# A survey of Video Steganography through LSB Insertion

**Dr. Vivek Kapoor**
Asst. Professor, Dept. Of Computer Engineering,
Institute Of Engineering &Technology,
Devi Ahilya University, Indore, India.

**Akbar Mirza**
Dept. Of Information Technology,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

**Abstract-Steganography is a term which is related to secret writing. It is an art of writing your information in an unrecognizable form. It is a supplementary of cryptography. In this paper, we described the different techniques of Steganography and especially video steganography. Video Steganography means when we use video files as a cover and hide data in them. We get through many technologies and made some comparisons between them. In this paper we proposed a methodology that is convenient for more data embedding as well as easy recovery of data from the carrier file.**

***Key words- Encryption, Steganography, Steganalysis, LSB Insertion, Cryptography***
.

## 1. INTRODUCTION

The art of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

Stenographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Stenographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment. Many governments have created laws that either limit the strength of cryptosystems or prohibit them completely. This has been done primarily for fear by law enforcement not to be able to gain intelligence by wiretaps, etc. This unfortunately leaves the majority of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all. Civil liberties advocates fight this with the argument that "these limitations are an assault on privacy". This is where Steganography comes in. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. To add multiple layers of security and to help subside the "crypto versus law" problems previously mentioned, it is a good practice to use Cryptography and Steganography together. As mentioned earlier, neither Cryptography nor Steganography are considered "turnkey solutions" to open systems privacy, but using both technologies together can provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

## 2. BACKGROUND

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists.

### 2.1 Data Hiding Process

Information can be hidden inside a multimedia object using many suitable techniques. As a cover object, we can select image, audio or video file. Depending on the type of the cover object, definite and appropriate technique is followed in order to obtain security. In this section, we will discuss different techniques or methods which are often used in image and video steganography.
Some of them are as follows:-

- Least significant bit insertion (LSB Insertion)
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

*2.1.1 Least significant bit insertion*

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with Message bit. This technique works well for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object.

*2.1.2 Masking and filtering*

Masking and filtering techniques are mostly used on 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected.

*2.1.3 Redundant Pattern Encoding*

Patchwork and other similar tools do redundant pattern encoding, which is a sort of spread spectrum technique. It works by scattering the message throughout the picture. This makes the image more resistant to cropping and rotation. Smaller secret images work better to increase the redundancy embedded in the cover image, and thus make it easier to recover if the stego-image is manipulated.

*2.1.4 Encrypt and Scatter*

The Encrypt and Scatter technique tries to emulate white noise. It is mostly used in image steganography. White Noise Storm is one such program that employs spread spectrum and frequency hopping. It does this by scattering the message throughout an image on eight channels within a random number that is generated by the previous window size and data channel. The channels then swap rotate, and interlace amongst each other. Each channel represents one bit and as a result there are many unaffected bits in each channel. This technique is a lot harder to extract a message out of than an LSB scheme because to decode you must first detect that a hidden image exists and extract the bit pattern from the file.

*2.1.5 Algorithms and transformations*

LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF etc . JPEG images use the discrete cosine transform to achieve compression. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT.

## 2.2 Cryptography Vs Steganography

Steganography means “cover writing” whereas cryptography means “secret writing”. Steganography is often confused with cryptography but there is substantial difference amongst two. The former uses a cover to hide the information and send it to the network. It is difficult for any unintended user to determine whether there is any secret information embedded or not. The important characteristic with steganography is that the cover should be chosen with enough redundant information so that even after embedding the message, it is not easy to detect for the message after looking at the message. Whereas, cryptography involves encrypting the message such that either it becomes unreadable or the original meaning of the message is entirely changed.

Steganography does not alter the structure of the secret message whereas, cryptography alters the structure of the secret message. Former prevents the discovery of the existence of the communication whereas latter prevents unauthorized user from discovering the contents of a communication.

Both the techniques can be combined to provide one more level of protection. The message can be first encrypted using cryptography to a cipher text. This cipher text then can be embedded In a cover media using steganography. This combined approach will satisfy the three goals of data hiding: security, capacity, robustness.

## 3. LITERATURE SURVEY

For studying the concepts of video steganography, we have surveyed many research papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography.

In Paper [1], Author proposed an advance approach for Video Steganography. The author uses LSB based methods for hiding the data and Advanced Encryption Standard for encrypting it. Author applied 1 bit, 2 bit and 3 bit LSB insertion scheme.

| S. No. | Author Name | Publication & Year | Technique Used | Topic Name | Outcome |
|---|---|---|---|---|---|
| **[1]** | Hemant Gupta And<br>Setu Chaturvedi | IJCSNS,<br>March<br>2014 | LSB<br>Based<br>Insertion | Video Steganography through LSB Based Hybrid Approach | Improved PSNR & Correlation Factor |
| **[2]** | S.S. Divya, M. Ram Mohan Reddy | IJOSTR,<br>July<br>2012 | LSB with RSA | Hiding text in audio using multiple lsb steganography and provide security using Cryptography | Lossless Recovery Of Data |
| **[3]** | Sherly A P and Amritha P P | IJDMS,<br>August<br>2010 | Tri-way<br>Pixel value<br>differencing | A Compressed Video Steganography using TPVD | High Imperceptibility And Capacity |
| **[4]** | Kousik Dasgupta, J.K. Mandal and Paramartha Dutta | IJSPTM,<br>April<br>2012 | Least<br>Significant<br>Bit<br>Insertion | Hash Based Least Significant Bit Technique<br>For Video Steganography(Hlsb) | Comparatively High Performance |
| **[5]** | Mritha Ramalingam | WASET,<br>February<br>2011 | Modified<br>LSB<br>Based<br>Technique | Stego Machine – Video Steganography using Modified LSB Algorithm | Platform-independent application with high portability and high Consistency. |

Information is covered by Video frames. Author used AVI format of Video because of its larger size, embedding data become easy and for sending it over network he then converted into frames of 8 bits.

This author is mainly concerned with how to embed data in a video file in form of BMP images and how we can make use of the internal structure of the video to hide data to be secured. The basic concept of this author which we have used in my research work and the second concept which has been implemented in our research work is how to use steganography using video file as a cover carrier.

Paper [2] is based on Audio Steganography but uses the same concept of LSB insertion. It is desired to maximize the lossless recovery of data from the cover object like audio, video or image. It help us to recover our hidden messages from Video frames.

In Paper [3], Author proposed a new Compressed Video Steganography scheme. Author defines a new way called tri-way pixel-value differencing (TPVD) that is used for embedding. In this scheme all the processes are defined and executed in the compressed domain. Though decompression is not required. The proposed algorithm has high imperceptibility and capacity. This algorithm provides high capacity and imperceptible stego-image for human vision of the hidden secret information. It gives us the idea of using Steganography in Compressed video domain like MPEG and hide information in the pixels of images.

In Paper [4], 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. This technique works on AVI and FLV video extension. In our study we learned that this technique is very helpful in undetectability from the techniques that are currently used in Steganalysis.

In Paper [5], Author designs a stego machine to develop a steganographic application to hide data containing text in a computer video file and to retrieve the hidden information. This can be designed by embedding text file in a video file in such a way that the video does not loose its functionality using Least Significant Bit (LSB) modification method. This technique is based on secrecy and imperceptibility of the hidden information. This technique gave us the idea of using JAVA as a platform and a good GUI (Graphical User Interface).

## 4. PROPOSED WORK

The proposed system is a stegnographic system by which the targeted data is hide on a given mask video frame. The given figure 2 shows the demonstration of the proposed stegnographic technique.

According to above given diagram the video file is first pre-processed for extracting the frames from video. After that the original text which is desired to hide in video is compressed first thus the amount of data is reduced significantly. After that a cryptographic algorithm is applied on the compressed data. Form the compressed data a pair of bits is extracted. On the other hand video file is processed to extract the video frames from file. In these color files each pixel is denoted using three pixel values <R, G, B>. each of the color pixel is thus defined using 24 bits here the LSB of each color channel is manipulated using the extracted bit pairs. And combined file video file is reconstructed.

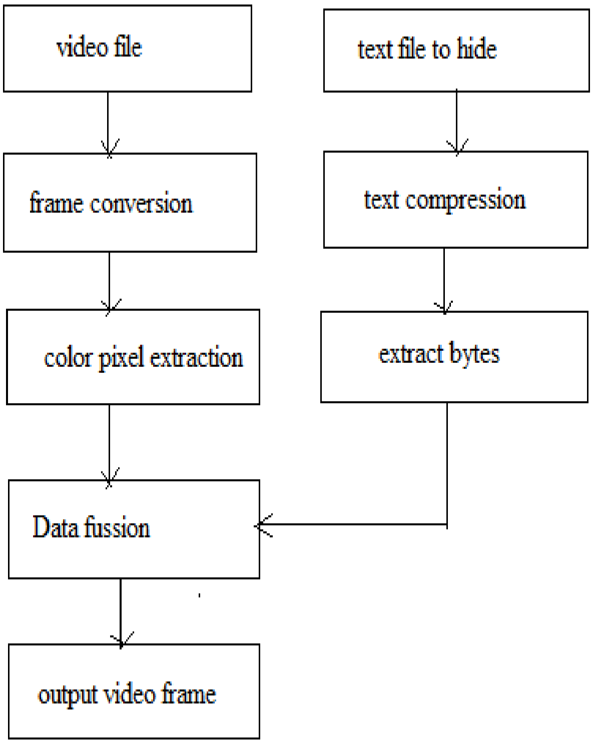

**Figure 1 proposed methodology Subsystem Architecture**

The functional overview of the proposed stegnographic 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.

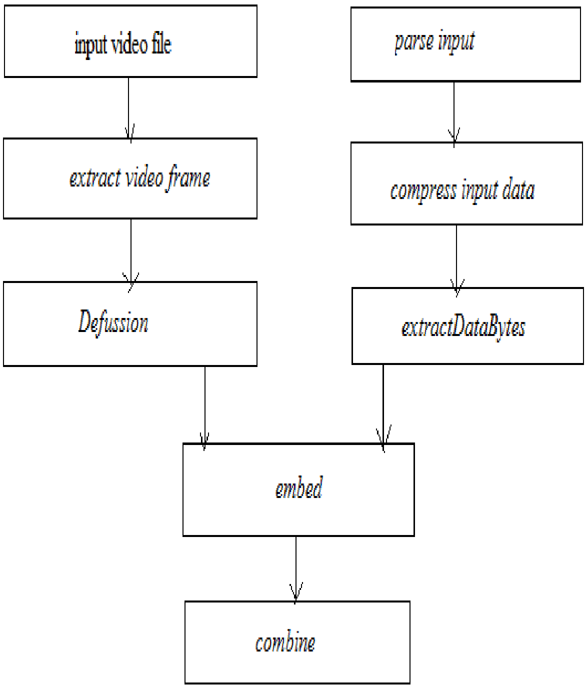

**Figure 2 subsystem**

## 5. Conclusion and Future Work

In our survey we conclude that neither Steganography nor Cryptography is a turnkey solution for all hacking activities. We can reduce them to a certain level. So we proposed a methodology that will be helpful in embedding data secretly and becomes undetectable through Stegnalysis. And this method also helpful in embedding large amount of data in a carrier file. The proposed method is also compatible with cryptography, we can use it in future. Performance analysis shall be published in next paper.

## 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] DebiprasadBandyopadhyay, KousikDasgupta, J. K. Mandal, ParamarthaDutta, “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] FrédéricLusson, Karen Bailey, Mark Leeney, “A Novel Approach to Digital Watermarking, Exploiting Colour Spaces”, MASAUM INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY 2012

[5] Manoj Kumar and Arnold Hensman, “Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography”, ISSC 2013, LYIT Letterkenny, June 20-21

[6] Saranya K , Mohan Priyar, Udhayan J, A Review on Symmetric Key Encryption Tec hniques in Cryptography, International Journal of Science, Engineerin and Technology, Volume 3, Issue 3, March 2014

[7] Marghny Mohamed”Data hiding by LSB substitution using genetic optimal key permutation
[10] M.Wu ,E. Tang and B.Liu,”Data hiding in digital binary image ,”in IEEE ICME New York City, NY,USA ,July 2000.

” in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.

[8] ]P.Karthigaikumar “Simulation of image encryption using AES algorithm”IJCA special issue on computer science New dimensions &perspectives, 166-172, 2011.

[9] M.Wu, Hiding in image and video Part I fundamental issues and solutions ,IEEE Trans Image processing,12(6):685-686, 2005.

[11] J.L. Rodgers, J. L. and W.A. Nicewander, “Thirteen Ways to Look at the Correlation Coefficient”, American Statistician 42, 59-66 ,1995.