ISSN:0975-9646

A Comparative Study of Un-optimized and Optimized Video Steganography

Ritesh Upadhyay, Prof. Y. S. Thakur, Dr. D. K. Sakravdia

[1] *Department of Electronics & Communication Engineering, Ujjain Engineering College, Ujjain*

***Abstract*- This paper presents a comparison between un-optimized and optimized video steganography. In today's world of internet communication, video is considered to be an effective and important tool for communication. Video steganography is a technique of hiding secret information in the video frames or the audio beats of the given cover video so that the presence of the secret information is concealed. The un-optimized base technique used in this paper for video steganography is a 3-3-2 LSB based technique. The un-optimized video frames were then optimized using Modified Genetic Algorithm which generated an optimum imperceptibility of hidden data. Peak signal to noise ratio (PSNR), mean square error (MSE) and image fidelity (IF) are the important mathematical measures for analyzing any steganographic technique. In this paper, we have compared all these three parameters for both un-optimized and optimized video steganography. Experimental results show a considerable improvement in these parameters for the optimized video steganographic technique.**

***Keywords* - LSB Embedding, Modified GA, MSE, Optimization, PSNR, Video Steganography.**

I. INTRODUCTION

Data hiding techniques have been used widely for the transmission of data over a long time. They are classified into two types: Watermarking and Steganography. Steganography comes from the Greek word "steganos" and "graptos" meaning covering and writing respectively. It is the art of embedding a message that is to be hidden in a medium, usually a picture, an audio file, or a video file, in such a way that no one apart from the sender and the intended recipient even realizes that there is a hidden message [1].

In this paper Video is used as a cover media for embedding secret message, where videos can be said as a collection of frames and audio, either in compressed domain or in uncompressed domain. The advantage of using video files in hiding information is primarily because video is more secure against hacker attacks due to the relative complexity of video compared to image files and audio files.

Video based steganography techniques are mainly classified into spatial domain and frequency domain based methods. Frequency domain techniques are mainly based on discrete cosine transforms (DCT) and wavelet transforms. S. Suma et. al. [3] proposed an integer wavelet transformation in cover video so as to get the stego-video. Whereas Li. et. al. in [4] proposed a DCT method for hiding the secret message. In spatial domain the most widely used method is LSB substitution [5] where as MSB substitution can also be used. Daniel Socek et. al. [6] proposed a novel video encryption with steganography in digital videos. Tamer Shanableh [7] proposes two data hiding approaches using compressed MPEG video.

Some other methods exist in literature [8] and [9] for video steganography or data hiding. Briefly, video-based steganography techniques generally take such analysis into account and try to maintain the statistics of the carrier before and after message hiding.

II. PROPOSED SYSTEM ARCHITECTURE

The system architecture proposed for encoding is depicted in Fig. 1. In the closed loop system, the carrier video is first splitted into image frames and audio beats separately by the splitter. Then the image frames are chosen randomly for hiding the message which is given to the embedder circuit. The secret message is first encrypted using a key (password taken from user) then it is given to the embedder circuit.

The embedding is done using the 3-3-2 LSB based technique (as described in the section III-A). The output of the embedder is the un-optimized stego frames. Next, the stego-frames are passed through an optimizer which optimizes the stego frames such that it is indistinguishable from the original frame. The Modified Genetic Algorithm has been used by the optimizer as an optimization technique.

The optimizer optimizes the stego-frames using the objective function as given in Equation (A). The stego-frames are then passed through a merger circuit which merges the stego-frames and all the remaining non-stego-frames and audio obtained from splitter module to make a stego video ready for transmission.

The system architecture for decoding is given in Fig. 2. The stego-video is passed through the splitter module which splits the video into image frames and audio beats. Then the stego-frames are selected and are given to the decoder circuit. The decoder separates the video frames and we get the encrypted secret message. Then the encrypted secret message is decrypted using the same key (password taken from user). Thus we get the output as the secret message which was embedded inside the carrier video.

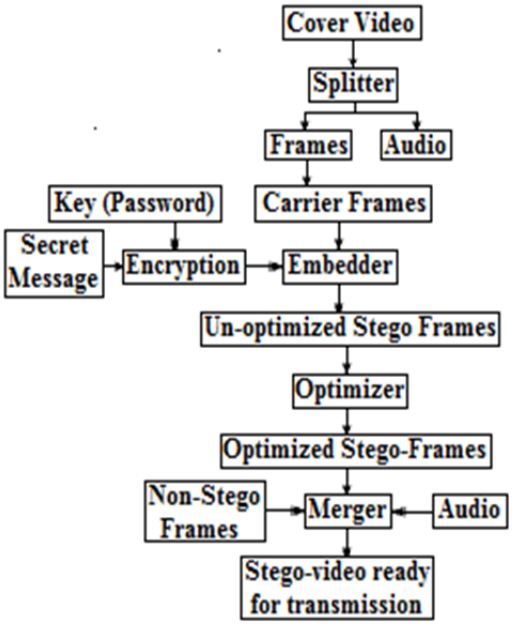

Fig. 1: Proposed system Architecture for Encoding process

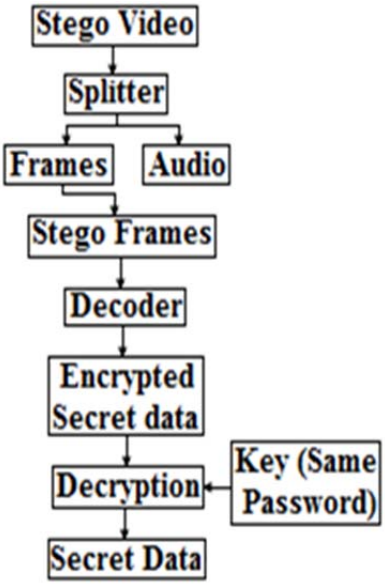

Fig. 2: Proposed system Architecture for Decoding process

III. IMPLEMENTATION

The proposed system architecture is implemented in MATLAB R2011b.

A. The un-optimized base technique: A 3-3-2 based LSB video steganography

In the un-optimized base technique, the 8-bits of secret message are embedded at a time in the LSB of RGB (Red, Green and Blue) pixel values of the carrier image frames in the 3-3-2 order respectively [10]. Thus first three bits of the secret message are concealed inside 3-bits of LSB of Red pixel, next 3-bits in the three bits of LSB of Green pixel. The remaining two bits of secret message are concealed in 2-bits of LSB of Blue pixel. Here, fig. 3 shows the detailed technique.

The particular distribution pattern is taken considering that the chromatic influence of blue to the human eye is more than that of red and green pixels. Hence without sacrificing the quality of the video an optimum payload can be achieved. Also this small variation in colors inside the large number of video frames would be very difficult for the human eye to detect.

1) Encoding Algorithm:

a. Find the LSB bits of each RGB pixels of the cover frame
b. Embed the 8 bits of the secret message into LSB of RGB pixels in the order of 3-3-2 respectively of the cover frame.
c. Reconstruct the stego video frames.

2) Decoding Algorithm:

a. Find the LSB bits of each RGB pixels of the stego video frame.
b. Retrieve the bits of secret data from LSB of RGB pixel of the stego frame in the order of 3-3-2 respectively.
c. Reconstruct the secret information.
d. Regenerate video.

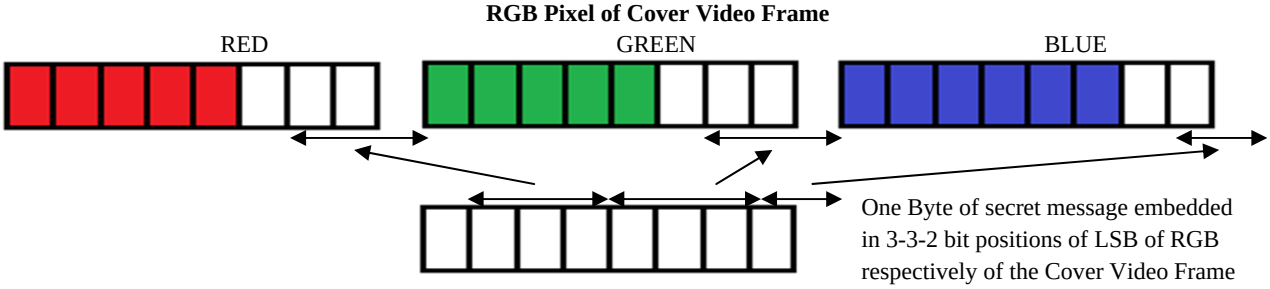

Fig. 3: Un-optimized base embedding technique showing One Byte of Secret message embedded inside LSB of corresponding RGB pixel value of carrier video frames in 3-3-2 order

B. Optimization technique using Modified Genetic Algorithm

The stego frames obtained from the base technique has resulted in changes of RGB pixel of the original frames but imperceptibility of the video needs to be taken care for successful steganography. For design of any steganographic schemes several factors should be considered like imperceptibility, embedding capacity, statistical undetectability (anti-steganalysis), Bit error rate (BER) after data extraction and robustness to attacks. However some of the factors conflict with one another, such as, increasing embedding capacity might reduce the imperceptibility, etc.. Hence any steganographic problem can be viewed as an Optimization problem where a steganography scheme maps a secret data (or stego signal) to a host media (or undetected region) [11]. Thus an objective function that minimizes all the mentioned parameters and giving a completely optimal solution is not possible. Hence, in this paper an objective function as in Equation (A) has been proposed where preferred parameters are optimized and letting all others be inequality constraints. The proposed objective function E has Mean square error (MSE) (f1), Human vision system (HVS) deviation (f2) and Image Fidelity Factor (IFF) (f3) as preferred parameters,

$$E = w1 \times f1 + w2 \times f2 + w3 \times f3 \qquad (A)$$

where *w*1, w2 and *w*3 are predefined weights. It is very difficult to decide the weights; one criterion can be that more general the factor larger is the weight. The other logic can be user's importance given to a particular factor over the other. Here the later approach has been used and the optimization is then performed on the given set of weights. The weights are considered as $w1 = 0.6$, $w2 = 0.2$ and $w3 = 0.2$. The most widely adopted statistical image quality feature for accessing image quality is MSE, given by Equation (D). It measures the distortion between pixels of stego frame and original frame. The other preferred parameter in objective function is SSIM (structural similarity) [12] which accounts for HVS characteristics. It takes care of substantial point-by-point distortions that are not perceptible, such as spatial and intensity shifts, as well as contrast and scale changes.

SSIM is a function of luminance comparison $l(x, y)$, contrast comparison $C(x, y)$ and structure comparison $s(x, y)$ as given in Equation (B):

$$SSIM = f(l(x, y), c(x, y), s(x, y)) \qquad (B)$$

This optimization problem is solved by Modified GA using the Optimizer module of the proposed system architecture explained in section II. A little research has been done in application of Modified GA to video steganographic problems, though some work exits in literature on image steganography [13].

Genetic Algorithm [14] has been used by researchers as an optimization tool in varied set of problems. This paper uses a Modified GA approach for optimization.

The proposed algorithm for Modified GA as an optimizer of the un-optimized base video steganography technique has been explained below:

1) *Input:* Stego frame(s) with secret data embedded in 3-3-2 target layers of LSB of each RGB pixels.
2) *Output:* Optimized Stego frame(s).
3) *Initialization of population:* Objective of this step is to get different chromosomal representation of the pixel value of the stego frame. A random selection of data points are made as initial population. Where each of the data points have same target layers.
4) *Mutation:* This step selects most of the times the best fitted pair of individuals for crossover. The fitness values of each individual chromosome are calculated using the fitness function as given in Equation (A). The best fitted value chromosome is selected twice and the least fitted value is discarded for mutation. A very small value (5%) is chosen as mutation probability. Depending upon the mutation value the bits of the chromosomes, except the target layers, are changed from '1' to '0' or '0' to '1'. The output of this is a new mating pool ready for crossover.
5) *Crossover:* Objective of this step is to perform crossover between the Mating pools selected in the previous step. A random single point crossover is chosen and portion lying on one side of crossover site is exchanged with the other side. Thus it generates a new pair of individuals.

The steps Mutation and Crossover are repeated iteratively till, either maximum number of iterations is exceeded or we get a chromosome having pixel value closest to the original value. The optimized stego frame(s) are then merged with non stego frames and audio in the merger module as explained in Fig 1. The final output is an optimized stego video ready for transmission.

IV. RESULTS AND DISCUSSIONS

The proposed technique of un-optimized and optimized video steganography were tested on four video files of which two are .avi video files and the other two are .mp4 video files. The secret message which is to be embedded inside the video could be of any type of file (.pdf, .jpg, .avi, .mp4, etc). The details of the four videos used and secret message used for implementation are provided in table I. Table II shows the comparison of both the un-optimized base technique and optimized video steganography technique in terms of PSNR, MSE, PC and %IF.

PSNR is defined as the measure of quality of the video signal. The signal in this case is the pixel value of the original video frame and noise is the difference between the pixel values of the stego video frame and the original video frame. Mathematically, PSNR (in dB) is given by the formula:

$$PSNR = 10 \log_{10} \frac{Max(i)^2}{MSE} \qquad (C)$$

where, Max(i) is the maximum possible pixel value of the image when the pixels are represented using 8 bits/sample

(for grey scale images, its value is equal to 255). A higher value of PSNR is always desirable.

The MSE is given as:

$$MSE = \frac{1}{H*W}\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}[\mathrm{I(i,j)} - \mathrm{K(i,j)}] \qquad \text{(D)}$$

where, i and j are the co-ordinates of the pixel.

I(i,j) is the pixel value of the original carrier frame and K(i,j) is the pixel value of the stego video frame.

Since, 8 bits of secret data are embedded per 3 Bytes of carrier image frame, so payload is equal to 2.66bpB (8/3=2.66bits/Byte).

Fidelity means the perceptual similarity between the signals before and after processing. Mathematically, the %age Image Fidelity (%IF) is given by the formula:

$$\%\, IF = \left(1 - \frac{\sum_{i,j}\left(I(i,j) - K(i,j)\right)^2}{\sum_{i,j} I^2(i,j)}\right) * 100 \qquad \text{(E)}$$

where, i, j, I(i,j) and K(i,j) are same as described above.

The bar graphs of all the four video for both un-optimized and optimized video steganography techniques are shown in figure 4, 5, 6 and 7.

On comparing the results, it can be seen that though the Payload Capacity remain same for both the techniques, the PSNR, MSE and %IF values show considerable improvement.

Table I: Cover Video file and Secret message Details

S. No.	Cover Video file information				Secret Message Resolution W*H
	Name of Video	Resolution W*H	Frames/second	Number of Frames	
1	1.avi	320*240	30	981	160*160
2	2.avi	320*240	30	856	
3	3.mp4	320*240	30	657	
4	4.mp4	320*240	30	410	

Table II: Result Analysis of Modified GA as an optimization technique over un-optimized base video steganography technique

Name of Video	Results obtained using un-optimized base video steganography technique 3-3-2 LSB				Results obtained using Modified GA as an optimization technique over un-optimized base technique			
	PSNR	MSE	%IF	PAYLOAD (bits/Byte)	PSNR	MSE	%IF	PAYLOAD (bits/Byte)
1.avi	42.67	3.515	85.27	2.66	45.17	1.976	94.52	2.66
2.avi	41.94	4.159	87.18	2.66	44.24	2.449	95.32	2.66
3.mp4	39.18	7.852	88.63	2.66	41.64	4.456	96.17	2.66
4.mp4	38.83	8.511	89.17	2.66	40.47	5.834	96.45	2.66

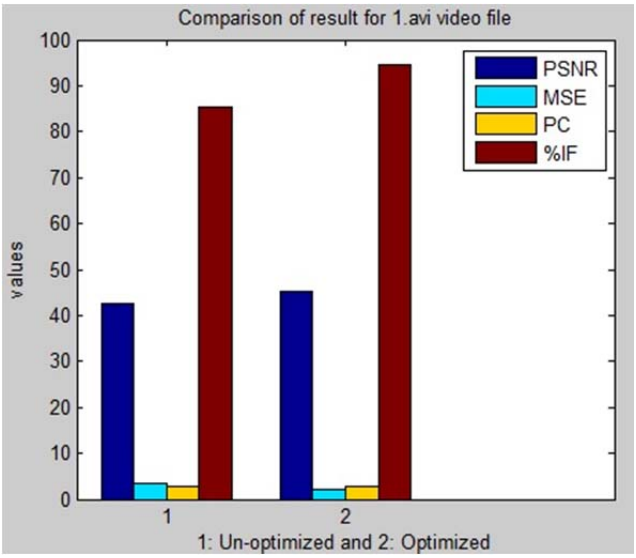

Fig. 4: Comparison of result for 1.avi video file (1: Un-optimized and 2: Optimized)

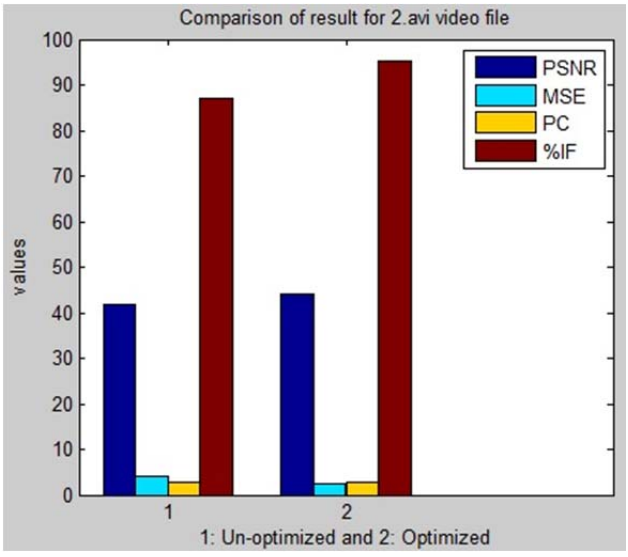

Fig. 5: Comparison of result for 2.avi video file (1: Un-optimized and 2: Optimized)

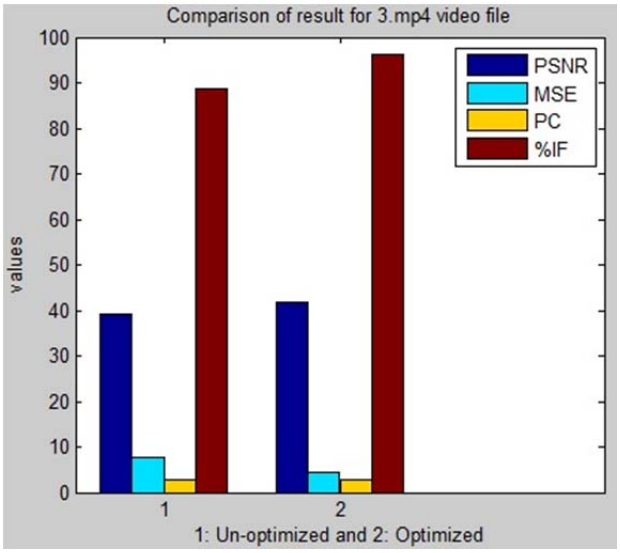

Fig. 6: Comparison of result for 3.mp4 video file (1: Un-optimized and 2: Optimized)

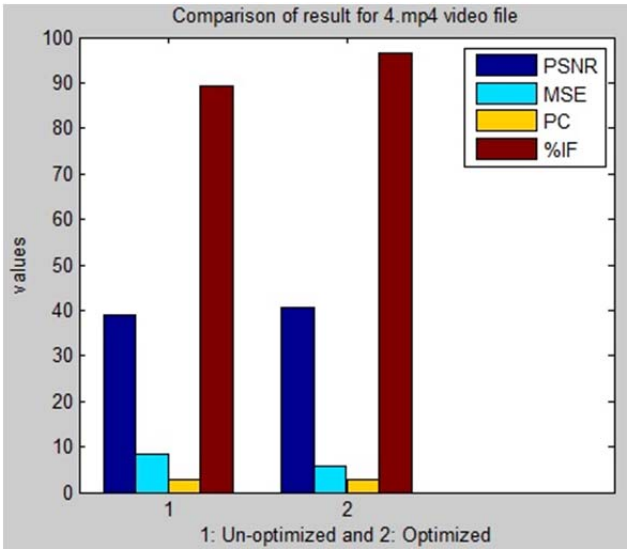

Fig. 7: Comparison of result for 4.mp4 video file (1: Un-optimized and 2: Optimized)

V. Conclusion

In this paper, a Modified GA based optimized video steganographic technique has been proposed. The optimizer optimizes the values over basic video steganography done using a 3-3-2 LSB technique. The optimizer uses an objective function which consists of 3 factors. A comparative study has been done of the proposed optimized technique and the un-optimized base technique in terms of PSNR, MSE and %IF. The PSNR value lies between 30dB and 50dB which is considered as standard. Generally, if the PSNR value exceeds 36dB, it becomes difficult for the human visual system to recognize any difference between a cover and stego file. The proposed techniques were applied in both compressed and uncompressed domain.

Reference

[1] R. Balaji and G. Naveen, "*Secure Data Transmission using Video Steganogrpahy*", IEEE, 2011.

[2] Kousik Dasgupta, Jyotsna Kumar Mondal and Paramartha Dutta, "*Optimized Video Steganography using Genetic Algorithm (GA)*", International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013, ELSEVIER.

[3] S. Suma, "Improved Protection in Video Steganography using compressed Video Bitsterams," in *International Journal on Computer Science and Engineering*, Vol. 02, No. 03, pp. 764–766, 2010.

[4] Y. Li, H.-X. Chen, and Y. Zhao, "A new method of data hiding based on H.264 encoded video sequences," in Proc. *IEEE Int. Conf. Signal Processing, ICSP*, pp. 1833–1836, 2010.

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

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

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

[8] V. Sampat, K. Dave, J. Madia and P. Toprani, "A Novel Video Steganography Technique using Dynamic Cover Generation," in Proc. *National Conference on Advancement of Technologies-Information Systems and Computer Networks, ISCON-2012*, Proceedings published in International Journal of Computer Applications, 2012.

[9] Wang Jue, and Zhang Min-qing,"Video Steganography Using Motion Vector Components," in Proc. of *IEEE 978-1-61284-486-2/11*, pp. 500- 503, 2011.

[10] 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).

[11] M. Wu and B. Liu, "Data hiding in image and video: Part IFundamental issues and solutions," in Proc. of IEEE Trans. Image Process., vol. 12, no. 6, pp. 685-695, 2003.

[12] Z. Wang, A.C. Bovik, H. R. Sheikh, and E .P. Simocelli, "Image quality assessment: From error measurement to structural similarity," IEEE Trans. Image Processing, vol. 13, no.4, pp.600-612, Apr .2004.

[13] S. P. Maity and M. K. Kundu,"Genteic ALgorithm for optimality of data hiding in digital images", in SOft Comput(2009)13, Springer-Verlag, pp. 361-373, 2009.

[14] Goldberg D, "Genetic Algorithm in Search, Optimization and Machine Learning," Addison-Wesley, 1989.

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