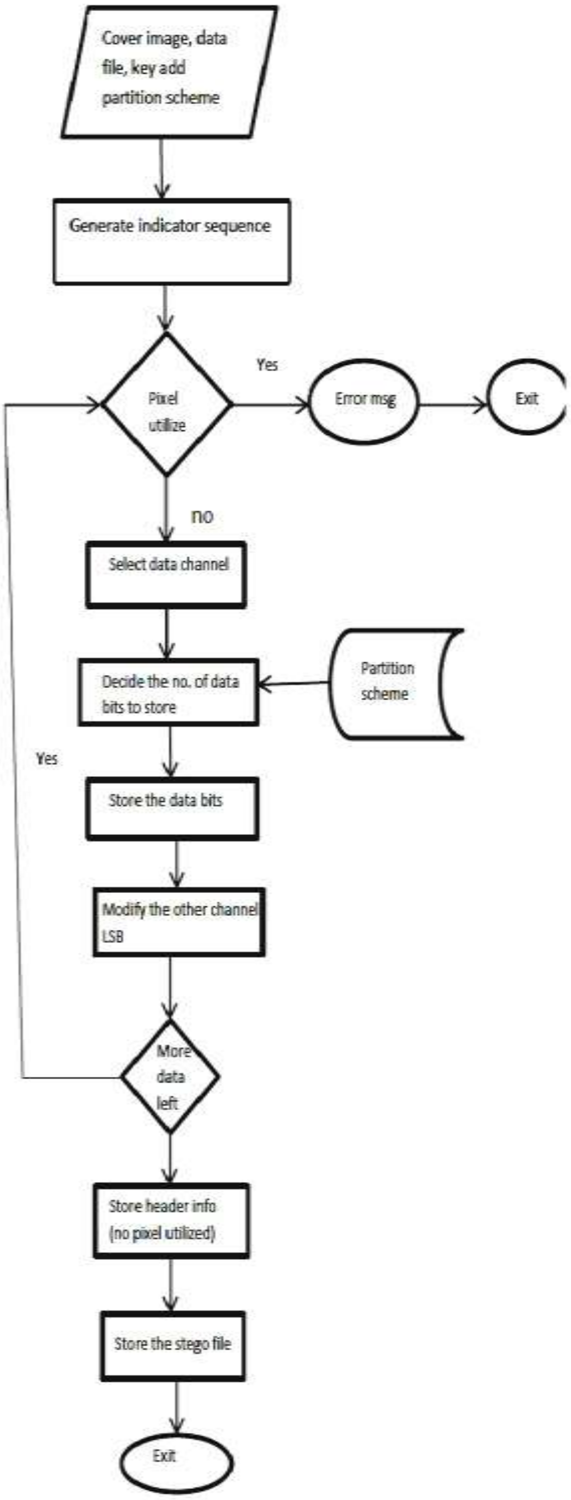
Input: cover video (AVI), hidden video (AVI).
Output: Stego video (AVI).
Step 1: Input is the cover file that is video in which we want to hide our secret message.

Step 2: The cover file is broken into frames.
Step 3: Find the pixel value of the broken frames.
Step 4: The RGB pixel whose color intensity value is low in comparison of its neighboring pixels is selected for embedding.
Step 5: Make sure that the RGB pixels are selected in alternate pattern.
Step 6: Break the secret message in its bit pattern.
Step 7: Now the embedding job is done. LSB position of RGB pixel is calculated.
Step 8: The last four bits of video frame pixel is replaced with the four bits of secret message.
Step 9: This process of embedding is continued until all the message bits have been successfully embedded in the cover file.
Step 10: Regenerate the video file. (stego file)

IV. EVALUTION OF THE PROPOSED TECHNIQUES

A. *LSB technique[10]*

The value of RGB pixel can be taken as follow:
R: 10110101 =181
G: 10010011 =147
B: 11001011 =203
and a RGB pixel value of message to be embedded in cover file is:


Cover image, data file, key add partition scheme
Generate indicator sequence
Pixel utilize
Yes
Error msg
Exit
no
Select data channel
Decide the no. of data bits to store
Partition scheme
Yes
Store the data bits
Modify the other channel LSB
More data left
Store header info (no pixel utilized)
Store the stego file
Exit

10000011 =131
000 10110= 22
01111101 =125

Now LSB substitution is done by replacing last four bits of cover frame RGB pixel by first four bits of the message bits.

R: 10110101(181) + 10000011(131) =10111000 (184)
G: 10010011(147) + 00010110(22) =10010001(145).
B: 11001011(203) + 01111101(125) = 11000111(199).

In same way we can do the embedding of entire message bits in the RGB pixels of carry video file.

Final video file after embedding of secret message is called as stego file.

Cover red + hidden message bitsLSB --> Stego red.
Cover green + hidden message bitsLSB --> Stego green.
Cover blue + hidden message bitsLSB --> Stego blue.

B. *Pixel selection on the basis of intensity values*

We propose the following algorithm.

- Three pixels are selected and used as channel. One of them acts as indicator based on its value the other pixel is compared.
- Message is stored in one of the two channels other than the indicator. The channel whose color value change is little is selected to embed the final secret message in least significant bit.
- Instead of storing the message in continuous pixel, alternating pixels are selected so that the changes made in the overall appearance of cover file is less observable. Through experimentations, we show that optimal partition may depend on the actual cover image used.

V. PERFORMANCE EVALUATION

The performance of any steganography technique is evaluated on the basis of its attributes. Two important attributes that characterizes the overall behaviorof any steganography are imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). Various methods are used to detect the imperceptibility of steganography file. Such as the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) to compare between cover video and stego video and also between hidden video and recover video calculated below

$$\text{MSE}= 1/(H * W)\sum_{i=1}^{H}(P(i,j) - S(i,j)) \qquad (1)$$

Where, MSE is Mean Square error, H and Ware height width and P(i,j) represents original frame and S(i,j) represents corresponding stego frame.

$$PSNR = 10\log_{10} L^2/MSE \qquad (2)$$

Where, PSNR is peak signal to noise ratio.L is peak signal level for a grey scale image it is taken as 255.

The value is calculated for every RGB and after that average value is calculated to get the estimation of entire pixel value.

Every data hiding process in video file is based on the following three important factors of cover medium:

- Capacity
- Security
- Robustness

Capacity refers to the amount of information that can be hidden in the cover medium without affecting its original characteristics.

Security is defined as an inability of the third person from getting the secret message without authentication.

Robustness refers to the amount of modification that can be done without having any adverse effect on the overall characteristics of the cover file.

VI. CONCLUSION AND THE FUTURE WORK

In this paper, we introduce a new idea in video based steganography, where secret message bits are embedded in the cover file by using LSB technique. For embedding, the selection of cover file RGB pixels is done on the basis of its color intensity value.

LSB technique is used to embed bits in the cover file. This approach leads to very high capacity with low visual distortions.

There are several ways to improve this algorithm:

- Variable length embedding can be done in order to increase the imperceptibility of the cover medium.
- For the selection of lower intensity based pixels number of channels used can be increased for getting more accurate result.

REFERENCES

[1] E. Cole and R.D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.

[2] I. J. Cox, J. Bloom, M. Miller, and I. Cox, *Digital Watermarking: Principles & Practice*. New York: Morgan Kaufmann, 2001.

[3] Y. Wu and F. Y. Shih, “An adjusted-purpose digital watermarking technique,” *Patt. Recognit.*, vol. 37, no. 12, pp. 2349–2359, Dec. 2004.

[4] A. Westfield, and A. Pfitzmann, Attacks on Steganographic Systems, in Proceedings of 3rd Info. Hiding Workshop, Dresden, Germany, Sept. 28−Oct. 1, pp. 61-75, 1999.

[5] J. Fridrich, R. Du, and L, Meng, Steganalysis of LSB Encoding in Color Images, in Proceedings of ICME 2000, Jul.-Aug. 2000, N.Y., USA.

[6] Hiding Messages Using Motion Vector Technique In Video Steganography P. Paulpandi1, Dr. T. Meyyappan, M. sc., M.Phil.,M.BA., Ph.D Research Scholar1, Associate professor Department of Computer Science & Engineering,AlagappaUniversity,Karaikudi.Tamil Nadu,India

[7] Dynamic least significant bit technique for video steganography ,Wafaahasanalwan

[8] A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing Ko-Chin Changa, Chien-Ping Changa, Ping S. Huangb, and Te-Ming TuaaDepartment of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 335, Taiwan, R.O.C.

[9] Pixel indicator high capacity technique for RGB image based steganography.AdnanGutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, AbdulrahmanShaheen, AleemAlviComputer Engineering Department, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia

[10] Dynamic least significant bit technique for video steganographyي وي دف لاءاف خلالةي ك يماذ يدلاةي مهال قلاات بلاةي نق تWafaahasanalwanComputer image processing/ Law college, Karbala university