MOTION PICTURE'S STEGANOGRAPHY: AN INNOVATIVE APPROACH

Nikita Nanasaheb Pawar

ME Student, Electronics and Telecommunication, Shreeyash College of Engineering and Technology, Maharashtra, India

Abstract

Motion picture's steganography i.e. video steganography is a science of hiding embedded elements by embedding video within the video file, which seems to be harmless attractive ones. A decoded encrypted file may cause hiding useful information using video steganography, so if the targeted encrypted file is deciphered, the covered message is unseen. The LSB approach is used to hide the secret video file. This paper provides several advantages of using proposed technique of video steganography along with certain area of application where it is been implemented.

Index Terms – *Video Steganography, Least Significant Bit, Discrete cosine Transform*

1. INTRODUCTION

The growth and developed enhancement of high speed computer inter-networks that of the Internet, has brought the increased change the ease of Information Communication. Ironically, the particular cause for the future development is of the apprehension - use of digitally formatted data. In comparison with the Analog media, the Digital media may offer several different advantages such as high quality, easy editing, high fidelity copying, compression etc. But such type modification in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the one point (sender) to the end point (receiver). So, Information Security is now becoming a non-separable part of Data Communication. In order to address this Information Security, Steganography plays a vital role.

The word steganography is derived from the Greek words "stegano's" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". Steganography is one of such pro-security aspect of innovation in which the secret data is embedded into a cover. The term of data hiding or steganography was firstly introduced with the help of an example of prisoners' secret message led by Simmons in 1983.

Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an "invisible" message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it.

2. LITERATURE SURVEY

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. DCT works by slightly changing each of the images in the video, only so much that it is not noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up. For example, if part of an image

has a value of 6.667 it will round it up to 7. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

Data embedding requirements include the following: 1) Imperceptibility: The video with data and original data source should be perceptually identical.

2) Robustness: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.

3) Capacity: Maximize data embedding payload.

4) Security: Security is in the key for embedding or encryption of data.

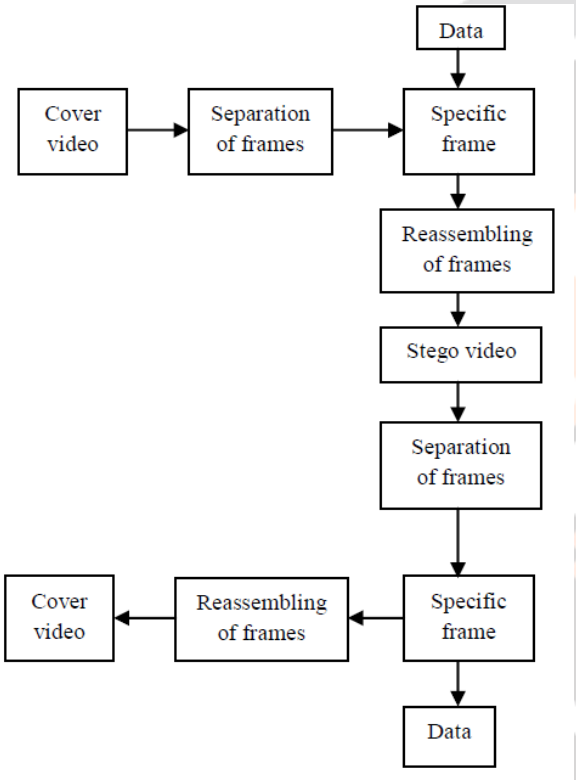

Fig-1: Fundamental model of Motion Pictures steganography

2.1 Least Significant Bit (LSB)

Least Significant Bit (LSB) insertion is an approach to embedding information in a cover video. Video is converted into a number of frames, and then convert each frame in to an image. After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue colour components can be used, since they are each represented by a byte. In other words one can store 3 bit in each pixel. An 800 x 600 pixel image can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

For example a grid for 3 pixels of a 24 bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the letter A, which binary representation is 01000001 and is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101100 00011101 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

Although the letter was embedded into the first 8 bytes of the grid, only the 2 highlighted bits need to be changed according to the embedded message. On average only half of the bit in an image will need to be modified to hide a secret message using the maximum cover size.

First we read the original video signal and text. We have to embed the text into the video signal. Then we have to convert the text data into the binary format. Binary conversion is done by taking the ASCII Value of the character and converting those ASCII values into binary format. We take the binary representation of samples of cover signal and we insert the binary representation of text into that cover signal. The LSB
bits of video signals are replaced by the binary bits of data and this encoded signal is called stego-signal is ready for transmission through internet. For the steganography the important video format is MPEG or DAT. The message which we want to hide is converted into ASCII and then converted into its binary representation with each word consist of 8 bits. These bits are substituted in the Least Significant Bits of binary representation of each image sample.

2.2 Encryption of video

1. Open MATLAB
2. In MATLAB open file location "C:\Users\Lenovo\Documents\MATLAB".
3. At this location a folder name file is present, right click on it and then 'Add to path>Select all folders and subfolders' and open the folder.
It contains a MATLAB file 'main.m', double click on it. A program will open in Script box.
4. Now from the menu select 'Run' option which will run the 'main.m' program.
Eventually this will create a window which lead you to Input and output process.
5. Now from the window select 'select video', which will open another window containing your video file, select it.
It is necessary that your Video file size should be more than size of Hidden video file. And both the videos must be less than 1Mb. If it is more than 1Mb it may take several times to encrypt and decrypt the data.
When the video file is selected, it starts decomposing the frames of the Video file and shows a message that 'file is decomposed'.
6. Now select 'select video to hide' option and select the video file which is to be hidden in the above selected file.
Again, when the video file is selected, it starts decomposing the frames of the Video file and shows a message that 'file is decomposed'.
When both the files are decomposed the frames are extracted in the folders 'extract_cover' and 'extract_stego'.
7. Now select "Process". This will create a file encrypted with cover and hidden video and generate a new 'stego.mp4' file.

2.3 Decryption

1. Now in the "main.m" window select 'stego video' in the output video section.
2. Select the stego video file generated after encryption process.
3. Select option 'Reverse Stego' which will directly decrypt your cover video and hidden video files.
And the final hidden video will be shown in the folder 'extract_video'.

3. APPLICATIONS

Steganography is applicable to, but not limited to, the following areas -
1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system for digital content distribution
4) Media Database systems

The area differs in what feature of the steganography is utilized in each system.

1. Confidential communication and secret data storing

The "secrecy" of the embedded data is essential in this area. Steganography provides us with:

- Potential capability to hide the existence of confidential data
- Hardness of detecting the hidden (i.e., embedded) data
- Enhancing the secrecy of the encrypted data

In practice, when you use some steganography, you must first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the steganography software) together with some key. When extracting, you (or your party) use an extracting program (another component) to restore the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" with your party before you start confidential communication.

Attaching a stego file to an e-mail message is another example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method.

There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System." There is some other communication method that uses the Internet Webpages. In this method you don't need to send anything to your party, and no one can detect your communication.

Each secrecy based application needs an embedding process which leaves the smallest embedding evidence. You may follow the following.
(A) Choose a large vessel, larger the better, compared with the embedding data.
(B) Discard the original vessel after embedding.

For example, in the case of Qtech Hide & View, it leaves some latent embedding evidence even if the vessel has a very large embedding capacity. You are recommended to embed only 25% or less for PNG / BMP output of the maximum capacity, or only 3% of the vessel size for JPEG output.

2. Protection of data alteration
We take advantage of the fragility of the embedded data in this application area. We asserted in the "the embedded data can rather be fragile than be very robust." Actually, embedded data are fragile in most steganography programs. Especially, Qtech Hide & View program embeds data in an extremely fragile manner.

However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

3. Access control system for digital content distribution

In this area embedded data is "hidden", but is "explained" to publicize the content. Today, digital contents are getting more and more commonly distributed over Internet than before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who can make access to the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital contents to e-mail messages and send them to the customers. But it will takes a lot of cost in time and labor.

If you have some valuable content, which you think it is distributable if someone really needs it, and if it is possible to upload that content on Internet in some covert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize this type of system.

We have developed a prototype of an "Access Control System" for digital content distribution through Internet. The following steps explain the scheme.
(1) A content owner classify his/her digital contents in a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.
(2) On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address, e-mail address, phone number, etc.) will be posted there.
(3) The owner may receive an access-request from a customer who watched that Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged). In this mechanism the most important point is, a "selective extraction" is possible or not.
4. Media Database systems

In this application area of steganography secrecy is not important, but unifying two types of data into one is the most important.

Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.
(1) The title of the picture and some physical object information
(2) The date and the time when the picture was taken
(3) The camera and the photographer's information

Recently, almost all cameras are digitalized. They are cheap in price, easy to use, quick to shoot. They eventually made people feel reluctant to work on annotating each picture. Now, most home PC's are stuck with the huge amount of photo files. In this situation it is very hard to find a specific shot in the piles of pictures. A "photo album software" may help a little. You can sort the pictures and put a couple of annotation words to each photo. When you want to find a specific picture, you can make a search by keywords for the target picture. However, the annotation data in such software are not unified with the target pictures. Each annotation only has a link to the picture. Therefore, when you transfer the pictures to a different album software, all the annotation data are lost.

This problem is technically referred to as "Metadata (e.g., annotation data) in a media database system (a photo album software) are separated from the media data (photo data) in the database managing system (DBMS)." This is a big problem.

Steganography can solve this problem because a steganography program unifies two types of data into one by way of embedding operation. So, metadata can easily be transferred from one system to another without hitch. Specifically, you can embed all your good/bad memory (of your sight-seeing trip) in each snap shot of the digital photo. You can either send the embedded picture to your friend to extract your memory on his/her PC, or you may keep it silent in your own PC to enjoy extracting the memory ten years after. Qtech Hide & View v02 may be a good program for such purposes.

If a "motion picture steganography system" has been developed in the near future, a keyword based movie-scene retrieving system will be implemented. It will be a step to a "semantic movie retrieval system."

4. ADVANTAGES

4.1 Highly secure

Since random data are also placed in unused frames in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganographed in ordinary video and can be transmitted over internet even in unsecured connection.

4.2 Capacity

Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50% of original image size can be used to hide the secret message. But there is limitation on how much information can be hidden into an image. Video Steganography has been found to overcome this problem.

4.3 Imperceptibility

Lowest chances of perceptibility because of quickly displaying of the frames, so it's become harder to be suspected by human vision system.

4.4 Video error correction

Since the transmission of any data is always subject to corruption due to errors, then the video transmission must deal with these errors without retransmission of corrupted data. This is another application for steganography rather than security purpose.

4.5 Less computational time

Since use of indexing concept, the process of retrieving the secret data from the steganographed video becomes very simple and requires very less time.

5. CONCLUSION

Steganography is the technique that provides confidential communication between two parties. In this paper, implementation of LSB technique of video steganography is mentioned which satisfy the three main objectives imperceptibility, capacity and robustness.

In case of video steganography, LSB based techniques results are good enough and can be improved by combining this technique with artificial intelligence, fuzzy logic neural network. It is the fast growing and upcoming field and has a great scope for research and development.

6. REFERENCES

[1]. " Video steganography: a comprehensive review ", Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa

[2]. "Advanced Video Steganography Algorithm", Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde

[3] "Different Techniques of Image and Video
Steganography: A Review", Abhinav Thakur, Harbinder Singh, Shikha Sharda

[4]."Implementation of Advanced Video Steganography Algorithm", Suchi Kumari1, Pritish W. Bhautmage2, Sanjeev Ranjan, Vol 2, Issue 1 (February, 2015), ISSN : 2348-2273

[5]. "Implementation of Video Steganography Using Hash Function in LSB Technique", S. Chitra, Narasimhalu Thoti, Vol. 2 Issue 11, November – 2013

[6]. "Steganography and Its Applications in Security", Ronak Doshi, 1 Pratik Jain, 2 Lalit Gupta, Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638

[7] "Improved Protection in Video Steganography Using DCT & LSB", Poonam V Bodhak, Baisa L Gunjal, Vol 1, Issue 4, April 2012

[8] "Video data hiding using Video Steganography", Ms. Prachi P. Sadawarte, Prof. P. A. Tijare, Vol. 6, Issue 2, February 2017

[9] "Video Steganography: an Impact of Hiding Cryptographic Data by Replacing LSB bit with Data Bit of AVI Video File", Ms. D. S. Maind, Dr. B. K. Sarkar, Vol. 1, Issue 7, September 2012

[10] "Different Techniques of Image and Video
Steganography: A Review", Abhinav Thakur1, Harbinder Singh2, Shikha Sharda, Volume 2, Spl. Issue 2 (2015)

[11] "Video Steganography technique using
Factorization and Spiral LSB methods", Vivek Kumar Jha, Srilekha Mukherjee, International Conference on Computer, Communications and Electronics, July 01-02, 2017