RESEARCH ARTICLE OPEN ACCESS

Video Steganography: Text Hiding In Video By LSB Substitution

Kamred Udham Singh*
*(Department of Computer Science, Faculty of Science Banaras Hindu University, Varanasi, (U.P.), INDIA)

ABSTRACT
The development of high speed computer networks and Internet has increased the easiness of Information Communication. In contrast with Analog media and Digital media provide several different advantages such as high quality, simple editing, high loyalty copying and authenticity. But in the field of data communication this type of development has increased the fear of sneaking the data while sending data from the sender to the receiver. Due to this reason Information Security is main problem of Data Communication. Steganography plays an important role in field of Information Security. Video and images are very common choice for hiding data. It is very important for effective and successful embedding process to select appropriate pixels in the video frames, which are used to store the secret data. We use video based Steganography because of large size and memory requirements. Hiding information in a carrier file we use least significant bit (LSB) insertion technique. In Least significant bit (LSB) insertion technique, for hiding information we change LSB of video file with the information bits .This paper will focus on hiding information in specific frames of the video and in specific position of the frame by LSB substitution.

Keywords **-** Steganography, cover video, stego-video, secret message, Data hiding, LSB bit method

I. INTRODUCTION

Steganography is a Greek word which means "covered or hidden writing". The idea of steganography is thousands of years old. The Greek soldiers used to pass secret message they shave a slave's head, tattoo a message on his head when the hair grow again then the tattoo could not be seen. Receiver shaves the head of slave and gets the message from the tattoo [1]. Invisible ink was also used during the World War II. Watermarking and fingerprinting are closely related to steganography. Data hiding can be used for secret transmission. Steganography is a technique for hiding secret information in digital image, audio and video to secure information from third party [2]. Different kind of techniques are proposed and already taken into practice. The capacity of steganography is in hiding the private data by indistinct, hiding its existence in a non-secret carrier file. In this sense, steganography is differing from cryptography, which involves creating the content of the secret information unreadable while not stopping non-intended viewers from learning about its existence.

Steganography apply in various fields such as military and industrial applications. Lossless steganography techniques are use for secure and successful transmission of information from sender to receiver. Usually, steganography was based on hiding secret message in digital image files. Recently, the computer programmers start interest applying steganographic techniques to video files as well as audio files.

This time multimedia objects like image, audio, video are used as a cover media by steganographic systems because public often send digital pictures in email and other Internet communication. The image file formats are JPEG, GIF, BMP, audio file formats are WAV, MP3, and video file formats are MPEG, MP4, and AVI [3]. On the basis of nature of cover item, Steganography technique can be separated into five types [4].

1. Image
2. Audio
3. Video
4. Text
5. Protocol

II. Requirements of Hiding Message in Digital Object:-

There are various embedding techniques that enable us to hide secret message in a given object. Meanwhile, whole methods definitely assure almost all the requirements so that steganography can be apply accurately [5].

Steganography techniques must satisfy these following requirements:

a) The integrity of the hidden data must be accurate after embedding it inside the stego object.
b) Robustness- The hidden data should be survived through any processing operation through which host signal undergoes and protect its loyalty.
c) Capacity-Maximize data embedding payload.
d) The stego object must stay unmodified or almost unmodified to the bare eye.
e) Security- Use a security key.

f) At a final point, we always presume that the hacker knows that there is hidden data inside the stego object.

Data hiding in object is the different idea than cryptography, but it uses some basic principles of cryptography [6].

III. Basic Model

The given figure depicts simple representation of embedding and extracting process in steganography. In this figure, a secret message is being embedded inside a digital video to produce the stego video using data embedding technique.

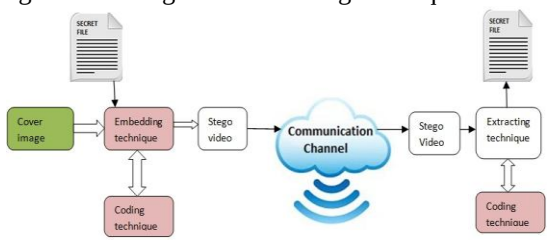


Figure 1 Structure of Steganography System

When stego object is produced then, it will be send via some public communications channel to receiver. The extracting process is simply the reverse of the embedding process. The receiver must decode the stego object to view the secret message by applying an extracting algorithm/technique.

3.1 Digital video basics

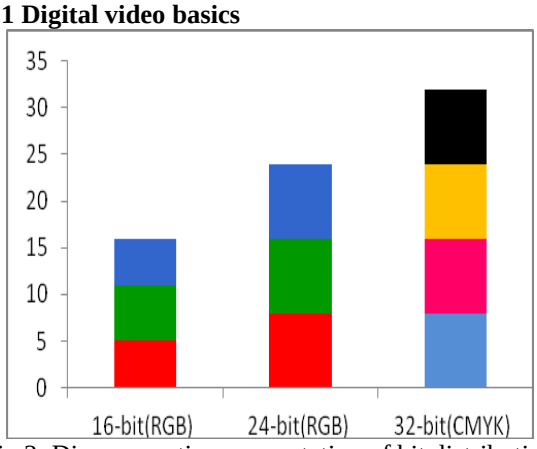


Fig 2: Diagrammatic representation of bit distribution of 16-bit (RGB), 24-bit (RGB), 32-bit (CMYK) digital image

Digital video contains a set of frames (images) which are played back at fixed frame rates based on the video standards. Digital video Quality depends on the combination of parameters like the fps (frames per second), the number of pixels in a frame, and frame size .The fps parameter standard is very common video formats, it's value lies between 24 and 30 fps but the other two parameters, the number of pixels in a frame and frame size present a number of modified from one video standard to another. Every image in a video called a frame which contains number of pixels having three or four color combinations like RGB (Red, Green, Blue) or CMYK (Cyan, Magenta, Yellow, Black). The rest of the mediator colors are composed from a mixture of these primary colors [7], [8].Because the human eye is mainly sensitive to green color, in few video standards the number of bits of every color combination may vary. Figure2 depicts 16-bit color standard in which red and blue colors are containing 5 bits while the green color containing 6 bits .In 24-bit RGB color standard, each red, green, and blue color containing 8 bits in length and has 256 alternatives in color density. On the other hand 32-bit CMYK color standard is required and this standard is generally used in modern computer displays [9].Audio Video Interleave (AVI) is a most common sequence video format advanced by Microsoft and IBM as a part of RIFF (Resource Interchange File Format) in 1992. It contains various sequences of dissimilar data types like audio and video sequences which stores images in BMP (Bit Map) format. Thus, without any major changes in AVI video sequences capacity and resolution computations of bitmap images can be applied.

IV. Video/Image Steganography

Today on the internet the most popular image formats are Graphics Interchange Format (GIF), Portable Network Graphics (PNG) and Joint Photographic Experts Group (JPEG). Most of the advanced techniques not use the structures of these formats but they use the Bitmap format (BMP) for its easy data structure [9].We use digital images for steganography because of the weaknesses in the HVS (human visual system) which has a low sensitivity in random pattern changes. Due to this weakness the secret message can be hiding into the cover video or image without being noticed. As we described above, a digital video contains a set of frames (digital images) which are played back at fixed frame rates based on the video standards. An image is a collection of pixels and each pixel is a mixture of three primary colors RGB (Red, Green and Blue). Pixels in the image are show row by row horizontally. Data hiding in the video/images get less troubled as contrasted to other multimedia files. When data is hiding in an image its size increase .So compression techniques are required. Video/image size can be decreased by compression technique. There are two type compression techniques lossy and lossless.

Algorithm of LSB with an Application The proposed algorithm, both for encoding and decoding along with application are given in this section. Embedding and extracting technique is given.

Algorithm of Embedding
Step 1: Input video object file.
Step 2: Read required message of the video.
Step 3: Split the video into frames.
Step 4: Find LSB bits of the cover frame.
Step 5: Get the position for embedding secret message using function given in equation 1.
Step 6: Regenerate video frames.

Algorithm of Extracting
Step 1: Input stego video file.
Step 2: Read required message from the stego video.
Step 3: Split the video into frames.
Step 4: Find LSB bits of the stego frame.
Step 5: Obtain the position of embedded bits of the secret message using function given in equation 1.
Step6: Regenerate video frames.

V. Proposed Approach

This proposed approach is based on video Steganography for hiding message in the video image, retrieving the hidden message from the video using LSB (Least Significant Bit) modification technique. LSB steganography techniques widely used image in based steganographic and examine under what conditions an observer can differentiate between stego-images) and cover-images. Fig-3 depicts two video images, one is the carrier image of the message and the other image is Stego image which contain the hidden message. To identify the difference between the original video and the Stego video image is not possible.

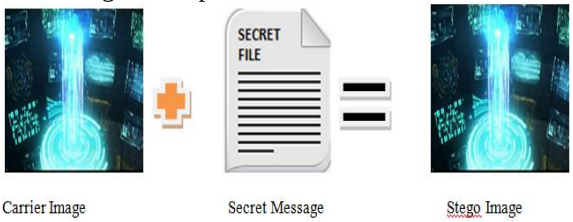
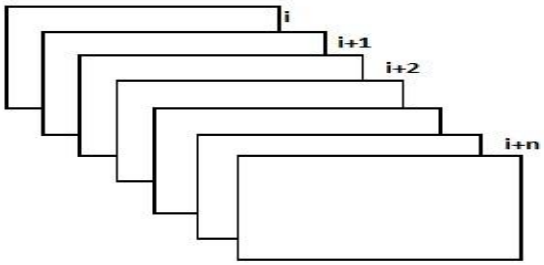


Fig-3: Steganography using video image

Frame Extraction



Consider we have n number of frames that are extracted from the video. The sound extraction from the frames can be done with the help of following equation.

$Si = \int_0^n a\,.et|T(i+1)s - T(if)|$ …… (1)

Where
$T(i+1)s$ = Starting Time of next Frame
Tis = Starting time of Current frame
t = Starting time of Sample
a = Amplitude of Sample
Si = Audio Sample Between frames.
Then the total video is given by the equation
Vi = Si + f …….. (2)

The general equation for calculate the value of whole video is given by
Vi = Concat |fisi + F(i+1).S(i+1)+----------
-+F(i+n).S(i+n)|

VI. Least Significant Bit (LSB) Technique

Data is hided in video file with the help of least significant bit (LSB) algorithm. LSB coding technique has the advantage of low computational complexity and very high watermark channel bit rate. By this technique, least significant bits of the individual pixels of carrier files are changed with the message bits [11]. Each pixel has 3 bits of secret message; one in each RGB component. For hiding three bits of message in every pixel's color , we use 24-bit image like BMP (Bitmap). The human eye cannot easily differentiate between 21-bit colors and 24-bit color [10]. 3 pixels of a 24-bit image are given below:

(00100110	11101000	11001001)
(00100111	11001001	11101001)
(11001000	00100111	11101001)

Character 'a' has an ASCII value 97 in decimal and its equivalents binary value is 1100001. These seven bits changed with the LSB of each seven bit of carrier bytes.

(0010011**1**	1110100**1**	100100**0**)
(0010011**0**	1100100**0**	1101000)
(1100100**1**	001001111	1101001)

With LSB technique a small difference in the colors of the video image. This would be extremely difficult for the human eye to discern the difference. [12].

VII. VII Conclusion

There are various kinds of steganography techniques are available to hide data in video but LSB substitution is a simple technique. The above mentioned approach is based on the research to hide message into video images (AVI) which provides a robust and secure way of data transmission. The proposed embedded video steganography has many advantages like user friendliness, simple and

successful process of embedding secret message with more security.

List of references

[1] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003

[2] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu and Daniel Borca, "Steganography in YUVcolor space", IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa-Canada, pp.1-4, October 2007

[3] P.Ramesh Babu, Digital Image Processing. Scitech Publications., 2003.

[4] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2): 26–34.

[5]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "Steganography and digital watermarking" School of Computer Science, The University of Birmingham. 2003. www.cs.unibo.it/people/phdstudents/ scacciag/home_files/teach/datahide.pdf.

[6] Debnath Bhattacharyya, P. Das, S. Mukherjee, D. Ganguly, S.K. Bandyopadhyay, Tai-hoon Kim, "A Secured Technique for Image Data Hiding", Communications in Computer and Information Science, Springer, June, 2009, Vol. 29, pp. 151-159.

[7] Wang H., Wang S.,"Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM-Voting Systems,Vol. 47, No. 10, pp. 76-82, 2004.

[8] Chincholkar A.A. and Urkude D.A., "Design and Implementation of Image Steganography", Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, pp. 111-113, 2012

[9] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al - Qershi, "Image Steganography Techniques: an Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue(3) : 2012

[10] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,"Application of LSB Based Steganographic Technique for 8-bit Color Images", WASET 2009

[11] 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

[12] Sutaone, M.S.; Khandare, "Image based Steganography using LSB insertion technique", IET, 2008.