# Video Steganography

MrudulDixit[1] Nikita Bhide[2]Sanika Khankhoje[2]Rajashwini Ukarande[2]
dixitma@yahoo.comnikitavbhide@gmail.comsanika.k20@gmail.comrajashwiniub@gmail.com

[1]Lecturer, [2]Students
[1, 2]Department of Electronics and Telecommunication
MKSSS's Cummins College of Engineering for Women
Pune, India

***Abstract* -The use of internet has increased tremendously over the years and the concept of data security is gaining momentum. Data could get corrupted if attacked by a virus or a hacker. The data needs to be protected from unauthorized users to prevent undesired actions. This paper deals with data security in which secret data is embedded in cover video. A methodology for creation of a stego video is defined using the Least Significant Bit (LSB) Replacement algorithm. The secret data to be hidden is replaced at the LSB positions of pixels of the carrier video frame. Thus it becomes very difficult for an intruder to guess that data is hidden in the video and the purpose of data security can be achieved. The performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) can be calculated to test the quality of stego video.**

***Keywords* –data hiding, LSB replacement, Mean, MSE, PSNR, steganography.**

## I. INTRODUCTION

The data that is transmitted has to be protected from various threats and only the receivers that are intended to receive the data should have access to it. Data security deals with protection of data from corruption and unauthorized access. Encryption and masking are two of the common data security technologies. It is essential for protection against different types of intruders who can hack the transmitted data. Apart from hackers, data can also be vulnerable to virus attacks, which can be secured using anti-virus software. Two common techniques of data security are Cryptography and Steganography. Cryptography is the process of converting ordinary information into unintelligible text. Steganography is an art of concealing data into a cover file.

Fig. 1. Data Security

## II. DATA SECURITY TECHNIQUES

### *A. Cryptography*

Cryptography is where security engineering meets mathematics. Cryptography is the art of physical scrambling of information using rearrangement and substitution ciphers which can only be read correctly by targeted person having the key. A video is a moving stream of number of images, so high amount of data can be embedded in it. Its relative complexity also gives an advantage over other types of media such as image and audio in terms of security against intruders.

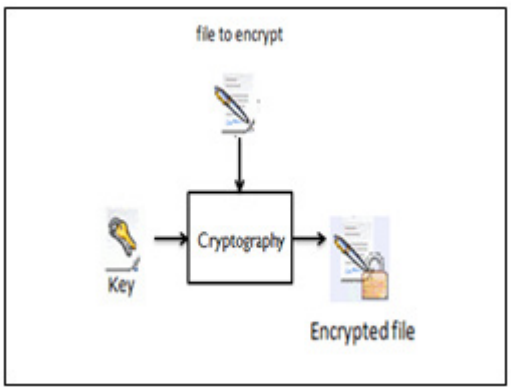



Fig. 2. Cryptography

### *B. Steganography*

Steganography is a technique that enables party to transmit data or message to another without the communication being perceptible to others. The message is embedded in cover media in a manner that only the sender and intended receiver have knowledge of the existence of the message, and the method to retrieve it. Steganography involves hiding the contents inside a file and not scrambling the data, so it is structurally unmodified and intact. Thus, Steganography has an advantage over cryptography as it involves both encryption and obscurity. Image, text, audio can be the cover media. Data in the form of text, audio and video can be embedded in the carrier. The most commonly used carrier is image. To transmit much higher amount of secret data, a video can be used instead.

978-1-4799-6272-3/15/$31.00(c)2015 IEEE

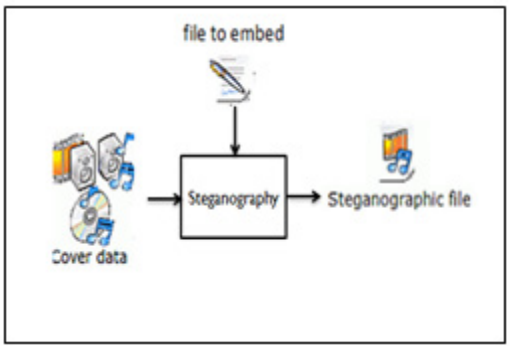



Fig. 3. Steganography

## III. VIDEO STEGANOGRAPHY

Video Steganography is a technique to hide any kind of files into a cover Video file. The use of the video based Steganography can be more secure than other multimedia files, because of its size and complexity.

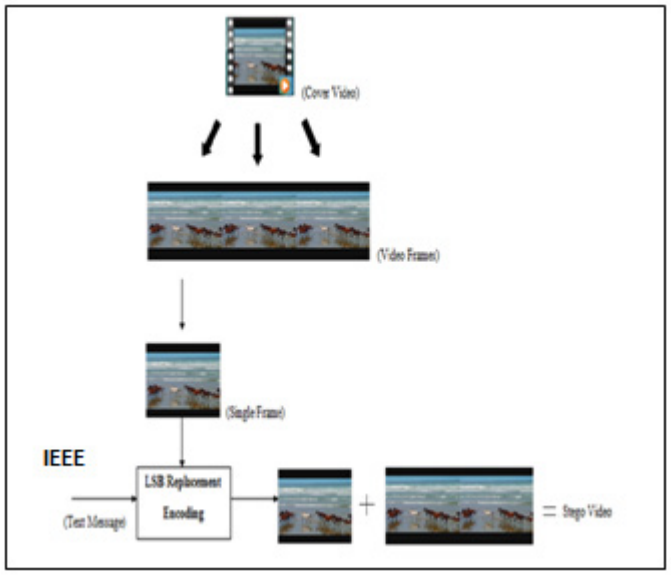



Fig. 4. Video Steganography

## IV. IMPLEMENTATION OF LSB BASED VIDEO STEGANOGRAPHY

The methodology proposed for achieving end result is the creation of a stego video which contains the secret data embedded in the cover video. At the receiver side, the cover video is split into frames and secret data is extracted. The secret data can be embedded in a single frame of the video or in multiple frames, to increase the complexity and security. The technique should satisfy both imperceptibility and robustness.

### *A. BLOCK DIAGRAM DESCRIPTION*

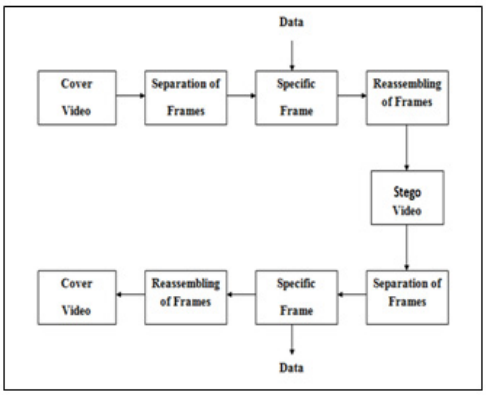



Fig. 5. Block Diagram

In the encoding technique the video in which the data is hidden, is called as the cover video. The frames of the cover video are separated and saved individually as .bmp images. A specific frame (image) is accessed, and the secret data is hidden in the frame using a suitable algorithm. The modified frame (with data) is integrated with the rest of the frames to generate a stego video. The cover video along with the secret data hidden in it forms the stego video. Similar procedure is followed in the reverse manner for decoding. The frames of the stego video are separated, data is extracted from the specific frame in which it is hidden, the frames are reassembled to obtain the original cover video.

### *B. 2-3-3 Based LSB Replacement*

LSB replacement algorithm is used for implementing steganographic algorithms. The video is read and separated into frames. The carrier video frame is read and its pixel values are converted into equivalent binary values. The secret information which is in the form of text, image and audio is converted into binary values and replaced at the LSB positions of pixels of the carrier video frame. The term 'Least Significant Bit' is based on the numeric significance of bits that make up a byte. The most significant bit or MSB has highest arithmetic value ($2^7$=128), whereas LSB has lowest ($2^0$=1).In this technique, 8 bits of secret data are embedded in the least significant bits of pixel values of Red, Green and Blue planes of carrier frames. The first 2 bits of the secret data are concealed inside 2 bits of LSB of Red pixel and similarly 3 bits each in LSBs of Green and Blue pixel values.

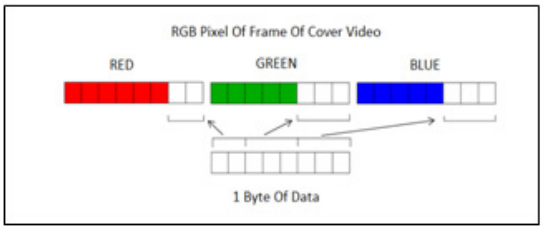



Fig. 6. RR-GGG-BBB based embedding technique

## V. RESULTS AND ANALYSIS

The analysis of stego frame for two videos was done by evaluating following parameters:

1) *Peak Signal to Noise Ratio (PSNR):*
Peak Signal to Noise Ratio (PSNR) is defined as the ratio of the maximum signal power and the power of corruptingsignal.

2) *Mean Square Error (MSE):*
The mean square error (MSE) is the square of the differencebetween the data and its approximation, divided by the number of elements.

3) *Mean:*
The mean is the arithmetic average of a set of values.

### *A. TABLES*

TABLE I. Mean of first frame for different videos (reference values)

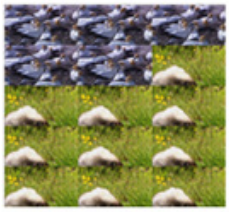
| Parameter | Video 1 | Video 2 |
|---|---|---|
| Mean of First Frame | 102.9759 | 116.7633 |

TABLE II. Analysis Parameters

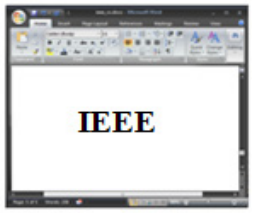
| Parameter | First Frame of Video 1 | First Frame of Video 2 | Ideal Values |
|---|---|---|---|
| Mean | 102.9760 | 116.7633 | Reference |
| PSNR | 95.5002 | 94.9887 | Infinity |
| RMSE | 0.0043 | 0.0045 | Zero |

### *B. FIGURES*

(A)



(B)

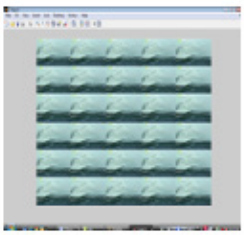



(C)

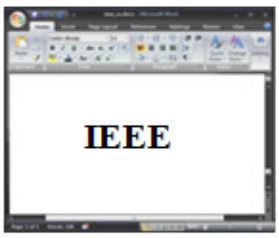
(D)

Fig. 7. For video 1: (A) cover video (B) frame conversion (C) secret data (D) stego video

(A)



(B)




(C)

(D)

Fig. 8. For video 2: (A) cover video (B) frame conversion (C) secret data (D) stego video

## V. CONCLUSION

Data hiding using LSB replacement technique has been implemented and tested for video steganography. Embedding of text in cover video was implemented. To check the quality of stego video, parameters like difference between mean of the cover frame and the stego frame, PSNR and RMSE were evaluated. Results showed that LSB technique is robust and requires less computation time.

## REFERENCES


[1] Saurabh Singh and Gaurav Agarwal, “Hiding image to video: a new approach of LSB replacement”, International Journal of Engineering Science and Technology, Vol. 2(12), pp. 6999-7003, 2010.

[2] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography", IEEE Security & Privacy Magazine, Vol. 1, Issue 3, pp. 32-44, June 2003.

[3] M Abhilash Reddy, P. Sanjeeva Reddy and GS Naveen Kumar, “DWT and LSB algorithm based image hiding in a video”,International Journal of Engineering Science & Technology, Vol.3, Issue 4, pp.170-175,2013.

[4] A. Hamsathvani, “Image hiding in video sequence based on MSE”, International Journal of Electronics and Computer Science Engineering, Vol. 1, no. 3, IISN pp. 1489-1493.