An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission

Vivek Kapoor, PhD
Department of Information Technology
IET DAVV, Indore, India

Akbar Mirza
Department of Information Technology
IET DAVV, Indore, India

ABSTRACT

The growth of high speed computing devices and Internet has made the Data communication very easy and fast. But this advancement has also increased the chances of getting the data snooped at the time of sending and receiving messages over network. So that Information has to be secured. In this paper, we proposed a method that uses Steganography. Steganography is a way of hiding secret information into a file (or any other thing that is convertible to Digital Format) and send it to the other end without being noticed. Proposed method takes Video as a carrier file and all the information is stored within that video file (that is called Video Steganography). The proposed method is based on Pixel Value Extraction of RGB model which uses Least Significant Bit insertion technique to insert the text within the Video file. Here the secret data is inserted into video frames after applying some checks onto it, related to its imperceptibility and capacity. In this paper we also have done some kind of Quantitative Analysis on different types of data. The result is evaluated in terms of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), that is, the output video file is compared to the original file, and we find minimal degradation that is quite imperceptible. Finally, we have some comparison drawn between some old methods with this new one.

Keywords

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

1. INTRODUCTION

Steganography is an art of hiding secret information within other files. The word Steganography is a combination of two Greek words ‘Steganos’ which means ‘covered or hidden’ and ‘Graphy’ which means ‘writing or drawing’. Steganography is used for Data Hiding. The file that is used for hiding the secret data is called ‘cover medium’ or ‘carrier file’ and the message that has to be hidden is knows as secret data. It can be used in different fields like military as well as Industrial Field.

Watermarking and Cryptography are the other techniques that are used for protecting data from unauthorized access. Traditionally, Steganography is used in text files as Text Steganography but today it can be used in Image files as well as Video Files. Size of video files is very large as compared to text files, it become very easy for us to hide data in video files. But there are some certain parameters which need to be considered, these are described next in the paper

Capacity – Capacity refers to the amount of data that can be hidden in the cover medium so that no perceptible distortion is introduced.

Imperceptibility – Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading the perceptual quality by data embedding.

Video based Steganography uses Video files as a cover medium. The video files come with an advantage of added security in hiding information. It is very difficult for the intruder to know the existence of any kind of message. Video based Steganography is mainly classified into two methods, first one is Frequency domain method and the other one is spatial domain method. In the Frequency Domain method, firstly frames are to be transformed into its frequency domain by using some predefined methods like Direct Cosine Transform (DCT) or DWT and FFT, after then the message is embedded in previously obtained Transformed Coefficients. On the other hand, in Spatial Domain method, we replace the pixel value with the secret information by using LSB methods. Here the message is directly embedded in selected pixels only that does not cause that much effect on the output video file.

In this paper, we proposed a method that is based on Spatial Domain method. In our opinion, there is a lot of work can be done in the existing methods of LSB insertion. In Spatial Domain method, there is large amount of data that can be stored without being noticed, because here data is stored according to the intensity of pixels, after embedding some bits the quality of video files may decrease. It depends on the color depth of the original video files and the number of bits inserted. The good quality of pixels and less bits insertion gives minimal degradation.

2. LITERATURE SURVEY

A number of Steganography methods have been proposed and implemented in literature, most of which is based on Spatial Domain. A lot of algorithm has been used for inserting secret bits in an image file. Here the LSBs of the image file are replaced with the same number of bits of the secret message. In this section we are going to get through some of these methods and algorithms. In [1] a robust Video Steganography technique based on LSB insertion with AES (Advance Encryption Standard) encryption is used. It is implemented as 1-bit, 2-bit and 3-bit LSB insertion and also improved the security level of hidden Information. In [2] same technique is used with RSA encryption. Lovely Malhotra[2] has implemented the Steganography in an audio file [2] enhanced the existing LSB technique by getting lossless recovery of data. Some other methods of LSB insertion can be found in [6].In [3], a new Compressed Video Steganography has been proposed that works on TPVD (Tri-pixel-value-differencing). The proposed system has high imperceptibility and capacity. It embeds data in MPEG format of video files which is an enhancement over the methods using AVI format. Machado [4] proposed a system named EzStego which embeds data bits to the GIF formats of the images. Kavaguchi [5] proposed a different method for inserting data in the blurred parts of the images by using BPCS (Bit Plane Complexity Segmentation). These techniques are quite different than traditional LSB methods.

Video Steganography has gained lot of attention from researchers lately. Some used Steganography with Cryptography by creating a secret key form the secret message. It can also be done in two ways like public key and private key cryptography. The former one requires two sets of keys and the latter one required a single key from both ends. [8] Proposes the same, the data is encrypted by some key and embedded to the video file and the key is also inserted through LSB insertion, as in key file.

3. PROPOSED WORK

The proposed work is for hiding text data in video file. This is based on the LSB insertion, in which some LSB's of Image Files are replaced by message bits.

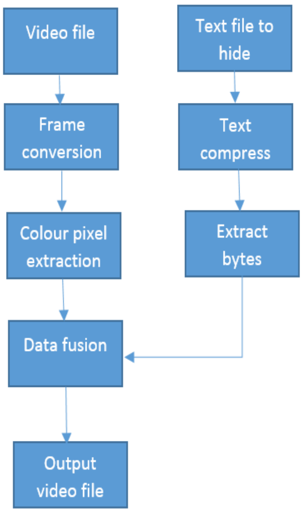


Figure 1 proposed methodology

3.1 System Architecture Sending Side

Functional diagram of the proposed method is drawn above. And the explanation of modules is given below

Video File- The video file which is used for a cover medium.

Frame Conversion- In this module all the frames of video files will be extracted. And are stored in at some place.

Text File- It is the text file which will be embedded in the video frames and sent over the network. It should be sent secretly without being noticed by anyone.

Text Compression- Before sending the text file, the text file will be compressed and the bytes are generated. Advantage of sending compressed data over the network is to minimize the payload and reduce extra burden of the network.

Color Pixel Extraction- In this phase the value of each color pixels is calculated in RGB 24 bit format. Then the pixel look like (0…255, 0…255, 0…255)

Extract Bytes- Here bytes are extracted from the secret message and chunks of bits are created. And these chunks are then embedded with the video frames.

Data Fusion- Text Files are then combine with video frames.

Output Video- At last output video file is generated. This file is then sent.

Block diagram of the receiving side

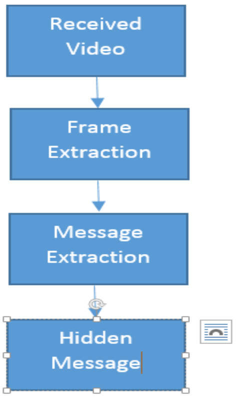


Figure 2 proposed methodology

3.2 System Architecture Receiving Side

The functional overview of the proposed stenographic model is given using figure 2.The system accepts two different kinds of input file first the video file which is used to hide data and second file which is desired to hide in video. The input text file is first compressed using the ZIP compressor the compressed file is then converted into bytes. On the other hand the input video file is processed and the video frames are extracted from the video file. Than after the data diffusion process is taken place. Due to this the pixels are selected which are utilized for the hiding data. Then after the compressed byte data is embedded to the video frame. Finally the embedded video frames are combined and converted into the final video file.

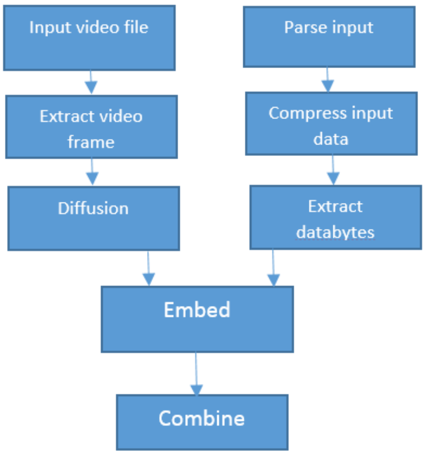


Figure 3. Subsystem Architecture

4. ALGORITHM FOR THE PROPOSED METHOD

In this section proposed Algorithm for Encryption as well as Decryption is provided.

4.1 Encryption Algorithm

Step 1: Read Video File of valid format. As a Cover Medium

Step 2: Process the input video.

Step 3: Divide video into frames.

Step 4: Input message in text format.

Step 5: Divide message into chunks of 2 bytes.

Step 6: Find the value of RGB pixels of video frame.

Step 7: Embed the 2 bytes of message into first 2 pixels of the frame starting from the first frame (1 byte each pixel)

Step 8: Generate the video frame.

4.2 Decryption Algorithm

Step 1: Input the received file.

Step 2: Process the video file.

Step 3: Divide video into frames.

Step 4: Find the 24 bit RGB pixels value of each frame.

Step 5: Find the position of secret data using serial scanning of video frames, according to encryption.

Step 6: Retrieve the message in the 2 bytes chunks.

Step 7: Reconstruct the secret message.

5. RESULTS AND PERFORMANCE EVALUATION

There are two important parameters of evaluating all Steganography technique, first is imperceptibility and the second is capacity. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis. Capacity means maximum payload is required, *i.e.* maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image.

The imperceptibility of the embedded data is indicated by comparing the original video frame to its stego video frame so that their visual differences can be determined and it is called as Data Quality. Mean squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) are the other two important measures of studying the stego frame and its corresponding cover frame. The studied quantities are given as below..

Data quality

Accuracy is a measurement of the truthiness of records that are recovered after decryption of the data.

$$Acuracy = \frac{accuratelyrecovreddata}{originaldata} X100$$

Mean Square Error

$$\mathrm{MSE} = \frac{1}{H * W}\sum_{i=0}^{H}(\mathrm{P(i,j)} - \mathrm{S(i,j)})^2$$

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

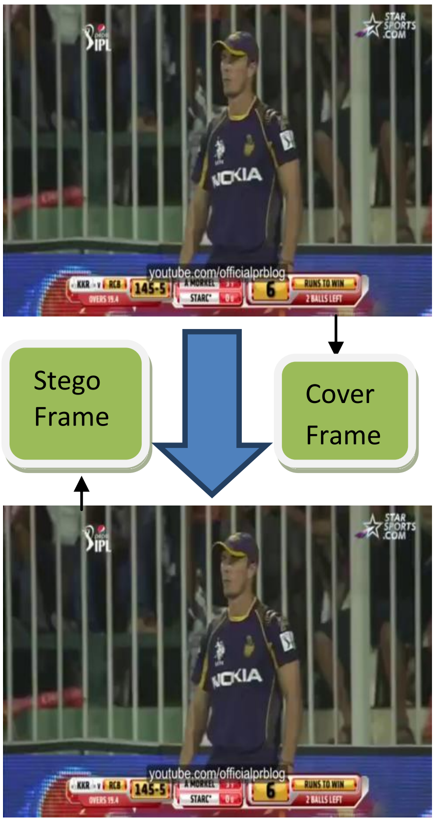
Peak Signal To Noise ratio

The PSNR measures the peak signal-to-noise ratio between two images. This ratio is often used as a quality measurement between the original and a compressed image. Higher the PSNR means better the quality of the compressed or reconstructed image. The PSNR value can be calculated as:

$$PSNR = 10log_{10}\left(\frac{L^2}{MSE}\right)$$

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

Here is the little demonstration of the cover image and the stego image. It is completely invisible to the human eye.



We have tested this technique on some different videos(different in size, resolution etc), and we got successful in keeping the Mean Square Error and Peak Signal to Noise Ratio low enough that it cannot be noticed easily in the Steganalysis process . Later in this section we provided a comparison between the basic LSB method [8] and our method, and we got encouraging result, the proposed method gives better MSE and PSNR values than the LSB [8] method. Table 2 compares the average PSNR of the proposed LSB embedding technique (per pixel, RGB) to the traditional layering technique in which embedding is done by layers of RGB. Our results show significant improvement in PSNR up to 1.5 dB more than the PSNR achieved using traditional LSB embedding techniques. And we also lowered the Mean Squared Error (MSE), lower MSE means increased indetectability. We picked some videos tested this system on them. We got improved results.

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				Stego Video
	Name of video file	Resolution	Frame/ Second	No. Of Frames	
01	Demo1.mp4	640*360	25	655	640*360
02	Demo2.mp4	512*288	15	180	512*288
03	Demo3.mp4	320*240	14	2884	320*240

Table 2. Results obtained from Proposed Method and LSB techniques

Name of Video	Results obtained using Proposed Method			Results obtained using LSB Method[8] (On Similar Videos)		
	PSNR	Avg. MSE	Pay Load	PSNR	Avg. MSE	Pay Load
Demo1.mp4	52.94	0.33	2.66	51.33	0.38	1
Demo2.mp4	52.22	0.39	2.66	50.89	0.42	1
Demo3.mp4	51.55	0.45	2.66	50.31	0.48	1

Fig 5(a) represents the graph of PSNR comparison

.

Fig 5(b) represents the graph of MSE comparison.

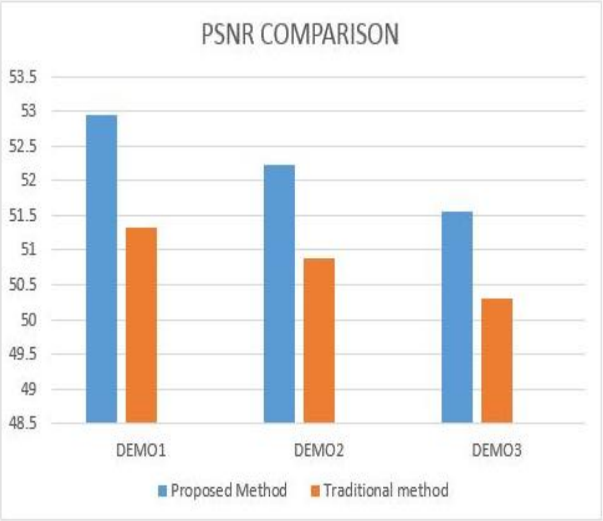


Fig 5(a)

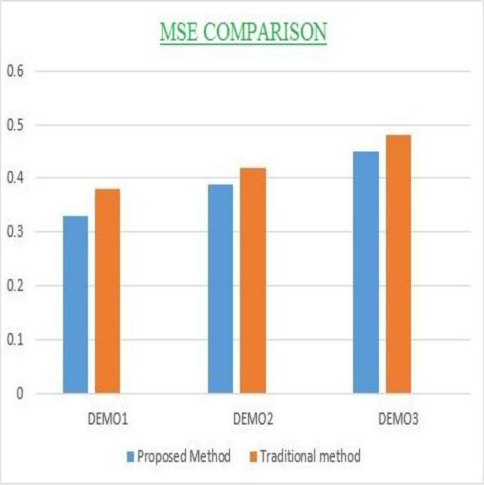
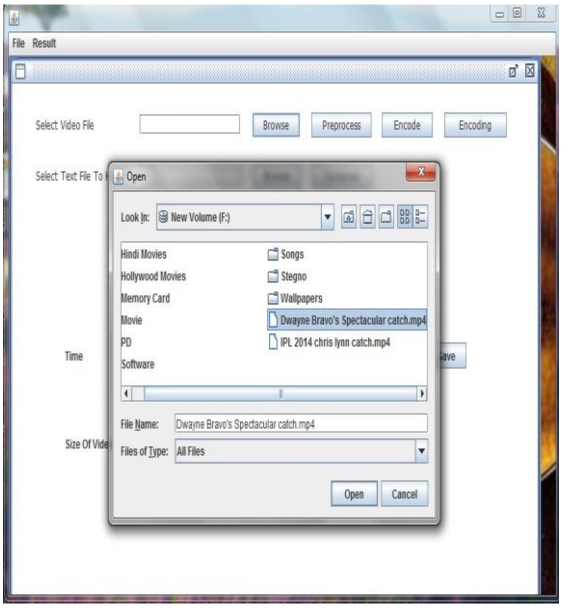


Fig 5(b)

6. SNAPSHOTS

Fig 6(a) shows the input video file selection



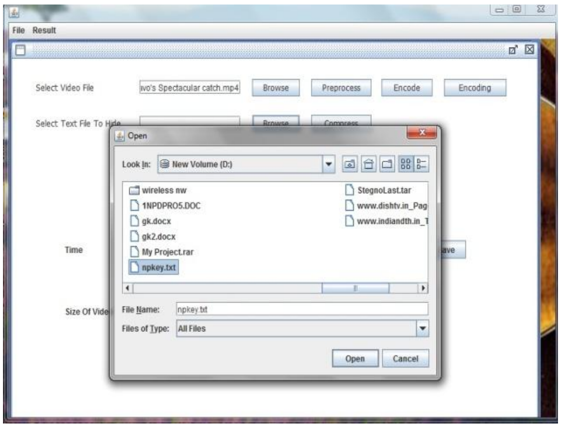
Look In: New Volume (F:)

Hindi Movies
Hollywood Movies
Memory Card
Movie
PD
Software
Songs
Stegno
Wallpapers
Dwayne Bravo's Spectacular catch.mp4
IPL 2014 chris lynn catch.mp4

File Name: Dwayne Bravo's Spectacular catch.mp4

Files of Type: All Files

Fig 6(b) shows the input text file selection



Select Video File: ivo's Spectacular catch.mp4

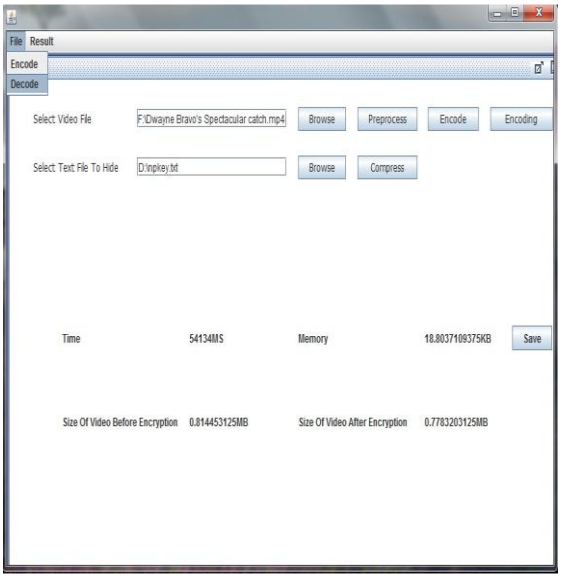
Look In: New Volume (D:)

wireless nw
1NPDPRO5.DOC
gk.docx
gk2.docx
My Project.rar
npkey.txt
StegnoLast.tar
www.dishtv.in_Pag
www.indiandth.in_T

File Name: npkey.txt

Files of Type: All Files

Fig 6© shows the time and memory used at the time of encryption



Select Video File: F:\Dwayne Bravo's Spectacular catch.mp4

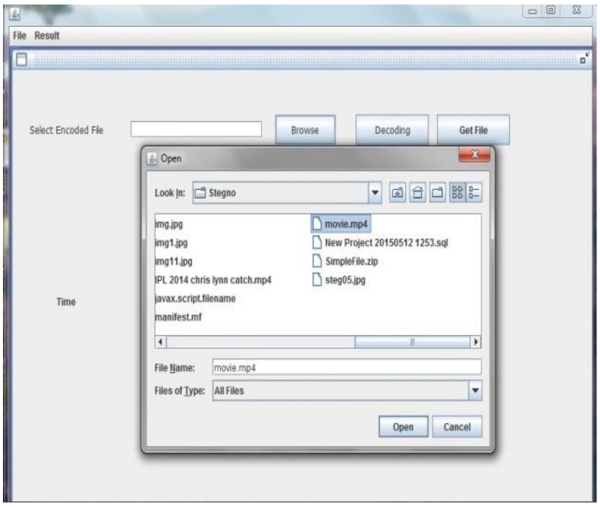
Select Text File To Hide: D:\npkey.txt

Time 54134MS Memory 18.8037109375KB

Size Of Video Before Encryption 0.814453125MB Size Of Video After Encryption 0.7783203125MB

Figure 6(c)

Fig 6(d) Desteganography module



File Name: movie.mp4

Files of Type: All Files

Figure 6(d)

7. CONCLUSION

In this paper an enhanced LSB Based Steganography method has been presented. The technique works in the spatial domain to hide the secret data in video files. The proposed method is designed for MPEG format; however it can work with other video file formats also like AVI, 3GP by doing some modification in it. Performance analysis of the proposed method is also done, and the comparison is made up between previous LSB method and proposed method, and the results are quite encouraging for the same. A secret key can be used at the receiving side, for providing more secure transmission of data, and a software based system for video steganography, both could be the future scope of this technique.

8. REFERENCES

[1] Hemant Gupta,SetuChaturvedi, ―Video Steganography through LSB Based Hybrid Approach‖,IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014

[2] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, ―A NOVEL SECURE IMAGE STEGANOGRAPHY METHOD BASED ON CHAOS THEORY IN SPATIAL DOMAIN‖, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014

[3] Lovely Malhotra, Neha Gupta, ―A DWT and DCT based Hybrid Approach for Audio Watermarking‖, IJCSMC, Vol. 3, Issue. 7, July 2014, pg.536 – 542

[4] R. Machado, http://www.securityfocus.com/tools/586/scoreit, .EzStego., Nov. 1996. [last accessed on 16-04-2012]

[5] E. Kawaguchi and R. O. Eason, Principle and applications of BPCS-Steganography, in Proceedings of SPIE Int'l Symp. on Voice, Video, and Data Communications, pp. 464-473, 1998.

[6] 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.

[7] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta3. Hash Based Least Significant Bit Technique For Video Steganography (HLSB)

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

[8] 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.

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

[10] Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, ―Implementation of LSB Steganography and Its Evaluation for various Bits_ Digital Information Management, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349

[11] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series.

[12] Mobasseri, B.: Direct sequence watermarking of digital video using mframes, Proc. International Conference on Image Processing, Chicago, IL, pp 399- 403, 1998.World Academy of Science, Engineering and Technology Vol:5 2011-02-26 428 International