ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

An Efficient Modified LSB technique for Video Steganography

Maninder Pal Singh[1], Harmandeep Singh[2]

Research Scholar, Dept. of ECE, GIMET, Amritsar, Punjab, India [1]

Assistant Professor, Dept. of ECE, GIMET, Amritsar, Punjab, India [2]

ABSTRACT: Video Steganography is a process of hiding secret information inside a video. This paper aims to provide an efficient, high capacity and a secure technique for video steganography. In this paper different images hides in different frames using proposed Modified LSB technique. The proposed technique is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared with original cover video as well as the Mean Square Error (MSE) measured between the original and steganograhic files averaged over video frames. Experimental results shows that proposed Modified LSB technique have better MSE, PSNR as compared to existing Modified LSB technique.

KEYWORDS: Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Modified Least Significant bit (MLSB), Video Steganography, and secret message.

I. INTRODUCTION

With the increasing rate of unauthorized attacks, unwanted access and security issues. It is more important to secure our data from hackers or any other unwanted accesses. While in Cryptography, it’s only encrypts the data but when communication takes place in presence of third party, the encrypted text can be decrypted and can be easily destroyed. While in Steganography, it hides the confidential data in some cover source in such a way that the existence of the data or any type of information is also hidden which do not detect any suspicion regarding the communication takes place between two parties [1].

Steganography is an art and science of hiding information in some cover media. The word steganography is derived from the Greek words “stegos” means “cover or protected” and “graphei” means “writing” defining it as “concealed writing or covered writing” [2].

TYPES OF STEGANOGRAPHY [3]

1. **Text Steganography**: It consists of hiding the information in the text files. In this Text Steganography, the secret data is hidden behind every nth letter of every word of text message. There are numbers of methods are available for hiding data in text file. Such of these method are:

   i. Format based Method

   ii. Random and Statistical Method

   iii. Linguistics Method

2. **Image Steganography**: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography, the pixel intensity is used to hide the data. In digital steganography, images are taken as a cover source because there are number of bits presents in digital representation of an image.
   Simply a digital image, which described using a 2-D matrix of the color intensity at each grid point (i.e. pixel). Generally, a gray scale images uses 8 bits, whereas at the other side color image uses 24 bits to describe the color image, which is known as RGB image.

3. **Audio Steganography**: It involves hiding data in an audio files. This method hides the data in WAV, AU, and MP3 sound files. There are different methods of audio steganography. These method are:
   i. Low Bit Encoding

ii. Phase Coding

iii. Spread Spectrum

4. **Video Steganography**: It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding data. Generally discrete cosine transform (DCT) alter the values which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, mp4, MPEG, AVI is the formats used by video steganography.

STEGANOGRAPHY TECHNIQUES

There are several techniques to conceal information inside cover image [4].
1. Spatial domain technique
2. Frequency domain technique

1. **Spatial Domain Technique**: These techniques manipulate the cover image bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes.

2. **Frequency Domain Technique**: The transform domain techniques embed the message in the frequency domain of the cover image.

II.LITERATURE SURVEY

In the literatures, amount of steganography technique for digital images and videos have been proposed.

1. Samidha et.al [5], the paper describes various image steganography techniques, based on spatial domain and by considering pixel values in binary format. Spatial domain based on physical location of pixels in an image. Generally 8 bit gray level or color images can be used as a cover to hide data. Again binary representations of these pixels are considered to hide secret information. Random bits from these bytes are used to replace the bits of secret. For the above purpose to be achieved, many parameters of an image are considered like physical location of pixels, intensity value of pixel, etc.
2. Mohd et. al [6], the Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for steganography, and thus the importance of image steganography. Embedding secret information inside images requires intensive computations, and therefore, designing steganography in hardware speeds up steganography. In this presents a hardware design of Least Significant Bit (LSB) steganography technique in a cyclone II FPGA of the Altera family.
3. Pooja et.al [7], suggest that the video is simply a sequences of images; hence much space is available in between for hiding information. In proposed scheme video steganography is used to hide secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8 bit binary values, and encrypted using XOR with secret key and encrypted frames using sequential encoding of cover video. To enhance more security each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR.

In this paper motivation is taken from ref. [5, 6, and 7] and used modified LSB technique for data hiding. This technique has better MSE and PSNR as compared to existing MLSB technique and also large capacity as compared to LSB.

III.PROPOSED METHODOLOGY

In this section explained Modified LSB technique transmitter as well as their receiver part. The description of transmitter block diagram as follows:

DOI: 10.15662/ijareeie.2015.0406062

1. **Cover Object**: Firstly a video file is read. Video is in any format like avi, mp4. The video consists of audio as well as images. On both parameter work can be done so according to requirement video information is extracted. In this block diagram frames information is collected like their:

a) Number of frames
b) Height
c) Width
d) Frame per second

After that frames extracted from video but for embedding of data only few frames required so some frames are selected on which data to embed.

2. **Secret Message**: The secret message in any format like images, audio, video or text. In this paper, image is used as secret message to hide.
3. **Stego Object**: To generate stego object modified LSB technique is applied on cover as well on message to hide the message in cover object. In this paper, stego frame is generated after hiding the color image inside it using modified LSB technique.

The stego frame again combine with other frames to make again video.

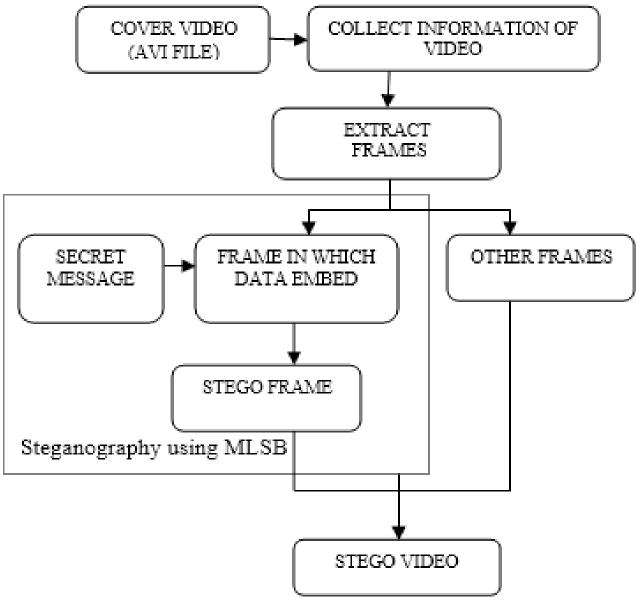

Fig.1 Block Diagram of Steganography

The description of receiver block diagram as follow in Fig. 2. For extracting the original message from Stego video at receiver side the stego video and cover video file is read and collected frames information then extract those frames on which data is hidden. Then Extracting algorithm is applied on selected frame to extract the original message from frames [8-12].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

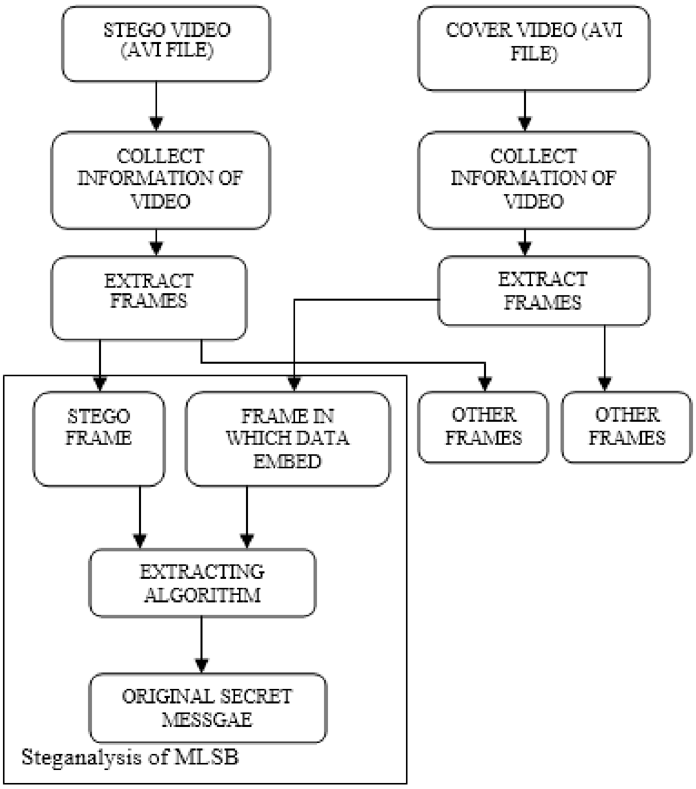

Fig.2 Block Diagram of Steganalysis

IV. SIMULATION RESLUTS

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar or different the stego image with cover image.
The following metrics are used:

1. **Mean Squared Error (MSE)** is computed by performing byte by byte comparisons of the cover image and stego image. The Computation expressed as [8]

$$\mathrm{MSE}=\frac{1}{M*N}\sum_1^M \sum_1^N (Fij - Gij)^2$$

M: numbers of rows of cover image
N: number of column of Cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image
Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. **Peak signal to noise ratio (PSNR)** measures in decibels the quality of the stego image compared with the cover image. Simply higher the PSNR which means better quality. PSNR is computed using the following equation [8].

$$\mathrm{PSNR}=20\log_{10} 255 - 10\log_{10} MSE$$

The cover file videos details are given in Table 1 are taken from MATLAB demo videos. The results are tabulated in Table 2 and 3.

Table 1: Cover Video File Details

Cover Video File Information				**Secret Message Resolution**
Name of Video File	**Resolution**	**Frames/sec**	**No. of Frames**	
Viptraffic.avi	160*120	15	120	40*30
Cat_video.avi	160*120	30	241	40*30
Scenevideoclip.avi	160*120	15	92	40*30
Shaky_car.avi	320*240	30	132	80*60
Atrium.avi	640*360	30	431	160*90

Table 2: Proposed Comparison in MSE & PSNR

	MSE	**PSNR**
Viptraffic.avi	0.27	47.85dB
Cat_video.avi	0.32	47.80dB
Scenevideoclip.avi	0.29	47.83dB
Shaky_car.avi	0.31	47.81dB
Atrium.avi	0.31	47.81dB

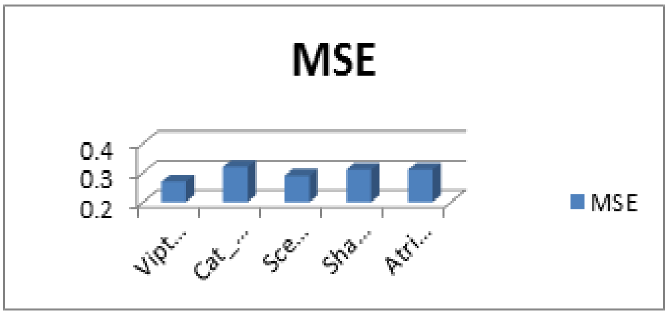

Fig. 3: Histogram for MSE

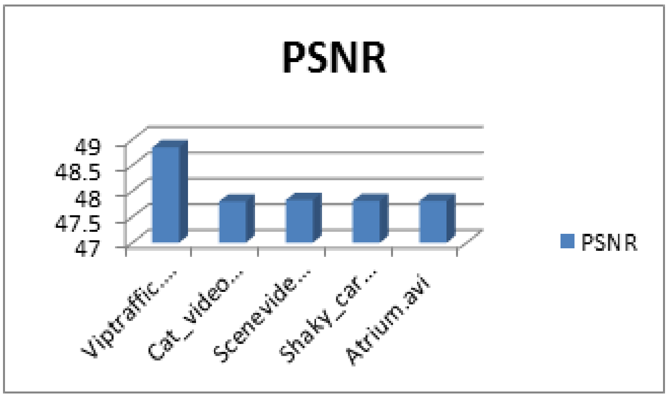

Fig.4: Histogram for PSNR

Table 3: Comparison between Existing and Proposed Results

Parameters	**Existing Results[4]**	**MLSB Technique Results**
Mean Square Error	2.4	0.27-0.31
Peak Signal to Noise Ratio	44.1 dB	47.80-47.85dB

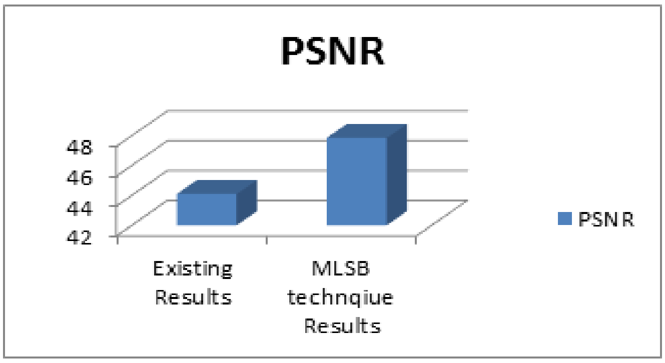

Fig.5: Histogram for PSNR compare with existing results

In Payload Capacity, maximum payload (bits per byte/bpb) for the technique has also been obtained i.e. the maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. In the proposed scheme the total number of eight bit of data are embedded in 2 pixels of the cover frame as shown in Table 4.

Table 4: Payload Capacity

Capacity	**LSB Results**	**MLSB Technique Results**
Payload Capacity	8	4

V. CONCLUSION

The MLSB approach is used to Embed of secret image into the meaningful cover frame of any type of video files. In this paper, taken different videos and hide data. The MLSB technique has better hiding capacity as compared to LSB and better MSE and PSNR as compared to existing MLSB technique.

REFERENCES

[1] Gunjan Chugh, Rakkumar Yadav and Ravi Saini, “A New Image Steganographic Approach based on Mod Factor for RGB images”, International Journal of Signal Processing and Pattern Recognition, vol.7, pp. 27-44, 2014.

[2] Rohit G Bal, Dr. P Ezhilarasu, “An Efficient Safe and secured Video Steganography Usinng Shadow Derivation”, International Journal of Innovative Research in Computer and Communication Engineering, vol.2, pp. 3251-3258, March 2014.

[3] Jasleen Kour, Deepankar Verma, “Steganography Techniques- A Review Paper ”, International Journal of Emerging Research in Management and Technology, vol.3, pp. 132-135, May 2014.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

[4] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh and Sahel Alouneh, "FPGA hardware of the LSB Steganography", International Conference on Computer, Information and Telecommunication Systems (CITS), Pages 1-4, 2012.

[5] Dr. Diwedi Samidha, Dipesh Agrawal, "Random Image Steganography in Spatial Domain", International Journal of Computer Science and Information Security, Volume 7 No. 3, March 2013.

[6] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh and Sahel Alouneh, "FPGA hardware of the LSB Steganography", International Conference on Computer, Information and Telecommunication Systems (CITS), Pages 1-4, 2012.

[7] Yadav Pooja Mishra, N. Sharma S, "A secure video steganography with encryption based on LSB technique", IEEE International Conference on computational Intelligence and Computing Research, vol 1, pp. 26-28, December 2013.

[8] Kousik Dasgupta, J.K Mandal and Paramarth Dutta, "Hash based Least Significant Bit Technique for Video Steganography", International Journal of Security, Privacy and Trust Management, vol.1, April 2012.

[9] N. F Johnson and S. Jajodia, "Steganalysis of images created using current steganography software", in Lecture notes in computer science, vol. 1525, pp.32-47, springer verlag, 1998.

[10] S. Dumitrescu, X. Wu and N. Menon, "On steganalysis of Random LSB embedding in continuous tone images", processing of the international conferences on image processing, vol. 3, pp. 641-644, June 2002.

[11] J. Fridrich, M. Goljan, D. Hogea and D. Soukal, "Quantitative Steganalysis of Digital Images: Estimating the Secret Message Length," in ACM Multimedia Systems Journal, Special issue on Multimedia Security, vol. 9, no. 3, pp. 288 – 302, 2003.

[12] U. Budia, D. Kundur and T. Zourntos, Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain, in IEEE Transactions on Information Forensics and Security, vol. 1, no. 4, pp. 502 – 516, December 2006.

[13] K. Kancherla and S. Mukkamala, Video Steganalysis using Spatial and Temporal Redundancies, in Proceedings of International Conference on High Performance Computing and Simulation, pp. 200–207, June 2009.