ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW PAPER

Available Online at www.ijarcs.info

An Analysis of LSB Technique in Video Steganography using PSNR and MSE

Anamika Saini
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Kamaldeep Joshi
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Kirti Sharma
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Rainu Nandal
University Institute of Engineering and Technology
Maharshi Dayanand University
Rohtak, India

Abstract: Security of data is always needed whenever communication is done and to achieve that purpose different techniques are used so that data should not be attacked by the third party. Different data concealing techniques like cryptography, watermarking etc. are used. But if we want the intruder not to even know about the presence of secret data we have to use the Steganography Technique. And this technique can be applied by using different files like text, audio, video etc. One of the steganography types as video steganography used to hide the secret data in an easy manner due to the complexity of its structure. We have different types of methods based upon Format, Cover, and Frequency in video steganography. This paper provides a review and analysis of the video steganography technique applied to AVI video file with LSB technique and the comparison of frames in the video file is analyzed with the help of different parameters to find how similar the cover video frame after embedding the secret data. The analysis is based on the PSNR, MSE, and the result is given.

Keywords: Video Steganography; LSB; PSNR; MSE; RMSE

I. INTRODUCTION

In the present environment of the internet, the bulk of technologies come into existence and their rapid adoption by the users in order to achieve the security of the confidential data while it's transmitting over the public communication channel. We have different types of techniques that are used to conceal the data over the network like Cryptography, Steganography, and Watermarking. Each of the technique is used to provide the security to data with the help of different approaches [1].

In Cryptography, the main objective is the protection of data and text file is used as the carrier medium for hiding data. In this, the meaning of the message is hidden. The secret key is necessary for the data hiding and due to this; it is very simple to know about the hidden data. The security level is high and capacity of hiding the data is also high in Cryptography. The attacks on this technique are called Cryptanalysis [2].

In Watermarking, the main objective is copyright protection of data and for this digital media is used as the carrier medium. There is also a restriction in the selection of the cover for data hiding. The secret key is optional for data hiding and there is only a few possibility of knowing about the hidden data by human eyes. For the retrieval of the data, cross correlation can be used. The capacity of hiding the data is low but the security level is high. The attacks can be done by the replacement of watermarks [3] [4].

Steganography is a technique which hides the presence of data by using different cover mediums. The different cover mediums can be Images, Audios, and Videos etc. The word Steganography is procured from the Greek words 'steganos' means 'cover or shelter' and 'graphei' means 'writing'[5].

The main objective of steganography is to provide secret communication that should be invisible to the unauthorized users. The secret key is optional to use in steganography. The data hiding through this technique could never visible to human eyes [6]. The capacity of hiding the data is very high and the security level is also high. The attacks on this technique are named as Steganalysis.

The comparison of different techniques and their protocols used are shown below in the tables [7].

Table 1 Comparison of Different Communication Technique

Communication Techniques	Integrity	Confidentiality	Un-removability
Cryptography	No	Yes	Yes
Watermarking	Yes/No	No	No
Steganography	Yes	Yes/No	Yes

Table 2 Types of Key Protocols used in Steganography

Types of Key	Key's Requirements	Security Provided
Pure Key	No need of Stego/Cipher key	Least secure
Secret Key	Need of Secret Key	More secure than pure
Public Key	Need one Public Key and one Private Key	More secure than Secret Key and Pure Key

II. BASIC BLOCK DIAGRAM

The basic block diagram for the steganography is represented in the following figure in which secret file, carrier file or cover file and the secret key is needed for embedding process then with the combination of these files new stego file is generated [8].

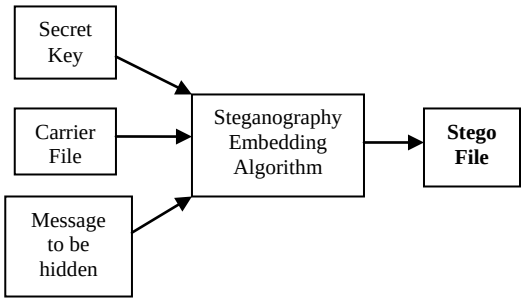

Figure 1. Basic Block Diagram of Steganography

- **Secret key:** It is cipher key using for the data hiding and retrieval.
- **Carrier File:** The particular file that is selected for data hiding and that carrier file may be text, Image, Audio, Video etc.
- **Message to be hidden:** The data that need to hide inside the cover/carrier file and that may be Image, Audio, and Video etc.
- **Steganography Embedding Algorithm:** The process that is used to embed the secret data file inside the carrier files with the help of stego key.
- **Stego File:** The resultant file generated after the processing of embedding algorithm is called as Stego file.
- **Steganography Extraction Algorithm:** The process of extracting the data from the cover file with the help of stego key.

In order to choose the cover media different types of Steganography techniques like Text, Audio, and Video etc. are introduced [9].

III. TYPES OF STEGANOGRAPY

A. Text Steganography

In the text by changing word's positions, by using context-free grammars', by doing the change in the format of text the cover text is produced to conceal the data [10].

B. Image Steganography

To hide the secret message in the pixels of the image and by the proper decoding method we can extract the message from the image. There is different kind of techniques like LSB, PVD, DCT and much more are there for hiding data in images [11].

C. Audio Steganography

Hiding the secret data in an audio or in frequencies which can't audible to the humans and for that purpose there are different techniques like Echo Hiding, Tone Insertion Phase Coding etc. are used [12].

D. Network Steganography

In this technique network's protocol are used as the cover media like TCP, UDP etc. [13].

E. Video Steganography

For the motive of enhancing the capacity of hidden data video steganography is used. In this technique, the different types of data can be hidden in text, audio, image, and video. Because of having the complex structure and high capacity of frames in a particular video we can hide more data in a video file as compared to an image [14].

IV. VIDEO STEGANOGRAPHY TYPES

There are different types of video steganography techniques in which data can be hidden in different formats. As shown in the fig below we can divide the video steganography technique into different types [15].

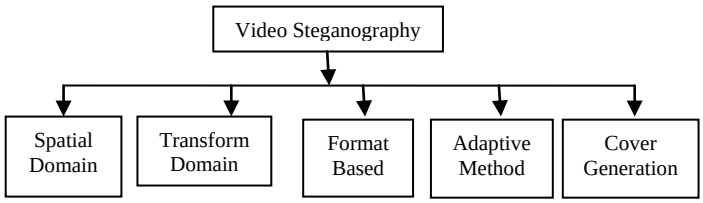

Figure 2. Types of Steganography

A. Spatial Domain(Substitution Based)

In this technique, the raw data is replaced by the secret message that needs to hide. The simplicity is the major advantage of this technique as well as it is very simple to embed the secret data with its high capacity of data embedding. The different types of spatial domain methods are LSB, BPCS, and TPVD etc. [16]

B. Transform Domain(Frequency Based)

In spatial domain technique the secret data can be easily detected by the intruder and to overcome this disadvantage we use transform domain technique. This technique is complex as compared to the spatial domain but it enhanced the security of stego file. The different techniques used are DCT, DWT, and DFT etc.

C. Format Based

Different type of video format file can be used for hiding the secret message. H.264/AVC is one of the compression standards of the video file which are used widely for the hiding mechanism of the secret file. Different format of video files like FLV, AVI, MPG etc. are used for hiding the data.

D. Adaptive Method

A new technique to conceal the data in a secure manner is an adaptive method that can be called "Static aware embedding" or "Masking". In this technique, research is done on the statistical features of the cover file which helps

to find the best place for hiding the data and that place is called ROI means "Regions-of-Interest".

E. Cover Generation

For the secret communication, an object is combined with the cover. The idea was implemented when dynamic cover video generation method is used. In this process, secret key and the secret message are required for the cover generation.

The function used in this is X (A, D) where:

- X= Function which is used to create container file by the use of message
- A= No. of samples needed to conceal the message
- D= Represents bits of message which have to hide [17]

V. LSB(LEAST SIGNIFICANT BIT) METHOD

The secret text is stored in the least significant bit of the frames of the video file. It is the simplest and most widely used method. Because of having simplicity in the work it is very easy to understand and implement this technique in the video file. The secret message is hidden in the video file by selecting a particular frame on the basis of an approach that is applied.

In this paper, LSB technique is applied in such a way that each character of the text message is hidden into the LSB of Frames [18]. MATLAB tools are used for the implementation of this technique. AVI (Audio Video Interleave) format of the video file is used for finding the changes into the cover video frame. Different steps are performed in this technique when the MATLAB coding has done.

Pseudo Code for Embedding Process:

```
1.) for(i=1:length(msg))
 m(i)=msg(i); %% Read the message of definite length and convert the character value in ASCII format.

2.) avi=VideoReader(fin); %%Read the video
 nFrames=avi.NumberOfFrames; %%calculate no. of farmes
 nFrames=floor(avi.Duration*avi.FrameRate); %%video is divided into several frames.

3.) for k=1:1:nFrames %%k is initialized to 1 and loop will run from 1 to n no. of frames.
 mov(l).cdata=read(avi, k); %%read all parameters of the frames
 im=mov(l).cdata;
[r c d]=size(im);
 if(l==1) %%first character of the message is hidden into first frame
 im(r,c,d)=length(m);
 im(r,c,d)=m(l-1); %%decrement in the length of message
 mov(l).cdata=im;
 l=l+1; %%increment in the frames no.

4.)for k=1:1:nFrames
 writeVideo(writerObj,mov(k)); %%write the new stego file
 end
```

Pseudo Code Extracting Process:

```
1.) [fname path]=uigetfile('newfile.avi');
fname=strcat(path,fname);
avi=VideoReader(fin); %%read the path and find the avi file from that

2.) nFrames=avi.NumberOfFrames;
 nFrames=floor(avi.Duration*avi.FrameRate); %%split the file into several frames

3.) Extract the secret message from the stego file.
 for k=1:1:nFrames %%k is initialized to 1 and the loop will go from 1 to no. of frames
 mov(l).cdata=read(avi,k); %%read all the parameters of frames
 A=[A im(r,c,d)]; %%save the message in A one by one
  mov(l).cdata=im;
  l=l+1; %%increment in the frames no.
```

In LSB, least significant bits of the pixel of the cover file are replaced with the secret message. It is the simplest technique which is used in video steganography and the different techniques with the combination of LSB can also be used for the secret communication like DLSB, HLSB, and RSA etc.

VI. RESULTS

Now the cover video that have AVI format and the details of the video file are given below:

Table 3 AVI video file details

Name of the video file	Secret message	Resolution (W*H)	Frames per second	No. of frames	File size
avifile.avi	**Text**	**320*240**	**15**	**55**	**883kb**

To hide the text message of 13 characters in each LSB of frames of cover video file from initial frame and it will be continued until the message is fully embedded.

Table 4 Details of secret data for hiding in the AVI file

Secret data	No. of Characters	Text to be hidden
Text	**13**	**STEGANOGRAPHY**

We have the different type of metrics on behalf of which we check how similar the cover objects after the embedding process. These metrics are discussed below [19].

1.) MSE

MSE stands for Mean Squared Error and it is calculated by the comparison of the stego file and cover file with each of the bytes. We have the following equation to calculate MSE value.

$$\mathrm{MSE} = \frac{1}{[\mathrm{N} \times \mathrm{M}]^2} \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - Y_{ij})^2 \qquad (1)$$

2.) PSNR

PSNR is the parameter of the video file that means Peak Signal to Noise Ratio. PSNR and MSE both are inversely proportional to each other and PSNR can be measured by the following equation.

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{I^2}{\mathrm{MSE}}\right] \qquad (2)$$

3.) RMSE

RMSE is a parameter that means Root Means Square Error which is calculated as the square root of MSE.

These following figures shows the first frame in cover video and the first frame of the stego file after embedding data:

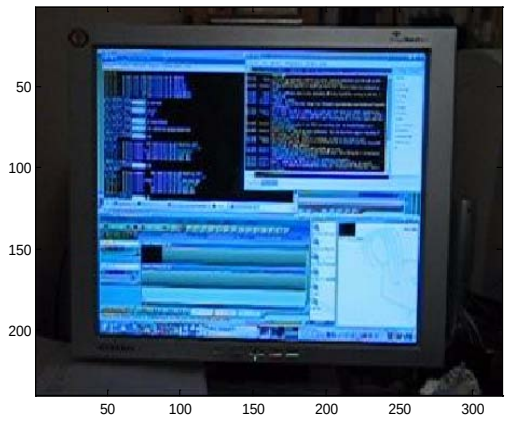

Figure 3. First Frame of the cover AVI video file

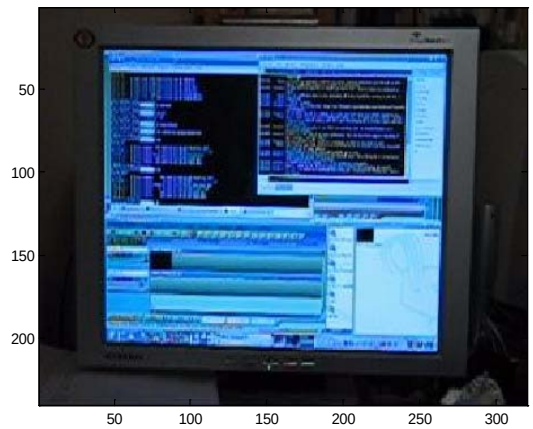

Figure 4. First Frame of the Stego AVI video file

Table 5 The values of PSNR, MSE and RMSE after embedding

Frame No.	MSE	PSNR	RMSE
1.	0.0115	80.4224	0.0244
2.	0.0115	67.5441	0.1074
3.	0.0011	77.6066	0.0337
4.	0.0012	77.4760	0.0342
5.	0.0040	72.1376	0.0633
6.	0.0040	80.7175	0.0236
7.	0.0010	78.1535	0.0317
8.	0.0022	74.6969	0.0471
9.	0.0022	79.0021	0.0287
10.	0.0016	76.0493	0.0403
11.	0.0016	76.1076	0.0401
12.	0.0015	76.3738	0.0389
13.	0.0015	86.7381	0.0118
AVERAGE	0.00345	77.1558	0.04131

VII. CONCLUSION

In this paper, we have analyzed about the least significant bit method of video steganography with the different parameter such as PSNR, MSE etc. The text message hiding process in each LSB of frames of cover video file starts from the initial frame and it will be continued until the message is fully embedded where one character of the secret message is hidden within each frame of the cover video file. The average values of above calculated PSNR, MSE and RMSE are 77.1558, 0.00345 and 0.04131 respectively.

VIII. REFERENCES

[1] Kamaldeep Joshi and Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend With Cryptography For Secret Communication", In Image Information Processing (ICIIP),Third International Conference on IEEE, December, 2015

[2] Swetha V, Prajith V and Kshema V, "Data Hiding Using Video Steganography-A Survey", International Journal of Computer Science & Engineering Technology, Volume-5, Issue-6, June 2015

[3] Kedar Nath Choudry and Aakash Wanjari, "A Survey Paper on Video Steganography", International Journal of Computer Science and Information Technologies, Volume- 6 (3) 2015

[4] Kamaldeep Joshi and Rajkumar Yadav, "A LL Sub Band Based Digital Watermarking in DWT", I.J. Engineering and Manufacturing, March 2017

[5] P. R. Deshmukh and Bhagyashri Rahangdale, "Data Hiding using Video Steganography", International Journal of Engineering Research & Technology, Volume-3, Issue-4, April 2014

[6] Mritha Ramalingam, "Stego Machine – Video Steganography Using Modified LSB Algorithm", World Academy of Science, Engineering and Technology 50, 2011

[7] Anamika Saini, Kamaldeep Joshi and Sachin Allawadhi, "A Review on Video Steganography Techniques", International Journal of Advanced Research in Computer Science, Volume-8, No.3, March-April 2017

[8] Ginni and Pushpinder Singh, "A Review on Secure Video Steganography Technique using LSB & MSB", International Journal of Advanced Research in Computer and Communication Engineering, Volume-5, Issue-3, March 2016

[9] Kamaldeep Joshi and Kirti Sharma, "Techniques of Image Steganography", International Journal of Computer & Mathematical Sciences, Volume-6, Issue-2, February2017

[10] Jasleen Kour and Deepankar Verma, "Steganography Techniques –A Review Paper", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May2014

[11] Kamaldeep Joshi, Rajkumar Yadav and Gaurav Chawla, "An Enhanced Method for Data Hiding Using 2-Bit XOR in Image Steganography", International Journal of Engineering and Technology, Volume-8, No.6, Dec 2016-Jan 2017

[12] Jayaram P, Ranganatha H R and Anupama H S, "Information Hiding Using Audio Steganography – A Survey", International Journal of Multimedia & Its Applications, Volume-3, No.3, August 2011

[13] Amruta B. Bhojane and Priti A. Khodke, "Data Hiding In Video Stream by Text Substitution", International Journal of Science, Engineering and Technology, ISSN (O): 2348-4098 ISSN (P): 2395-4752

[14] Shahd Abdul-Rhman Hasso, "Steganography in Video Files", International Journal of Computer Science Issues, Volume-13, Issue-1, January 2016

[15] Abhinav Thakur, Harbinder Singh and Shikha Sharda, "Different Techniques of Image and Video Steganography: A Review", International Journal of Electronics and Electrical Engineering, Volume-2, Issue-2, 2015

[16] Bharti Chandel and Shaily Jain, "Video Steganography: A Survey", IOSR Journal of Computer Engineering, Volume-18, Issue-1, Jan – Feb. 2016

[17] Mennatallah M. Sadek, Amal S. Khalifa and Mostafa G. M. Mostafa,"Video Steganography: A Comprehensive Review", Published online: 20 March 2014 # Springer Science + Business Media New York 2014

[18] Kamred Udham Singh, "Video Steganography: Text Hiding In Video by LSB Substitution", Int. Journal of Engineering Research and Applications, Volume-4, Issue-5, May 2014

[19] Maninder Pal Singh and Harmandeep Singh, "An Efficient Modified LSB technique for Video Steganography", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Volume-4, Issue-6, June 2015