# SECURE DATA HIDING AND DATA EXTRACTION INTO VIDEO

**Prof. Hemangi Kute[1], Prof. Poonam Pate[2], Prof. Akshita Chanchlani[3], Prof. Pawan Pate[4]**

[1, 2, 3] *Assistant Professor, Computer Department, Sinhgad Academy of Engineering, (India)*

[4] *Assistant Professor, Electrical Dept., VDF School of Engineering, Latur, (India)*

## ABSTRACT

*This paper proposes a novel scheme to hide a data in video. Today's world is known as world of Internet, but exchanging data over internet is not secure. Many times problem arise related to data security. So to secure data (message) the concept of Steganography is used. In this system sender encode the data in video and saves the data encoded video. Sender sends the video to receiver using exiting mail system. Receiver now decodes the data encoded in video. Data encoding and decoding into video can be done by using LSB Replacement or Substitution Techniques. There is no difference in a video and video encoded with data.*

***Index Terms: Data Abstraction, Data Hiding, Data Extraction, Video Encryption, Steganograohy***

## I. INTRODUCTION

Now days the security of data or information is indispensable factor for security of the data. Because of getting more popularity to internet as well as digital media, requirement of transmission of data securely is increased. In present there are many systems available in market which uses concept of Steganography. Such as ImageHide2.0, Steganography1.50, etc. But the drawback of these systems is they can hide message in only Image and audio file format. The size of the image and audio file is comparatively small to hide long message or data.

So we are designing the system which can hide the message inside the video file and that message will be encrypted.

Steganography is the art and science of hiding Secret message. Steganography is a term coming from the Greek words **stegos** which means that "roof or covered" and **graphia** means that "writing". That is Steganography is covered writing.Using Steganography, you can embed a secret message inside a video and send or store it without anyone knowing of the existence of the secret message.

The goal of this system is to hide data (message) in video and retrieve that message whenever needed. This system is data (message) hiding system, which encodes the secret data into video file and decodes video file to get original message back. This system allows user to store message more securely. Hence user can send secure information over unsecure network. As encrypted data is hided in to video so generally hacker is not able to identify that the file which he has hacked, contains some message.

This system allows authorized user to encode text message into video file format and decode it using same system to get original text message. It is necessary to have this system with both sender and receiver.

## II. PROPOSED SCHEME

We are proposing the system "Implementation of Steganography using video" which is very simple to interface and providing useful utilities for security of data. This system will allow user to encode video with hidden message and decode video to get back original message. This system will hide the data in video file and for that purpose we will use the LSB Replacement Technique or Substitution Technique.

The system will be basically divided into two parts. That is embedding and retrieving of message. The basic part for embedding the message will be hiding message into video and second module that will be used for retrieving the message which will be hidden into these video.

A sketch of proposed scheme is given in below Fig. 1. At the sender side, the owner of the image first selects the video and then he types the message which he wants to encode into the video. Then the data hider, without any knowledge of original video content, hides the data (message) using data hiding key. The data (message) encoded video is then stored. When we see the original video and data (message) encoded video then there is no difference between this original video and data encoded video.

The data (message) encoded video is mail to the receiver. At receiver side, data accessor can extract the data from video using same data hiding key and data accessor will separate out the video and message. Now receiver will get the original message send by the sender.

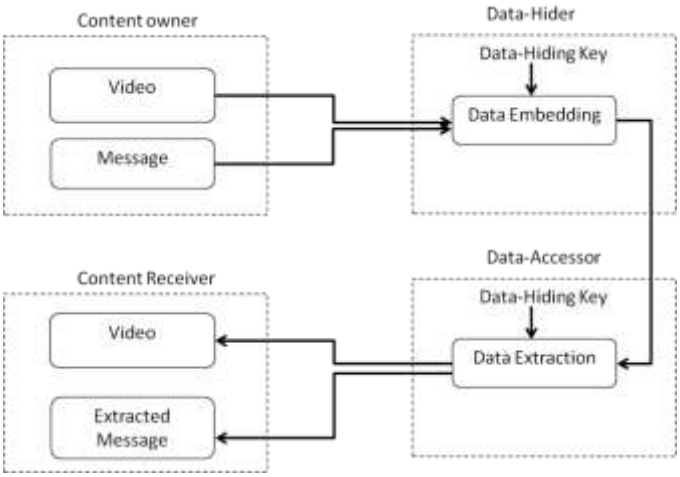


**Fig.1. Sketch of the Scheme**

There are two basic operation or process are used

### 2.1 Encoding Process

This system performs Encode process. User selects input video file (i.e. Source video), from where information of video is collected. User also provides output video file where encoded video is going to be stored with message to be hidden. For encoding purpose LSB Replacement or Substitution Technique is used.

In data embedding phase, some parameters are embedded into a small number of pixels. LSB of the other pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. According to a data-hiding key, the data-hider pseudo-randomly selects encrypted pixels that will be used to carry the parameters for data hiding.

The other pixels are pseudo-randomly permuted and divided into a number of groups. For each pixel-group, the data hider collects the least significant bits of the pixels.

The data-hider generates a matrix which is having two parts; the left part is an identity matrix, the right part is a pseudo-random binary matrix. This pseudo-random binary matrix is derived from the data-hiding key. Then, embed the values of the parameters into the LSB of selected encrypted pixels. At the same time the most significant bits (MSB) of all pixels are kept unchanged.

When the video files are created, there are usually some bytes in video file that are not required or not important. These areas of a given video file can be replaced with data (message) that is to be hidden without damaging the original video. Such type of method is called as LSB replacement Method. Generally this method is used for Image and video files. The value 11111111 can be replaced by 11111110. This Least significant bit change is unpredictable by Human Eye.

**Example**

Videos are made up of number of frames and each frame consists of thousands of pixels. We are dividing given video into number of frames. Each pixel is made up of RGB (Red, Green and Blue) color. Each color of RGB is represented by 8-bits of data. Consider a given example that represents three pixels of a one of the frame of given video. Here each pixel is represented with RGB color.

| | R | G | B |
|---|---|---|---|
| 1st Pixel | (10101111 | 11101011 | 11011001) |
| 2nd Pixel | (11011011 | 11001001 | 00001001) |
| 3rd Pixel | (11001010 | 00100100 | 11011111) |

So we use three pixels to store one byte of message. Suppose we want to store or encode character A.

Let Character A=10000001, is inserted, the following result occurs-

| | R | G | B |
|---|---|---|---|
| 1st Pixel | (10101111 | 11101010 | 11011000) |
| 2nd Pixel | (11011010 | 11001000 | 00001000) |
| 3rd Pixel | (11001010 | 00100101 | 11011111) |

So resulting pixel of video have slightly changed values which is undetectable by Human Eye.

**2.2 Decoding Process**

Decoding process is exactly opposite to encoding. Here we simply read only LSB (least significant bit) of pixels. And then combine these bits into bytes. Each byte will represent a character. These characters in turn form a message. In this way we get the original message.

**Example**

As we already encoded message into video. We will consider encoded pixel of above example,

| | R | G | B |
|---|---|---|---|
| 1st Pixel | (10101111 | 11101010 | 11011000) |
| 2nd Pixel | (11011010 | 11001000 | 00001000) |
| 3rd Pixel | (11001010 | 00100101 | 11011111) |

This produces bit sequence 10000001, where 10000001 presents A. So message retrieved is A.

## III. SYSTEM INFORMATION

Below Fig.2 shows the system flow diagram. These diagram shows sender side as well as receiver side operations. Here sender first login the system. Sender enters user name and password and authenticates himself. After successful registration sender selects the video that he want to send and also the message that he want embed into that video. Data hider uses the data hiding key to embed the data into video. After that sender saves the data (message) embedded video. Later on sender send the video through current mailing system. And sender sign out the system. At receiver side, receiver first select the video that he wants to access the message. Data accessor displays the message using data hiding key to receiver. After getting the embedded message receiver sign outs the system.

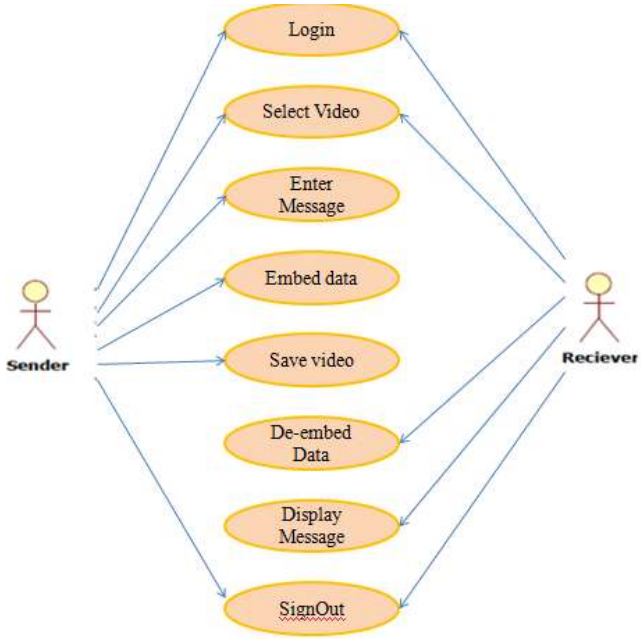


**Fig. 2 System Flow Diagram**

### 3.1 Hardware Requirement

| | | |
|---|---|---|
| Computer processor: | | Pentium IV onwards |
| Clock speed | : | 1.2 GHz Processor |
| Hard Disk | : | 10 GB minimum |
| RAM | : | 128 MB minimum |

### 3.2 Software Requirement

| | | |
|---|---|---|
| Operating System: | | Windows family O.S. |
| Language | : | Java |
| Tools | : | jdk 1.6.0, Net Beans 7.2.1 |
| Server | : | Mongo DB |

## IV. TESTING

Testing is one of the important step to be performed to ensure successful implementation of the system .The basic idea of carrying out testing is to ensure no error exits in the functionality and operability of the program. Therefore the most useful and practical approach is with intension of finding errors .This is the phase where the system is intentionally made to fail so as to make the system full proof and error free up to the limit possible.

Initially Test data is prepared to check the software. During this phase the system is used experimentally to ensure that the software does not fail. Special test data are inputs for processing and the result is examined. It is very essential for increasing its effectiveness and accuracy.

The testing of system is necessary to ensure the following issues: Completeness, Correctness and Reliability.

In general the system was thoroughly checked at each level, right from the beginning. System was checked at different levels.

- Testing of data entry procedures is done.
- Testing of data validation id done.
- Entering data via different screens (forms) is done.
- Testing for data insertion and updation is done.
- Record saving procedure is done.
- Error routines were checked.

Again here time complexity also checked. Video with larger size require more time to embed the data (message). And video having less size require less time to embed the data (message) into video. For video testing, run both the video on separate machine simultaneously. And see the difference between two video that is before and after data (message) embedded to video.

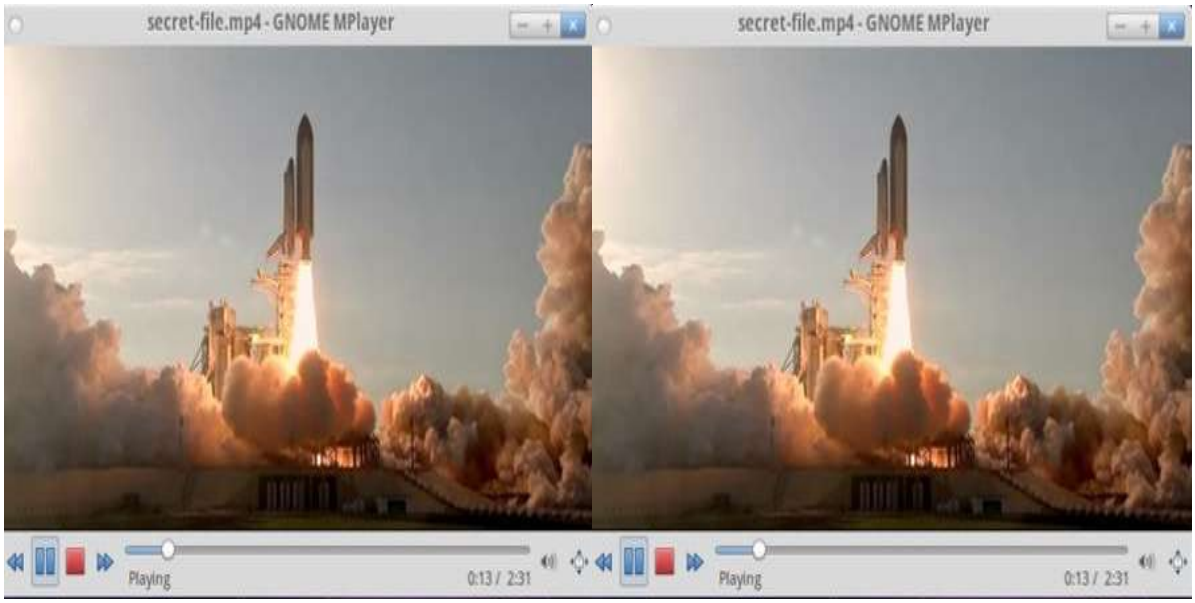


**Fig 3 Video before embedding the data (message)** **Fig.4 Video after embedding the data (message)**

After seeing both Fig 3.and Fig 4., we found that there is no any difference between video before embedding and after embedding the data (message) into video. Because of LSB replacement techniques, Human eye cannot be able to predict this small LSB change in pixels of different frames of a given video. As frames moves very fast and continuously it is unpredictable to fine such small change in video.

## V. CONCLUSION

In this paper, data hiding in video using Stegnography is proposed. This system mainly consists of data hiding and data extraction process. Data hider hides the data (message) into video using data hiding key. The data acessor access the data from video by using same data hiding key. The sender or receiver who's having this system only knows the user name and password. By using this username and password sender as well as

receiver authenticate himself. First sender can select his video and enter the message that he want to send and click on encode button to embed the data (message) into video. After successful data embedding process sender saves the data embedded video. When we run the video before and after data (message) embedding, there is no difference between both the videos. Sender sends the video to receiver. Receiver again login the system and authenticate himself. Receiver use these video and press the decode button. Data accessor displays the embedded data (message) to receiver. In this manner receiver get the data. Thus, the event of embedding data (message) into video and extracting data (message) from video is achieved successfully with the proposed system.

## REFERENCES

[1] X. Zhang, "Separable Reversible data hiding in encrypted image," IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[4] Kessler, G. An Overview of Steganography for the Computer Forensics Examiner. [online] 2004 February. Available at http://www.garykessler.net/library/fsc_stego.html; Accessed on 02 July 2004.

[5] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.*

[6] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process., vol. 19, no. 4,*pp. 1097–1102, Apr. 2010.

[7] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,*pp. 53–58, Feb. 2011.

[8] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.*

[9] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.*

[10] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.*