HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGONAGRAPHY(HLSB)

Kousik Dasgupta[1], J.K. Mandal[2] and Paramartha Dutta[3]

[1]Department of CSE, Kalyani Govt. Engineering College, Kalyani-741 235, India

kousik.dasgupta@gmail.com

[2]Department of CSE, Kalyani University, Kalyani-741 235, India

jkm.cse@gmail.com

[3]Department of CSS, Visva-Bharati University, Santiniketan-731 235, India

paramartha.dutta@gmail.com

ABSTRACT

Video Steganography deals with hiding secret data or information within a video. In this paper, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. The proposed method is analyzed in terms of both Peak Signal to Noise Ratio ($PSNR$) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic video file. The proposed technique is compared with existing LSB based steganography and the results are found to be encouraging. An estimate of the embedding capacity of the technique in the test video file along with an application of the proposed method has also been presented..

KEYWORDS

Steganography, Video Steganography, cover video, cover frame, secret message, LSB

1.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 image, video or an audio file. Any stego 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 [2]. 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 [3, 4]. 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 DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. The secret data is inserted in Least Significant Bits (LSB) of the intensity pixels of the video. Various techniques of LSB exists, where [5] proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. Whereas in [6] selected LSB steganography algorithm is proposed. Various other techniques exist in literature [7, 8]. In literature other than the LSB techniques some other methods also exit in spatial domain such as motion vector and linear code [4] and specific algorithms for compressed video streams [3].

In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI file as a cover medium. The results obtained are significant and encouraging.

The rest of the paper is arranged as follows, section 2 described the proposed video steganographic technique. The algorithm is proposed in section 3 with an application of it in AVI carrier file. Section 4 gives results and performance evaluation with other LSB technique. Conclusion and future work are presented in Section 5.

2.PROPOSED TECHNIQUE

The technique is a Hash based Least Significant Bit technique for Video Steganography has been proposed. The flow diagram of the same is given in Figure 1.

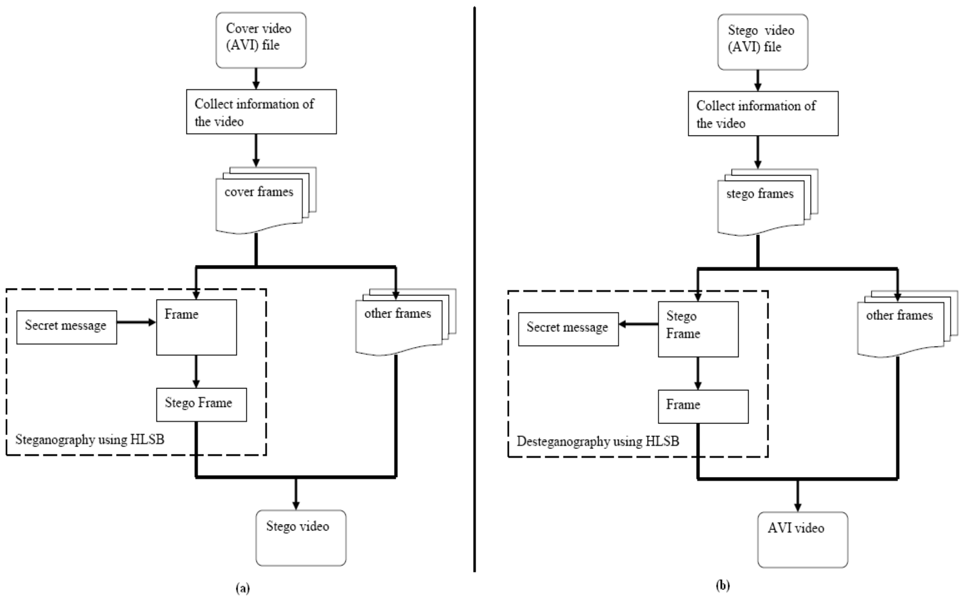

Figure 1. Block diagram of HLSB Video Steganography technique (a) Encoding and (b) Decoding

A video stream (AVI) consists of collection of frames. To ensure security the secret data is embedded in these frames as payload. The information of the cover video (AVI) such as number of frames (n), frame speed (fp/sec), frame height (H) and width (W) are extracted from the header. The video is broken down into frames. Proposed LSB based technique is used to conceal the data in the carrier frames.

Eight bits of secret data is considered at a time and concealed in LSB of RGB pixel value of the carrier frames in 3, 3, 2 order respectively. The detailed technique has been depicted in Figure 2. This distribution pattern is taken because the chromatic influence of blue to the human eye is more that red and green pixel. Thus the quality of the video is not sacrificed but we could increase the payload. Also this small variation in colours in the video image would be very difficult for the human eye to detect.

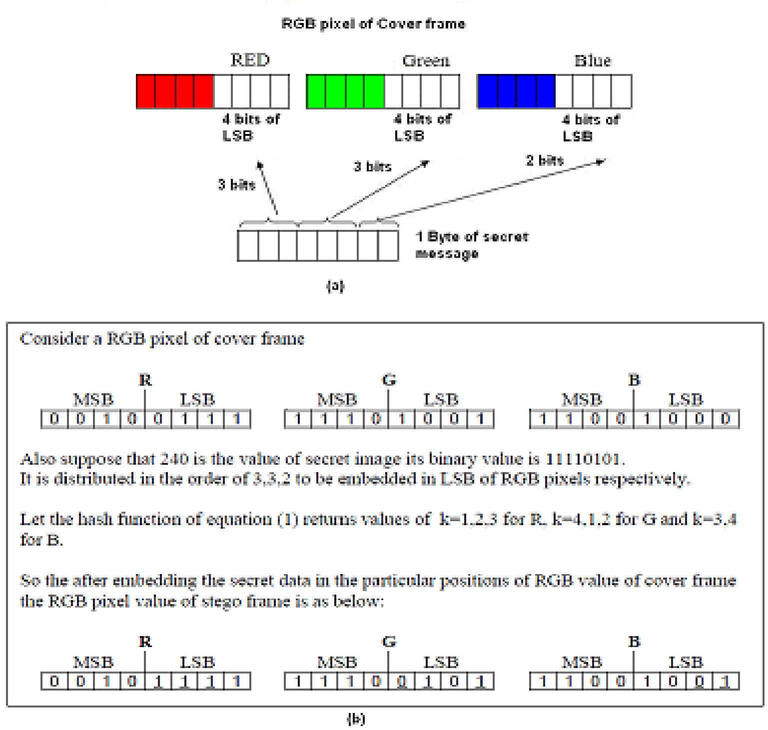

Figure 2. Proposed hash based LSB embedding technique (a) shows secret data embedded in 4 bits of LSB in 3,3,2 order in corresponding RGB pixels of carrier frame and (b) example of embedding of bits using hash function

The embedding positions of the eight bits within four (4) bits of LSB is obtained using a hash function of the form,

$$k = p\%n \qquad (1)$$

where, k is LSB bit position within the pixel, p represents the position of each hidden image pixel and n is number of bits of LSB which is 4 for the present case.

The bits are distributed randomly during fabrication which increases the robustness of the technique compared to other LSB based techniques [5, 6]. After concealing data in multiple frames of the carrier video, frames are then grouped together to form a stego video, which is now an embedded video to be, used as normal sequence of streaming.

The intended user follows the reverse steps to decode the secret data. During decoding the setgo video is again broken into frames after reading the header information. Using the same hash the data of the secret message is regenerated. The extracted stream of the secret information is used to authenticate the video. The algorithm of the proposed technique has been outlined in section 3.

3. ALGORITHM OF HLSB WITH AN APPLICATION

The proposed algorithm, both for encoding and decoding along with application are given in this section. Encoding technique is given in section 3.1 whereas decoding technique is given in section 3.2. Application of the proposed technique is given in section 3.3.

3.1. Algorithm of Encoding

Step 1: Input cover video file or stream.

Step 2: Read required information of the cover video. Step 3: Break the video into frames.

Step 4: Find 4 LSB bits of each RGB pixels of the cover frame.

Step 5: Obtain the position for embedding the secret data using hash function given in equation 1.

Step 6: Embed the eight bits of the secret image into 4 bits of LSB of RGB pixels of the cover frame in the order of 3, 3, 2 respectively using the position obtained from step 5.

Step 7: Regenerate video frames.

3.2. Algorithm of Decoding

Step 1: Input stego video file or stream.

Step 2: Read required information from the stego video. Step 3: Break the video into frames.

Step 4: Find 4 LSB bits of each RGB pixels of the stego frame.

Step 5: Obtain the position of embedded bits of the secret data using hash function given in equation 1.

Step 6: Retrieve the bits using these positions in the order of 3, 3, 2 respectively. Step 7:

Reconstruct the secret information.

Step 8: Regenerate video frames.

3.3. Application of HLSB technique

An application of the proposed algorithm with a test video (drop.avi) has been shown in figure 3. It shows a carrier video (drop.avi) and a secret image (message.png) and after steganography the output stego file is as given in drop-s.avi. On decoding the secret message (message.png) is obtained back without any loss or noise. The quality of the secret data can be analyzed by using the Peak Signal to Noise Ratio (PSNR) value of original secret image and image. The value of Mean Square Error (MSE) comes infinity (∞), meaning that the two images are identical.

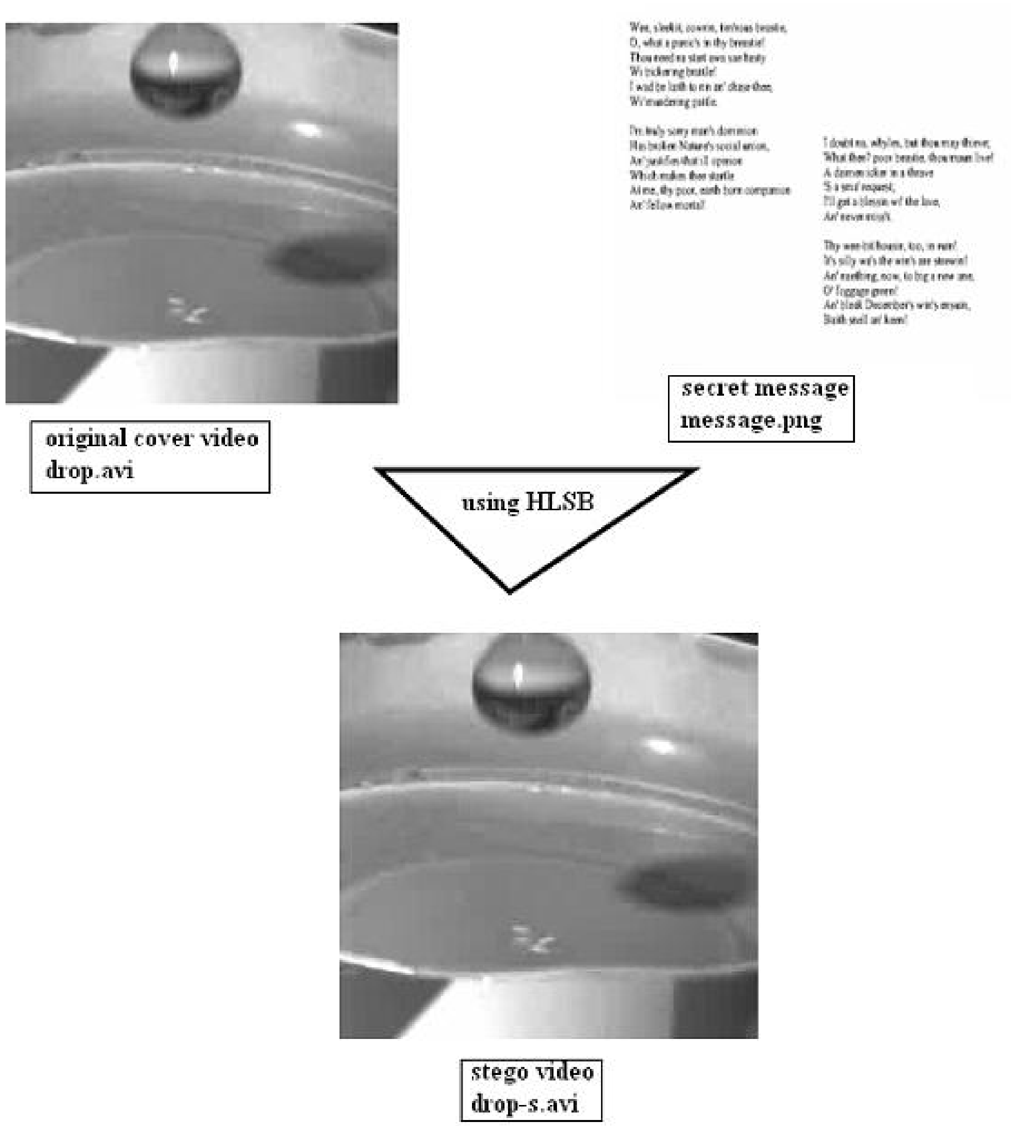

Figure 3. Application of the proposed HLSB technique

4. RESULTS AND PERFORMANCE EVALUATION

Any Steganography technique is characterized mainly by two attributes, imperceptibility and capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility). The performance of the proposed technique is evaluated using three different video streams (drop.avi, flame.avi and american football.avi) and one secret data (message.png).

The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined.

Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) between the stego frame and its corresponding cover frame are studied. The quantities are given as below,

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i, j) - S(i, j))^2 \tag{2}$$

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

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \tag{3}$$

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

Maximum payload (bits per byte/bpb) for the technique has also been obtained i.e. maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. In the proposed scheme eight bits of data are embedded in 3 pixels of the cover frame.

The cover file video details are given in Table 1 and results are tabulated in Table 2.

Table 1. Cover Video File details.

S.No	Cover video file information				Secret message Resolution W_1 *H_1
	Name of video file	Resolution (W*H)	Frame /sec.	No. of frames	
01	drop.avi	256 * 240	30	182	640 * 480
02	american football.avi	176 * 184	30	455	
03	flame.avi	256 * 240	30	294	

Table 2. Results obtained from HLSB and LSB techniques

the video file	Results obtained using HLSB				Results obtained using LSB			
	PSNR	Avg. MSE	IF	Payload (bpB)	PSNR	Avg. MSE	IF	Payload (bpB)
drop.avi	44.34	0.34	0.23	2.66	48.56	0.42	0.32	1
american football.avi	45.67	0.34	0.25	2.66	52.34	0.52	0.34	1
flame.avi	42.66	0.34	0.35	2.66	48.56	0.38	0.38	1

5. CONCLUSION

A secured hash based LSB technique for video steganography has been presented in this paper. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Performance analysis of the proposed technique after comparison with LSB technique is quite encouraging. A software based Steganographic Engine for video steganography is the future scope of the technique.

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] Stefan Katzenbeisser and Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 1999.

[3] D. Stanescu, M. Stratulat, B. Ciubotaru, D Chiciudean, R. Cioarga and M. Micea, Embedding Data in Video Stream using Steganography, in 4th International Symposium on Applied Computational Intelligence and Informatics, SACI-2001, pp. 241-244, IEEE, 2007.

[4] Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.

[5] Mritha Ramalingam, Stego Machine Video Steganography using Modified LSB Algorithm, in World Academy of Science, Engineering and Technology 74 2011, pp. 502-505, 2011.

[6] Juan Jose Roque and Jesus Maria Minguet, SLSB: Improving the Steganographic Algorithm LSB, in the 7th International Workshop on Security in Information Systems (WOSIS 2009), Milan, Italy, pp.1-11, 2009.

[7] Hema Ajetrao, Dr.P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images,in International Conference on Computational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.

[8] A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas, Data Hiding in Video in International Journal of Database Theory and Application Vol. 2, No. 2, pp. 9-16, June 2009.

Authors

Kousik Dasgupta did his Bachelors in Engineering in Electronics and Power Engineering from Nagpur University, Nagpur, India in 1993. Subsequently, he did his Masters in Computer Science & Engineering in 2007 from West Bengal University of Technology, Kolkata, India. He is currently Assistant Professor in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He served industries like ABB and L & T during 1993-1996. He is co-author of two books and about 10 research publications. His research interests include soft computing,
computer vision and image processing and steganography. Mr,. Dasgupta is a Life Member of ISTE, India, Associate Member ofthe
Institute of Engineers, India and Chartered Engineer [India] of The Institute of Engineers, India. He is a Fellow of OSI. India.

Jyotsna Kumar Mandal, M. Tech.(Computer Science, University of Calcutta), Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in omputer Science and Engineering, University of Kalyani, India. Life Member of Computer Society of India since 1992 and life member of Cryptology Research Society of India. Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 25 years of teaching and research experiences. Eight Scholars awarded Ph.D., one submitted and 8 are pursuing. Total number of publications is more than two hundred.

Paramartha Dutta did his Bachelors and Masters in Statistics from Indian Statistical Institute, Kolkata, India in 1988 and 1990, respectively. Subsequently, he did his Masters in Computer Science in 1993 from Indian Statistical Institute, Kolkata, India. He did his Ph.D. in 2005 from Bengal Engineering and Science University, Shibpore, India. He is currently a Professor in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He was an Assistant Professor and Head of the Department of Computer Science and Engineering of College of Engineering and Management, Kolaghat, India during 1998–

2001. He has served as a Research Scholar in the Indian Statistical Institute, Kolkata, India and in Bengal Engineering and Science University, Shibpore, India. He is a co-author of four books and about 120 research publications. His research interests include evolutionary computing, soft computing, pattern recognition, multiobjective optimization and mobile computing. Dr. Dutta is a Fellow of OSI, India. He is the member of ISCA, CSI, IETE, India and IAENG, Hong Kong.