World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:5, No:2, 2011

Stego Machine – Video Steganography using Modified LSB Algorithm

Mritha Ramalingam

***Abstract*—**Computer technology and the Internet have made a breakthrough in the existence of data communication. This has opened a whole new way of implementing steganography to ensure secure data transfer. Steganography is the fine art of hiding the information. Hiding the message in the carrier file enables the deniability of the existence of any message at all. This paper 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 away that the video does not loose its functionality using Least Significant Bit (LSB) modification method. This method applies imperceptible modifications. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

***Keywords*—**Data hiding, LSB, Stego machine, Video Steganography

I. Introduction

STEGANOGRAPHY is an ancient art of conveying messages in a secret way that only the receiver knows the existence of message. The subject of steganography has been brought into the limelight by several intelligence agencies and the news media in recent times. Apart from using state of the art, communication technologies and media, the agencies are using cryptography as well as steganography to aid themselves with their objectives [1]. So, a fundamental requirement for a steganographic method is imperceptibility; this means that the embedded messages should not be discernible to the human eye.

The word steganography derives from the Greek word steganos, which means covered or secret, and graphy which means writing or drawing. Steganography is also referred to as Stego. The concept of steganography has existed for thousands of years. The Greek used to pass secret information by writing in wax-covered tablets: wax was first scraped off a tablet, the secret message was written on the tablet, and then the tablet was covered again with the wax [2]. Another technique was to shave a messenger's head, tattoo a message or image on the bald head, and let hair grow again so that the tattoo could not be seen. Shaving the head again revealed the tattoo [2]. The use of invisible ink was also used extensively during the World War II. The invisible ink method and other traditional stego methods were extensively used but the invisible secret message gets revealed when heated. Then the image files are used to hide messages. But image files are not the only carriers [7]. Secret information can be hidden in computer image files (JPEG, GIF, BMP), audio files (WAV, MP3) [5], video files (MPEG, AVI), or even text files. Provided the steganographic algorithm is good enough and a Stego'd video along with the original video, even an adept steganography expert would be unable to detect the hidden information from the image. Making use of the Internet, secret information hidden in the carrier can be transmitted quickly, secretly, and securely.

Over the past few years, numerous Steganography techniques that embed hidden messages in multimedia objects have been proposed. This is largely due to the fact that multimedia objects often have a highly redundant representation which usually permits the addition of significantly large amounts of stego-data by means of simple and subtle modifications that preserve the perceptual content of the underlying cover object [7]. Hence they have been found to be perfect candidates for use as cover messages.

A message, either encrypted or unencrypted, can be hidden in a computer video file (containing the picture of, for instance, an innocent 2 year old baby) and transmitted over the Internet, a CD or DVD, or any other medium [8]. The image file, on receipt, can be used to extract the hidden message. This design incorporates the most powerful modified LSB algorithm to encode the message into video file.

Steganography Vs Cryptograpy -Steganography is not an alternative to cryptography [1]. Steganography is the dark cousin of cryptography. While cryptography provides privacy, steganography is intended to provide secrecy. In other words, cryptography works to mask the content of a message; steganography works to mask the very existence of the message.

II. Proposed System

The existing systems lack good user interface, non-provision of choosing the key and more encode-decode time consumption. There are lots of steganographic programs available. A few of them are excellent in every respect; unfortunately, most of them lack usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems. The proposed application will take into account these shortcomings, and since it will be written in Java, operability over multiple operating systems and even over different hardware platforms would not be an issue. This proposed stego machine provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. This system would be mainly

[1] Mritha Ramalingam, Lecturer, AIMST University, Semeling Bedong, 08100, Kedah Darul Aman, Malaysia. (e-mail: mrirtha@yahoo.com).

concerned with the algorithm ensuring the secure data transfer between the source and destination. This proposed system is based on video Steganography for hiding data in the video image, retrieving the hidden data from the video using LSB (Least Significant Bit) modification method. This design looks at a specific class of widely used image based steganographic techniques, namely LSB steganography and investigate under what conditions can an observer distinguish between stego-images (images which carry a secret message) and cover-images (images that do not carry a secret message).

Fig.1 shows two video images, one- carrier image of the message and the other - the image labeled Stego'd image contain the hidden message. It is not viable to identify the difference between the original video and the Stego'd video image.

Fig. 1 Steganography using video image

Steganography Terms:
Cover-Medium – The medium in which information is to be hidden, also sometimes called as Cover-image or carrier.
Stego-Medium – A medium in which information is hidden
Message – The data to be hidden or extracted

In summary:
Stego_medium = hidden_message + carrier + stego_key

A. Least Significant Bit (LSB) Modification Method

The least significant bit (LSB) algorithm is used in this stego machine to conceal the data in a video file. The main advantage of the LSB coding method is a very high watermark channel bit rate and a low computational complexity. The robustness of the watermark embedded using the LSB coding method, increases with increase of the LSB depth is used for data hiding. In this method, modifications are made to the least significant bits of the carrier file's individual pixels, thereby encoding hidden data [6]. Here each pixel has room for 3 bits of secret information, one in each RGB values. Using a 24-bit image, it is possible to hide three bits of data in each pixel's color value using a 1024x768 pixel image; also it is possible to hide up to 2,359,296 bits. The human eye cannot easily distinguish 21-bit color from 24-bit color [3]. As a simple example of LSB substitution, imagine "hiding" the character 'A' across the following eight bytes of a carrier file:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Letter 'A' is represented in ASCII format as the binary string 10000011.

These eight bits can be "written" to the LSB of each of the eight carrier bytes as follows (the LSBs are italicized and bolded):

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

With such a small variation in the colors of the video image it would be very difficult for the human eye to discern the difference thus providing high robustness to the system [4].

B. Advantages of Proposed System

The advantages of the proposed stego machine are

- A very usable and good looking wizard based GUI (Graphical User Interface) for the system
- Ability to operate the system with no prior training and consultation of any help files
- Ability to conceal and reveal the exact hidden data from video file without disturbing the running application or new application
- Ability to encrypt and decrypt the data with the images
- With this system, an image, after hiding the data, will not degrade in quality

III. Modules Of Stego Machine

The video stegomachine performs the process of conceal and reveal in following modules. The modules of Video Stegomachine are

- Video Header Information
- File Handling
- Encryption
- Steganography – Conceal data
- DeSteganography - Reveal original data
- Decryption
- Graphical User Interface

A. Video Header Information

The video header module collects the header information of an AVI (Audio/visual interleaved) file which is based on the RIFF (resource interchange file format) document format which it is used to verify the AVI format of the carrier file. This module is used to store the information about AVI Main Header, AVI Stream Header, Audio, and BITMAP. This information is used to verify whether the carrier file is in AVI format and to check whether it is a Video, Audio, or any other format.

B. File Handling

In file handling, the AVI (Audio/visual interleaved) file header is skipped and its contents are opened in an ASCII

format for processing. This reads the AVI file in terms of byte corresponding to the header and creates a Key file. The text file which is to be embedded is converted into binary value. Then each bit in the binary value is then converted to 8 bit value which is done by appending zeros in front of the bit.

C. Encryption

The message to be hidden inside the carrier file is encrypted along with a key to disappoint the prying eyes of nosy people. This is to enhance the security during data transmission. This strong encryption method provides robustness to the Stego machine. In this module, the input message is first converted to byte value. The key is obtained from the user which is added to the respective byte and stored in a separate byte array which is then converted to character to get the encrypted form of message. The input to this function is the plain text message and a key value to encrypt the message.

D. Steganography – Conceal data

This module performs the process of steganography. Here the carrier file (AVI file) length is obtained and checked for whether it is eight times greater than that of the text file. Find the starting point of the data in the AVI file and create a key file by writing the content of the AVI file starting from the data to the end. The carrier file is converted into binary. The result is overwritten to the data part of the AVI file and as well as written into the newly created text file. The output obtained for this system is a stego'd video file, and a key file which is to be shared by a secure channel. Fig. 2 depicts the clear picture of concealing the data

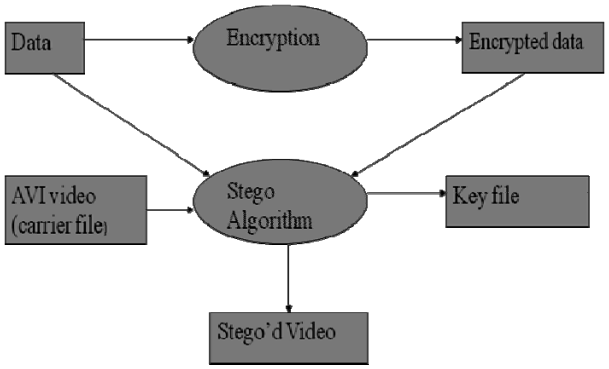

Fig.2 Stegonography of Stegomachine

E. DeSteganography- Reveal Original data

This DeSteganography module decodes the video file to retrieve the hidden data from video. Here the carrier file (AVI file) and the Key file are given as input. The AVI file and the Key file are opened in a Random Access Mode to find the starting point of the data in the AVI file. This reads the AVI file and Key file Byte by Byte and finds the difference between them. The output obtained is an original AVI video file, and a data file that is the message which is hidden inside the AVI video file. Fig.3 illustrates the process of revealing the original data from Stego'd video file.

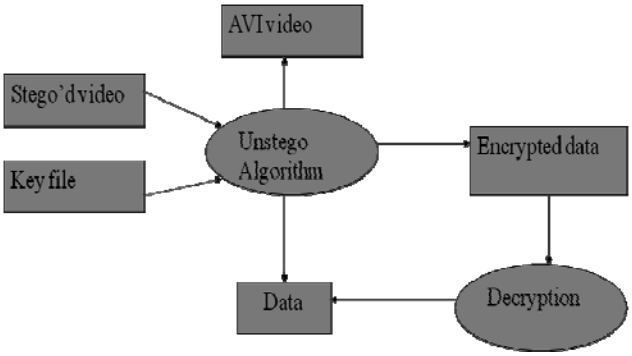

Fig.3 DeSteganography

F. Decryption

The hidden message is decrypted using the key, as once the algorithm gets revealed, all encrypted data with the algorithm could be decrypted. This module first converts the input message to byte value. The key is obtained from the user which is subtracted from the respective byte and stored in a separate byte array which is then converted to character to get the decrypted form of message. The input to this function is the encrypted message file and a key value to decrypt the message

G. Graphical User Interface (GUI)

This GUI is created as a user friendly wizard and does not need any previous training to operate it. It helps user to do steganography without encryption and encryption without steganography. This will help user with a wizard to

- Hide a message in a video file
- Retrieve the hidden message in a stego'd video
- Encrypt a text file
- Decrypt an encrypted file

IV. Sample Outputs

Few sample outputs are shown below.

Steganography - Concealing data:

The wizard in Fig. 4(a) and Fig. 4(b) shows the process of concealing. To hide the data into the video file, the required text file and AVI (Audio/visual interleaved) file are chosen and text file is embedded in to the AVI file to form Stego'd video. Now the Stego'd video image contains the hidden text file.

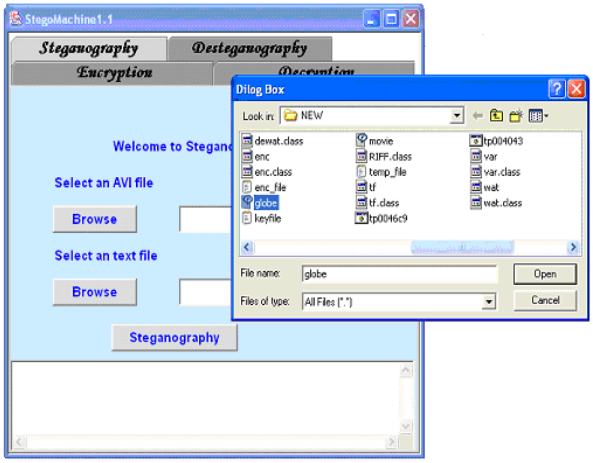

Fig. 4(a) Steganography- Select Text file and Video file

Fig. 4(b) Steganography

DeSteganography - Revealing original data:

The wizard in Fig. 5 shows the process of revealing the original data from Stego'd video file. To disclose the hidden text file from AVI file, the Stego'd video and key file are chosen. Accordingly, the hidden message is retrieved.

Fig. 5 DeSteganography

V. Conclusion

The proposed system based on the research findings developed an application which would be able to hide data into video images (AVI) that provides a robust and secure way of data transmission. This Stego system implements steganography in video image and reveal process without restarting the application or starting a different application. Also this system is a Platform-independent application with high portability and high Consistency.

References

[1] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," Proc. IEEE, 1999

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

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

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

[5] Mazdak Zamani, Azizah A. Manaf, and Shahidan Abdullah, "A Genetic-Algorithm-Based Approach for Audio Steganography" WASET 2009

[6] 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

[7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series.

[8] Mobasseri, B.: Direct sequence watermarking of digital video using m-frames, Proc. International Conference on Image Processing, Chicago, IL, pp 399- 403, 1998.