IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

A Study Paper on Video Based Steganography

Himani Trivedi
Research Scholar,
Dept. of CSE, SVIT, Gujarat , India

Prof. Arpit Rana
Assistance Professor,
Dept. of CSE, SVIT, Gujarat, India.

Abstract— Steganography is the practice of hiding secret message or private information within other multimedia data i.e. text, image, audio or video. Recently video steganography has become privilege for providing large amount of data to be transferred secretly. Video is simply a collection of images, hence more space is available for hiding of information based on factors such as carrying files, type of message to be embedded and method of compression used etc., the technique used in video steganography can differ. The strength of steganographic technique lies in its capacity to keep the message as secret as possible and also the amount of data that can be hidden, as large as possible. In spite of the fact that numerous approaches already exist in video steganography researches are going on in this field. This paper gives a survey on the methods used in this area.

Keywords— Steganography, Video Steganography, Embedding Algorithm, Video-frame, Stego.

I. Introduction

Now days, when we hear the term like ‘Digital India’, it shows the fact that how much this word ‘Digital’ is important to us. So, we having a lot of digital data every day and these data are in text, image, audio or video form. Though, this data is shared over the network with the help of internet. So, it is very important to maintain the privacy of data. For providing confidentiality and integrity to the data there are various techniques has been used so far like cryptography, steganography and watermarking.

Cryptography is a technique in which original data (Plaintext) is converted to some unreadable form of data (Cipher text) with help of some secret key using some ciphering algorithm. Steganography is a practice of secret communication of data. In Cryptography, Secret message is kept in an unreadable pattern to a third person, while in steganography method existence of secret message is hidden from the third person.

In Steganography technique, sender sends a message by hiding it within some multimedia data like text, image, audio or video. For video steganography cover media is video and within that video we can hide secret data like text, image, audio and video.

For embedding secret message within cover media, a convenient algorithm is used by sender and same algorithm receiver used for extracting secret message. Some shared secret – key known as Stego-key is used in steganography algorithm. Fig.1 Shows Block Diagram of Steganography.

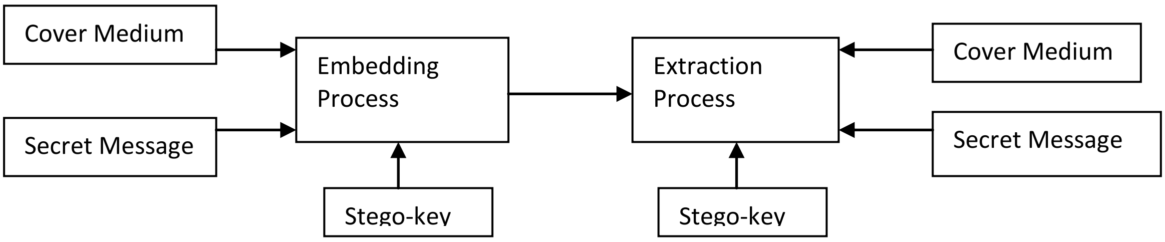

Fig 1: Block Diagram of Steganography

Essential Features of Steganography Technique:

- Embedding Capacity: How much data we can embed in the cover file without affecting its original quality.
- Undetectibility: Data should be concealed in the carrier file in such a way so that any unauthorized could not notice existence of secret message in cover file.

- Robustness: It is the capacity of the embedding algorithm to retain the embedded data even after going through the compression and decompression process.
- Tamper Resistance: If an attacker detects the message in the cover file then it will be very hard him to edit or destroy the message.

II. VIDEO STEGANOGRAPHY

Video Steganography is a technique in which cover medium is video within that secret message is embedded. Advantage of video steganography is that the amount of data that can be hidden will be large and also minimal changes in continuous flow of information cannot be easily identified. We know that video is a collection of frame or images with some audio. So, first step for video steganography is selection of frame in which secret message is to be embedded. Embedding of message within some frame or image of video can be done using any of image steganography technique.

III. METHODS USED IN VIDEO STEGANOGRAPHY

In this section, we present some of the techniques used in video steganography. Steganography methods have mostly two types, spatial domain and frequency domain technique.

If the steganography is done by changing the bits of the binary representation of the image, then the technique used is spatial domain technique. If the image is first transformed to the frequency domain and then the processing is done, then the technique used is frequency domain technique.

A. Spatial Domain Based Method

Spatial domain method of steganography basically works on hiding information in pixels of video frames. The most popular method of steganography based on spatial domain is least significant bit(LSB) method. LSB has high embedding capacity of data, less embedding complexity and easy in implementation. Here, the LSB of each byte of cover video frame will be replaced with secret message. In that, only LSB plane of the entire frame will be affected, which causes not much twist to the cover image.

For Example, following is the three adjacent pixels of an image with RGB encoding:

```
00001101   00011101   11111001
10000110   00011111   11011010
10001111   00110000   11011011
```

Message to be hidden is of 9 bits, which is given by: 101101101
If we overwrite these 9 bits over the LSB of the 9 bytes above, the result will be:

```
00001101   00011100   11111001
10000111   00011110   11011011
10001111   00110000   11011011
```

Thus, 9 bits are hidden successfully at a cost of only changing 4 bits.
The limitation in this method is that the hidden image or frame can easily be destroyed. LSB is also low Robustness to attack.

Pixel value Differencing is another approach of achieving spatial domain based steganography. Secret message bits are concealed in pixels by dividing them on basis of their difference which provides better results in terms of imperceptibility and higher embedding capacity.

B. Transform Domain Based Method

In transform domain method, image is first transformed from spatial domain to frequency domain. Discrete cosine transforms (DCT) and discrete wavelet transform (DWT) are method of transform domain based method.

DCT is most common form of transform domain steganography. In this method, image is transformed from spatial domain to frequency domain. After transformation image has low, high and middle frequency components. Here, the low-order DCT coefficients correspond to large feature of pixels and high-order coefficients corresponds to fine features.so the high-order coefficients are selected for embedding secret information. Embedding is done by simply changing DCT coefficinets.DCT is a lossy compression transforms because we cannot calculate the cosine value exactly and repeated calculation can cause rounding error in the results. DCT gives the effects of spreading the location of pixels over the image. Using this method, the secret message is more secured against attackers, but it cannot hide much data.

In Discrete wavelet transform, it decomposes the signal into wavelet coefficients from which the original signal can be reconstructed again. The wavelet coefficients represent the signal in various frequency bands. Image is divided into four sub bands: LL, HL, LH and HH. From which LL sub band embed the secret data.

IV RELATED WORK

Ashish T. Bhole ET. Al, 2012 [1], In this paper author defines the video steganography for secured communication in insecure communication channel. In this paper, they use two method Random Byte hiding and LSB technique for hiding secret data into video file. In Random byte hiding method, the information is hiding in each line of the video frame at different place. For ex, if the line begins with pixels value of 'zz', the information is stored over the 'zz'+x location, where x is only known to the authorized receiver. While in LSB technique, secret message is embedded within LSB of each pixel of the frame.

Rahul Paul ET. Al, 2013 [2], In this paper, author have used video file as the cover file and embedded the information in the frames where the scene has changed in the video sequences using LSB replacement technique. For additional security they have randomized the pixel positions where the information bits are embedded by generating an indexed based chaotic sequence and arranging the pixel position according to the sequence. The experimental results show that original cover video and stego video are visually identical.

Rajesh G.R ET. Al, 2013 [3] , In this paper, author proposed new embedding algorithm to hide data in moving video. In this proposed algorithm 2D-DCT of video is taken and secret message is embedded within that video. The PSNR value is calculated to evaluate the quality of the video after the data hiding. The 2D-DCT of the video is taken and the secret message is embedded by checking the DCT coefficients of the video frame.

Ramadhan J. Mstafa ET. Al, 2016 [4], In this paper they have proposed a DCT-based robust video steganography method using BCH codes. To improve the security of the proposed algorithm, a secret message is first encrypted and encoded by using BCH code. Then, it is embedded into discrete cosine transform (DCT) coefficients of video frames. The hidden message is embedded into DCT coefficients of each Y, U and V planes excluding DC coeffients. The proposed algorithm is tested under two types of video slow and fast moving videos. The hidden ratio of the proposed algorithm is approximately 27.53%, which is evaluated as a high hiding capacity with a minimal tradeoff of the visual quality. The robustness of this algorithm was tested under different attacks.

Essam H. Houssein ET. al, 2016 [5], In this paper, author propose the approach of an advanced technique for encrypting data using Advanced Encryption System and hiding data using Haar Discrete wavelet transform. HDWT aims to decrease the complexity in image steganography while providing less image distortion and lesser detectability. One fourth of the image carrying the details of the image in a region and other three region carrying a less details of the image. Then the cipher text is concealed at most two least significant bits (LSB) positions in the less detailed regions of the carrier image.

Abhinav Thakur ET. Al, 2015 [6], In this paper, author proposed the different method of steganography. Firstly, cover video is decomposed into different frames. A single level discrete wavelet transform is applied on selected frame and on secret image. A private key is used during the process of encoding and decoding to provide high security. Encoding and decoding of secret data is done using Arnold function. Then the Inverse Discrete wavelet transform is applied to get the stego-video. The performance parameters like PSNR and MSE calculated to measure the quality of stego video.

CONCLUSION

This paper gives overview of different video steganography methods. From this all the method have their advantages and disadvantages like LSB method has high capacity of embedding of data but low robustness to attack while DCT and DWT is robust against attack but they have less embedding capacity of data. So, if we work on hybrid of spatial and frequency domain method then we can achieve high security, high capacity and robustness to data. For better security also we can also combine cryptography with steganography.

REFERENCES

[1] Ashish T. Bhole, Rachna Patel, 2012 Steganography over video File using Random Byte Hiding and LSB Technique, IEEE international conference on computational intelligence and computing research.

[2] Rahul Paul, Anuja kumar Acharya, virendra kumar yadav, saumya Batham, 2013, Hiding large amount of data using a new approach of video steganography, 4th international conference on the next generation information technology summit.

[3] Rajesh G.R, A. Shajin Narguman, 2013 , Steganography algorithm based on discrete cosine transform for data embedding into raw video streams, Chennai fourth international conference on sustainable energy and intelligent system.

[4] Ramadhan mastafa, Khaled M. Elleithy, 2016, A DCT-based robust video steganography method using BCH error correcting codes, IEEE.

[5] Essam H. Houssein , Mona A. S. Ali, Aboul Ella Hassanien , 2016, An image steganography algorithm using Haar discrete wavelet transform with Advanced encryption algorithm, Federated conference on computer science and information system.

[6] Abhinav Thakur, Harbinder singh, Shikha sharda,2015, Secure video steganography based on discrete wavelet transform and Arnold transform, International journal

[7] B. Karthikeyan, Suddep Gupta, 2016, Enhanced security in steganography using encryption and quick response code,

IEEE WispNet Conference.

[8] Dr. M. U. Umamaheshwari, 2010, Analysis of different steganographic algorithm for secured data hiding, International journal of computer science and network security , Vol10No.8.

[9] Mrudul Dixit, Nikita bhide, Sanika Khankhoje, 2015, Video Steganography, International conference on pervasive computing.

[10] Tarik Faraj idbea, salina abdul samad, 2015, an adaptive compressed video steganography based on pixel value differencing schemes, international conference on adaptive technologies for communication.

[11] Pooja yadav, Nischol Mishra , Sajneev sharma, 2013 , A secure video steganography with encryption based on LSB Technique, IEEE international conference on computational intelligence and computing research.

[12] Vladimir Hajduk, Martin Broda, 2016, Image steganography with using QR Code and cryptography, 26th conference on Radioelektronica.