International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind
Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

VIDEO STEGANOGRAPHY USING LSB

P. Rajani Devi*

Abstract

The revolution in digital information has created new challenges for sending a message in a safe and secure way. Whatever method we choose, the most important question is its degree of security. Steganography is the art and science of invisible communication. Steganography plays an important role in field of Information Security. As for steganography cover types, almost any digital file format can be utilized for this purpose. Video is a very promising type of cover-media since it can carry a large amount of secret data. In addition, video steganography is becoming very important due to the frequent use and popularity of videos over the internet. Substitution-based techniques for implementing video steganography replace redundant data of the cover with the required secret message. Substitution-based techniques have numerous methods including the famous Least Significant Bit (LSB) technique, Bit Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD) etc., LSB is one of the oldest and most famous substitution-based techniques. In spite of its simplicity, it is capable of hiding large secret messages. In this paper we will discuss video steganography with Least Significant bit substitution technique.

Keywords:

Video Steganography;
Secret message;
Embedding;
Extracting;
Least significant bit method;
Stego image.

Author correspondence:

P. Rajani Devi,
MTech, Computer Science and Technology,
Baba Institute of technological sciences, Visakhapatnam.

1. Introduction

Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating" in a way which hides the existence of the communication. Cryptography is also widely used to provide security of information it scrambles the secret message, such that it becomes meaningless to eavesdroppers. However, this is not always adequate in practice as the encrypted content itself draws attention the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .mpeg, .dat,.gif, .jpeg, .mp3, .txt and .wav.On the basis of nature of cover item, Steganography technique can be separated into five types
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.
Steganography techniques must satisfy these following requirements:

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

* Computer Science and Technology, Baba Institute of Technological Sciences, Visakhapatnam.

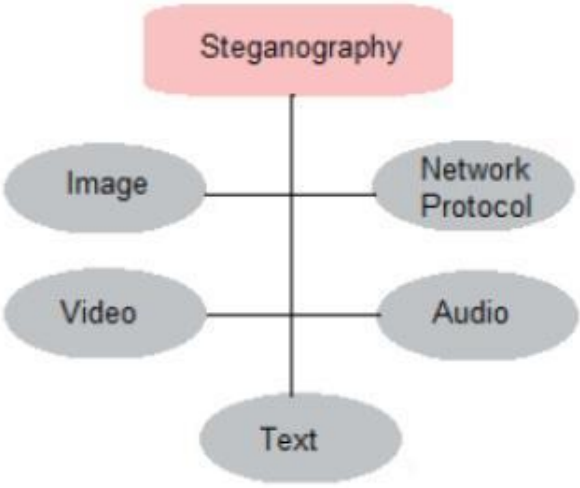

Figure 1: **Steganography Techniques**

1.1. 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.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.

Terminology used in steganography

- **COVER OBJECT**: Describes the file used for hiding information
- **SECRET MESSAGE:** Refers to the data that is embedded in the cover through an embedding module
- **STEGO OBJECT**: This is produced combining the cover object with the embedded data
- **SECRET KEY**: It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.

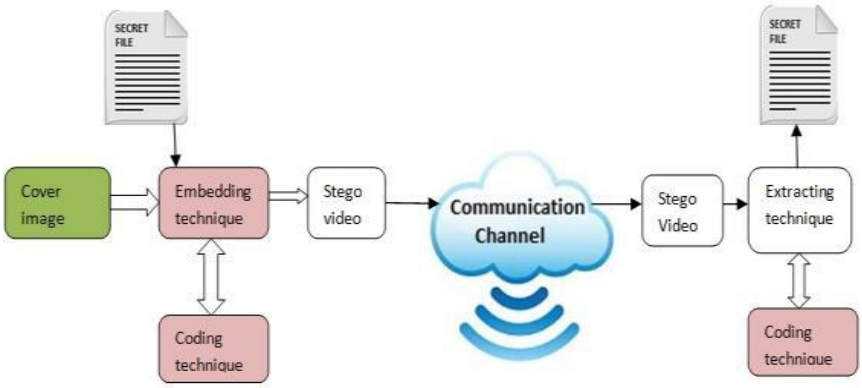

Figure 2: **Structure of steganographic system**

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].

2. Video Steganography

Video steganography, can be viewed as an extension of image steganography. In fact, a video stream consists of a series of consecutive and equally time-spaced still images; sometimes accompanied with audio.Therefore, many image steganographic techniques are applicable to videos as well.Video streams have high degree of spatial and temporal redundancy in representation and have pervasive applications in daily life, thus they are considered as good candidates for hiding data. Video steganography can be then employed in various useful applications. One application is to use video steganography for military and intelligence agencies communications . As the video content is dynamic, lower chances of detection of the hidden data compared with images. In addition to the image attacks that can be applied on the separate frames of video; there are much more attacks for videos such as lossy compression, change of frame rate, formats interchanging, addition or deletion of frames during video processing. Handling a video stream as multiple two-dimensional images, does not consider the dependencies that exist among pixels in their three dimensions [2]. The hiding capacity is much higher in the case of video. Videos provide new dimensions for data hiding such as hiding messages in motion components. The audio components of the video file can also be utilized for data hiding. 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 hidden 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 the function below
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 the function below
Step6: Regenerate video frames.

3.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 is one of the oldest and most famous substitution-based techniques. In spite of its simplicity, it is capable of hiding large secret messages. It operates by replacing some LSBs of pixels from the cover video with the secret message bits. To identify the difference between the original video and the Stego video image is not possible.

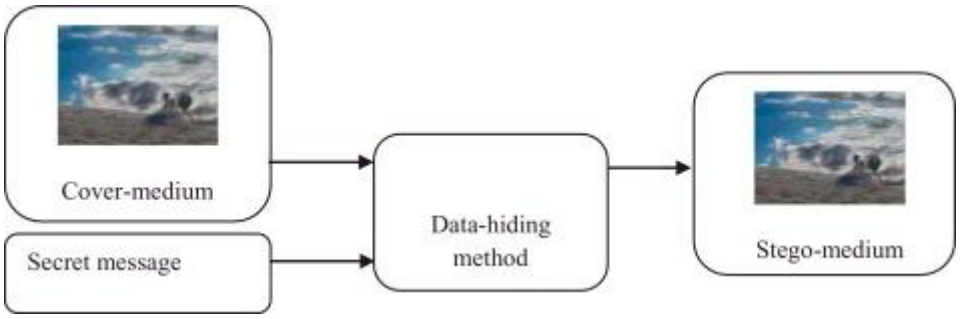

Figure 3: **Steganography Model**

3.1 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.

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

Where T(i+1)s = Starting time of next frame
T(if)= 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 equation Vi = Si+f ---------- (2)

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.
(00100111 111010001 1001000)
(00100110 110010000 1101000)
(11001001 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].

3.2 Applications of Video Steganography

Steganographic technique can be used anytime one wants to hide data. The most important reason to hide data is to prevent unauthorized persons from becoming aware of the existence of a message. Steganography is employed in various useful applications such as copyright control of materials, enhancing robustness of image search engines and smart IDs where individual's details are embedded in their photographs. Other applications are TV broadcasting, video-audio synchronization, TCP/IP packets and checksum embedding and safe circulation of secret data.
Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. In the business world, data hiding can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used in the noncommercial sector to hide information that someone wants to keep private. It can be used in forensic applications for inserting hidden data into media files for the authentication of spoken words and other sounds, and in the music business for the monitoring of the songs over broadcast

radio. Steganography also have some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patient's image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars a link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems.

4. Conclusion

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly.

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.

References

[1] Arya 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. StACM-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 forvarious 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.