Progress Report on Ph.D work, as on 6.1.2014

Design and Implementation of Steganographic Engine for Secret Data Sharing and Authentication of Videos: An Overture

Kousik Dasgupta
Dept. of CSE, Kalyani University

Abstract

Steganography is the act of hiding a message inside a container in such a way that can only be detected by its intended recipient. The container can be of different types text, image, audio and video. With the explosion of Internet and reach multimedia content, use of video as a container has become topic of interest for the research fraternity. Though, with the use of internet it has become more vulnerable to interception by unauthorized people over the world. One of the solutions to overcome these issues is cryptography, but the information secrecy does not exist any more. As hiding data is for confidentiality, the work focuses on the utilization of digital video as cover to hide data and maintaining confidentiality. Digital video used as cover can be said to be collection of frames and audio. Frames obtained can be of different types, I, B and P frames, each of them containing varied range of information. The message can be hidden in both frames and audio parts. In the present context frames are used as container, further each frame can be said to a collection of pixels or information.

The techniques used for video steganography can be differentiated as Spatial domain, Transform Domain, Linear Motion estimation etc. In the present work some spatial domain techniques are discussed. Further in spatial domain the information can be embedded in Least Significant Bit (LSB) or Most Significant Bit (MSB) of the pixel of each frame. LSB based techniques for embedding has been reported, as LSB techniques are prone to Steganalysis attack. This issue is taken care by applying a hashing function over the base LSB technique.

Any steganographic scheme can be said to be govern by mainly two factors imperceptibility and embedding capacity. Genetic Algorithm (GA) as an optimization tool for providing imperceptibility is reported. Use of GA also allows embedding in higher order bits thus in a way improving the embedding capacity. The reported works are compared with some existing schemes and results reported.

Keywords: Steganography, Video Steganography, Spatial domain, LSB and MSB, Hash, Genetic Algorithm

1. Existing Work

Literature survey suggests use of frequency and spatial domain techniques for Video steganography: Patel K et.al. [1] proposes use of a Lazy Lifting Wavelet transform to first transform the video and then apply LSB in the sub-bands of the obtained video for encoding.

Thakur V and Saikia, M. [2] proposes a procedure for embedding the secret message in DCT higher order coefficients of AVI videos.

Kelash, H.M. et.al. [3] proposed steganography algorithm based on color histograms for data embedding into Video clips directly. Each pixel in video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel.

Whereas Niu Ke and Zhong Weidong [4] proposes an information hiding scheme compatible with H.264 baseline is proposed. The scheme takes into account the features of Context Adaptive Variable Length Coding (CAVLC) which is used in H.264 baseline entropy coding. By modifying trailing ones sign flag and levels' words in CAVLC embeds the secret information.

Gujjunoori, S. and Amberker, B.B. [5] proposes a reversible data embedding scheme for MPEG-4 video which embeds the data into middle frequency coefficients of quantized DCT blocks and use HVS based visual quality metrics.

S. Suma [6] proposed an integer wavelet transformation in cover video so as to get the stego-video. Where as Li. et. al. [7] proposed a DCT method for hiding the secret message. Daniel Socek et. al. [8] proposed a novel video encryption with steganography in digital videos. Tamer Shanableh [9] proposed two data hiding approaches using compressed MPEG video.

2. Techniques

This section abstracts the techniques implemented:

2.1. A 3-3-2 bit LSB based Video Steganography Scheme

The scheme takes eight bits of secret data at a time and conceal them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight (08) bits of message six (06) bits are inserted in R and G pixel and remaining two (02) bits are inserted in B pixel. The technique has been depicted in Figure 1.

2.2. HLSB Video Steganography

A Hash based Least Significant Bit (HLSB) technique for Video Steganography is reported which tries to improve on 3-3-2 bit LSB technique. The flow diagram of the same is given in Figure 2.

A video stream (AVI) consists of collection of frames and 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 cover video is then broken down into frames. A 3-3-2 LSB based as explained in section 2.1 has been applied to conceal the data in the carrier frames. The embedding positions of the eight bits out of the four (4) available bits of LSB is obtained using a hash function of the form,

$$k = p\%n \tag{1}$$

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. Thus the bits are distributed randomly during fabrication which increases the robustness of the technique. 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 function which is known to the intended user, the data of the secret message is regenerated.

2.3. Optimized Video Steganography using Genetic Algorithm(GA)

The system architecture for **Optimized Video Steganography (Encoding)** is given in Fig. 3(a). In the closed loop system, the carrier video is first converted to frames by the module **Splitter**. The Splitter module breaks the video into audio and frames. Though both audio and frames can be used to embed secret data, one or multiple frames have been used as a carrier in the paper. The carrier frame(s) is given as input to the **Embedder**. The embedding is done using the 3-3-2 LSB base embedding technique (as described in 2.1). The output of the embedder is stego frame(s). Now the stego frame(s) goes through an **Optimizer**, which optimizes the stego frame such that it is indistinguishable from the original version. The optimizer uses Genetic Algorithm a global optimization technique and optimizes the stego signal using the objective function an given in Equation 2.

$$E = w_1 \times f_1 + w_2 \times f_2 \tag{2}$$

The objective function E has Mean square error (MSE) (f_1) and Human vision system (HVS) deviation (f_2) as preferred parameters over others. w_1 and w_2 are predefined weights with values 0.8 and 0.2 respectivley.

Next the optimized value goes through a **Anti-steganalysis test** module. In this a steganalytic subsystem as described in [10] has been used. The module analyses the gradient energy as statistical features. However it is difficult to achieve anti-stegalysis and optimization at the same time. Hence, an iterative procedure is used which works in closed loop. The stego frame(s) are then passed through a **Merger** module. It merges the stego frame(s) and all the remaining non stego frames and audio obtained from splitter module to make a **Stego Video**.

Embedding in higher order bits have also been implemented with the Optimized Video Steganography using GA.

2.4. Video Steganography using Local Search

The base techniques of embedding in MSB and LSB are enhanced using few Local search techniques to get optmized frame(s). The details of the technique are not reported as the works are under the process of review/publication.

3. Results and Discussion

results) Any Steganographic technique is evaluated on basis of payload and imperceptibility. Where the former describes the capacity of secret data embedded in the carrier media, measured as payload (bits per byte or bpB and the later gives the measure of embedded data imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility).

Two types of perceptibility measure fidelity and quality have been reported in this work. Fidelity means the perceptual similarity between signals before and after processing. However, quality is an absolute measure of the goodness of a signal to avoid any suspension and therefore detection. The quality measure is given by $PSNR$ [11] as given in Equation 3.

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

where, L is peak signal level for a grey scale image it is taken as 255. The value of MSE is calculated by Equation 4.

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P_{(i,j)} - S_{(i,j)}) \tag{4}$$

where, H and W are height and width and $P_{(i,j)}$ represents original frame and $S_{(i,j)}$ represents corresponding stego frame. Whereas the fidelity measure is measured by Image Fidelity (IF) [11] as given in Equation 5.

$$IF = 1 - \frac{\sum_{i,j} (I_{i,j} - \bar{I}_{i,j})^2}{\sum_{i,j} I_{i,j}^2} \tag{5}$$

where, i and j are coordinates of the pixel, $I_{i,j}$ is pixel value of carrier frame and $\bar{I}_{i,j}$ is pixel value of stego frame.

The results obtained using 3-3-2 bit based LSB technique (as explained in section 2.1) and Hash based technique (reported in section 2.2) with the properties of carrier video used are detailed in table 2 and table 1 respectively.

Performance evaluation of GA as an optimizer (section 2.3) over 3-3-2 bit LSB based Base Video Steganography Technique (base technique) is reported in table 3 and the carrier video used are given in table 4 respectively.

4. Conclusion

Novel video steganography techniques have been reported. Performance evaluation has been done of the proposed techniques with some existing techniques. The results obtained are encouraging for further analysis and research. Though very few Video Steganlysis techniques are reported in literature the future scope of work includes testing of the reported techniques against video steganalysis and some new technique(s) are on the anvil.

5. Publications

Kousik Dasgupta, J.K.Mandal, Paramartha Dutta, “Hash Based Least Significant Bit technique for Video Steganography(HLSB),” in*International Journal of Security, Privacy and Trust Management (IJSPTM)*, pp 1-11, April 2012 (DOI: 10.5151/ijsptm.2012.2201).

Kousik Dasgupta, J.K.Mandal, Paramartha Dutta, “Optimized Video Steganography using Genetic Algorithm (GA),” in Proceedings of *International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013*, pp 131-137, 2013, Procedia Tehcnology (DOI:10.1016/j.protcy.2013.12.345).

References

[1] Patel, K.,Rora, K. K., Singh, K. and Verma, S. *Lazy Wavelet Transform Based Steganography in Video*, in Proceedings of International Conference on Communication Systems and Network Technologies (CSNT), 2013, DOI-10.1109/CSNT.2013.109, pp:497-500.

[2] Thakur, V. and Saikia, M., *Hiding secret image in video*, in Proceedings of International Conference on Intelligent Systems and Signal Processing (ISSP), 2013, DOI-10.1109/ISSP.2013.6526892, pp:150-153.

[3] Kelash, H.M., Abdel Wahab, O.F., Elshakankiry, O.A., and El-sayed, H.S., *Hiding data in video sequences using steganography algorithms*, in Proceedings of International Conference on CT Convergence (ICTC), 2013, DOI-10.1109/ICTC.2013.6675372, pp:353-358.

[4] Niu Ke and Zhong Weidong, *A video steganography scheme based on H.264 bitstreams replaced*, in Proceedings of International Conference on Software Engineering and Service Science (ICSESS), 2013, DOI-10.1109/ICSESS.2013.6615345, pp:447-450.

[5] Gujjunoori, S. and Amberker, B.B., *A reversible data embedding scheme for MPEG-4 video using HVS characteristics*, in Proceedings of International Conference on SIntelligent Systems and Signal Processing (ISSP), 2013, DOI-10.1109/ISSP.2013.6526886, pp.:117-121.

[6] S. Suma, *Improved Protection in Video Steganography using compressed Video Bitsterams*, in Proceedings of International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, pp.: 764766.

[7] Y. Li, H.-X. Chen, and Y. Zhao, *A new method of data hiding based on H.264 encoded video sequences*, in Proceedings of IEEE Int. Conf. Signal Processing (ICSP), 2010, pp. 18331836.

[8] D. Socek, H. Kalva, Spyros S. Magliveras, O. Marques, D. Culibrk and B. Furht, *New approaches to encryption and steganography for digital videos*, in Proceedings of Multimedia Systems, Springer-Verlag, 2007.

[9] Tamer Shanableh, *Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering*, in Proceedings of IEEE Transactions on Information Forensics and Security, VOL. 7, NO. 2,2012, pp.:455-464.

[10] W.-N. Lie, G.-S. Lin, and S.-L. Cheng, *Dual protection of JPEG images based on informed embedding and two-stage watermark extraction*, in Proceedings of IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 330-341, 2006.

[11] M. Kutter and F. A. P. Petitcolas, *A fair benchmark for image watermarking systems*, in Proceedings of Electronic Imaging ’99. Security and Watermarking of Multimedia Contents, vol. 3657, The International Society for Optical Engineering, pp. 1-14, 1999.

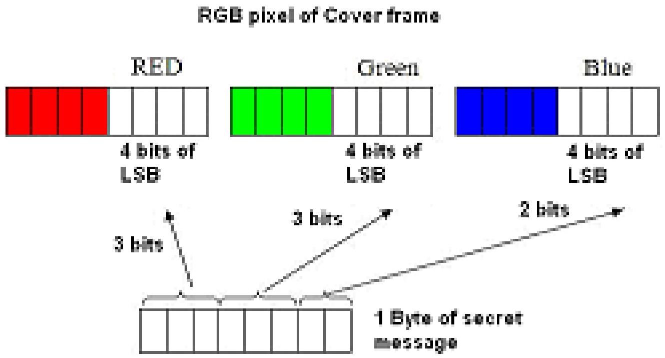

Figure 1. A 3-3-2 bit embedding technique showing 1 Byte of secret data embedded inside 4 bits of LSB in 3,3,2 order into corresponding RGB pixels of carrier frame

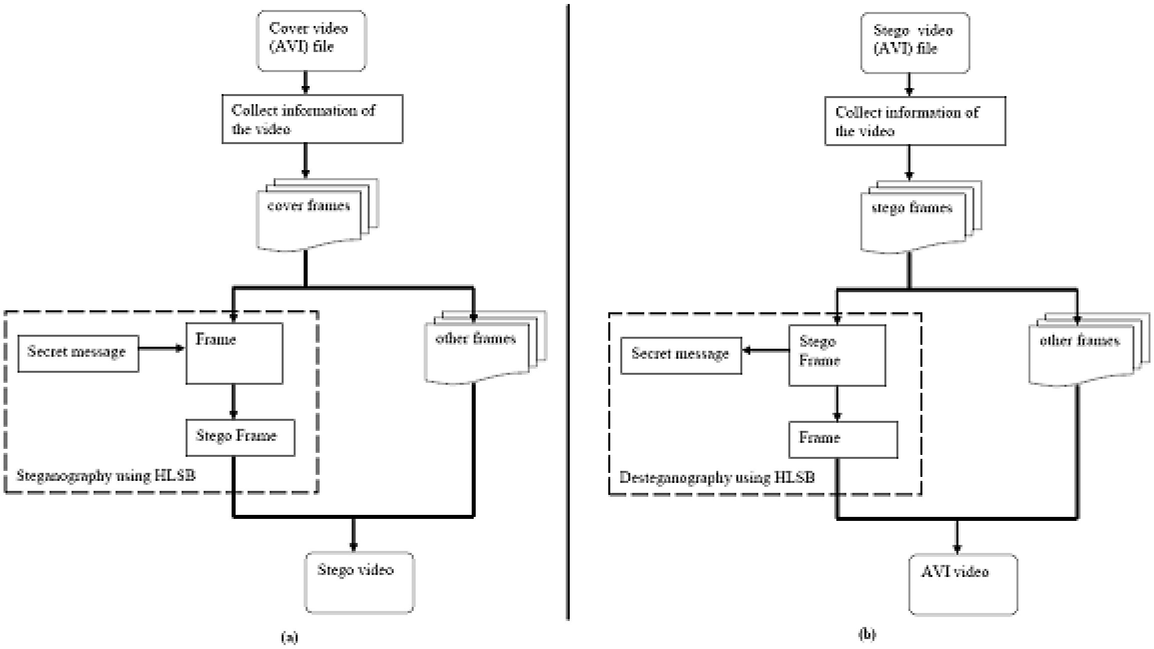

Figure 2. Block diagram of HLSB Video Steganography technique (a) Encoding and (b) Decoding

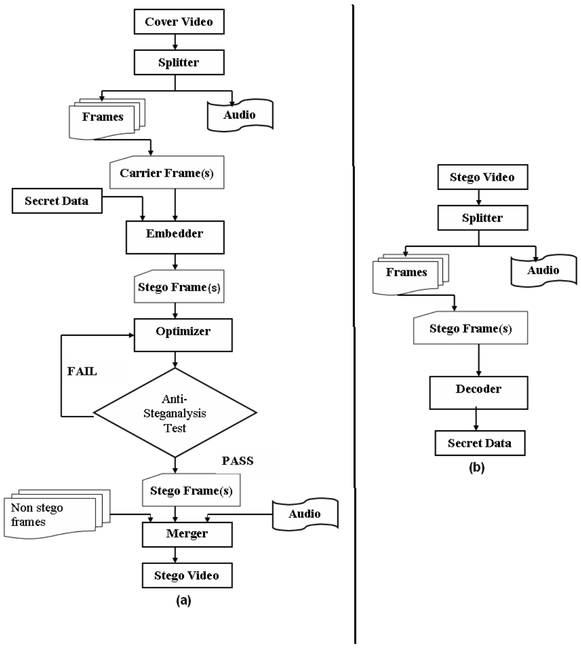

Figure 3. System Architecture of the proposed GA based Optimized Video Steganography technique (a) Encoding and (b) Decoding

Table 1. Cover Video File details

S.No.	Cover video file information				Secret message Resolution $W*H$
	Name of video	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. Performance evaluation using HLSB and 3-3-2 LSB techniques

Name of video	Results obtained using HLSB			Results obtained using 3-3-2 LSB based Video Steganograpgy Technique		
	PSNR	IF	Payload (bpB)	PSNR	IF	Payload (bpB)
drop.avi	44.34	0.23	2.66	48.56	0.42	2.66
american football.avi	45.67	0.25	2.66	52.34	0.34	2.66
flame.avi	42.66	0.35	2.66	48.56	0.38	2.66

Table 3. Cover Video File details

S.No.	Cover video file information				Secret message Resolution $W*H$
	Name of video	Resolution W*H	Frame/ sec	No. of frames	
01	tree. avi	320*240	30	450	150*150
02	globe. avi	320*240	30	107	
03	computer. avi	320*240	30	510	

Table 4. Performance evaluation of GA as an optimizer over Base Video Steganography Technique 3-3-2 LSB

Name of video	Results obtained using GA as an optimizer over Base technique			Results obtained using Base Video Steganograpgy Technique 3-3-2 LSB		
	PSNR	IF	Payload (bpB)	PSNR	IF	Payload (bpB)
tree. avi	39.374	0.99	2.66	38.03	0.87	2.66
globe. avi	34.372	0.99	2.66	32.67	0.89	2.66
computer. avi	41.613	0.99	2.66	39.21	0.86	2.66