REVIEW ON DIGITAL VIDEO STEGANOGRAPHY

[1]Dipika Deshmukh, [2]Dr. Gajanan D. Kurundkar
[1]Phd Scholar, [2]Assistant Professor
[1]School of Computational Sciences,
[1] SRTM University, Nanded, (India)

Abstract: ***The growth of the Internet has paved the way for easy access to information, and has contributed to the fast development of multimedia based applications. This has made security issues very critical and challenging. Various types of media carry information like image, audio and video and protecting these from unauthorized access is an important area of active research. Steganography is the best technique for hiding the data. It is the science or art of embedding private information into the cover media with the alteration to the cover image, which cannot be easily recognized by human eyes. Video Steganography is a method for hiding data in a video file and hence it decreases the probability of access by unauthorized user. In Steganography different carrier file formats can be used, among which videos are popular due their regular use on internet. Video Steganography has a lot extra scope of hiding secret data because of the nature of video which has lots of numbers of redundant bits. As per the requirement of user there are different video Steganography technique proposed leading to own positive and negative points. The video Steganography techniques are helpful in application having high security requirements. This paper describes survey of video steganographic algorithms which are used by several authors.***

Index Terms -: Data hiding, embed, Steganography, stego video

1. INTRODUCTION

Secure transmission refers to the transfer of data such as top secret or proprietary information on secure channel. Many secure transmission methods require a type of encryption. In order to open the encrypted file or hidden data an exchange of keys is done. Many infrastructures such as banks depend on secure transmission protocols to avoid a terrible break of security.

Security is very important because it allows you to securely guard data that you don't want anyone else to have access to. Businesses use it to keep corporate secrets, government use it.

Internet is the greatest medium for communication but it faces more problems related problems related to security like hacking, copyright, eavesdropping etc. There are a variety of techniques for security of data like cryptography, watermark and Steganography. Cryptography is a technique which is used to protect the secrecy of communication. There are many special methods to encrypt and decrypt the data in order to keep the message secret. But, it is not sufficient to keep the content of a message secret, at the same time it is also important to keep the existence of message secret. The technique in which the existence of hidden message is reserved secret is called as Steganography [1].

Watermark is generally a small quantity of or agents of companies to hide secret message inside data that is used to designate the ownership of the particular object or data file. The watermark may be a signature of the author located in the document for pride of authorship [2].

2. STEGANOGRAPHY SYSTEM

Steganography is an art of hiding the information in other media or host object. It is an old method of communication. It is used from since ancient times by the people. For hiding the data used back of slaves, scalp of slaves, invisible ink, and wax in ancient time. As time passes, in the digitized world secret communication becomes necessary. Following are some basic terms related to Steganography system and which are necessary to realize [4].

Cover media- It is the object in which secret data is embedded in such a manner that it is not easily possible to detect the presence of data.
Stego media- It is the object obtained after embedding the data.
Secret data-The data or information to be hidden in cover media.
Steganalysis-It is the procedure of detecting the existence of secret information in the cover object.

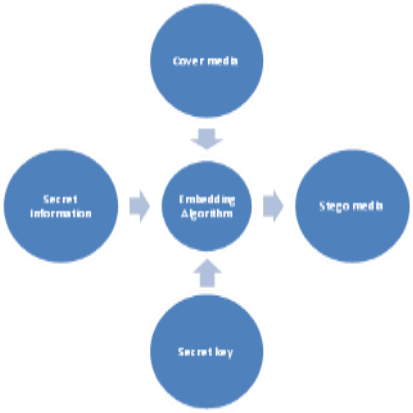

Figure 2.1 Steganography systems [4]

3. VIDEO STEGANOGRAPHY

Video is the technology of electronically recording, sending, storing, capturing and reconstructing a series of images representing scenes in motion. Traditional text and image based Steganography have less data hiding capacity. Video Steganography overcame this capacity problem. In video Steganography we can hide much more data in video. We can hide data in each frame of video. Hence Video Steganography has more capacity than Image Steganography [5].

An effective video Steganography technique should have the following characteristics

Imperceptibility

Imperceptibility refers to the visibility of alteration inside the cover media. High Imperceptibility means growing the invisibility of slight modifications in cover object. Modern day Steganalysis approaches are very much intelligent to detect minor modifications. High Imperceptibility has motivated researches to intend steganalysis resistant video Steganography methods [6].

Payload

Payload refers to the amount of secret message that can be covered inside cover media. Video are gaining popularity as extremely used cover media object due to their high embedding capacity and embedding efficiency[6].

Statistical Attacks

The attacks applied on stego object to extract hidden information are known as statistical attack. Steganography algorithm must be strong against statistical attacks. It describes robustness feature [6].

Security

The mainly significant feature of any steganographic algorithm is security. The embedding process should have high security with minimum exposure to attacks. Some approaches have been proposed to secure message in Steganography [6].

Computational Cost

Data hiding and Data retrieval are the two parameters used to calculate computational cost of any Steganography approach .Data hiding time refers to the time necessary to embed data inside a cover video frame and data recovery refers to extraction time of secret message from the stego frame [3, 6].

Perceptual Quality

Increment in hiding capacity may also lead to ruin of video quality or degradation of original contents of video. Video Steganography approach must handle control degradation of video excellence [3, 6].

4. LITERATURE SURVEY

Discrete Cosine Transform

In 2002, Wang presented data hiding steganographic algorithm. He use discrete cosine transform for increasing the payload capacity with keeping simplicity and robustness. In his steganographic method, computed coefficients of I- frames and then embed the secret information by performing modulation between secret information and quantized DCT coefficient [4]

In 2012, Hong Zhao et al. Used 3D discrete cosine transform to capture the correlation structural features like Kurtosis, Skewness, absolute Central moment and mark are sensitive to the data Hiding and these features are used for classifying statistics. To differentiate the cover and stego video used unsupervised K means clustering. The standard 40 video are tested for effectiveness of proposed technique [7].

Bit Plane Complexity Segmentation Technique (BPCS)

In 2004, Hideki Noda and his team presented video Steganography for lossy compressed video. This is very simple method for transmitting the secret data. In this method by using wavelet compress the video first then embed the secret data by applying the BPCS. This method is tested for 3-D SPIHT-BPSC and JPEG 2000-BPSC Steganography [4].

In 2010, Peipei Shi et al. suggested that BPCS techniques can be used for Steganography. In this method embedding capacity is increased up to 50%. It also gives an idea for higher security and reliability with PSNR is 38.03 db based on Chaos and BPCS algorithm [8].

In 2007 Lane proposed vector embedding method for Steganography. MPEG-I and MPEG-II video codec standard was used in the method. Host video frame pixels contain the audio information [4].

Least Significant Bit Method (LSB)

In 2009, Eltahir et al. proposed a video streaming Steganography system which was based on LSB and this method save up 33.3% portion of image for hiding the data. This is the progress for LSB. The idea behind his method is by using 3-3-2 approach using 24 bit RGB image. It takes 3 bits of red and 3 bits of green and 3 bits of blue color. Collectively made 1 byte is used for data hiding. They did not found any variation in both frames and their histograms [9].

In 2009, A .J. Mozo et al.used flash videos for video Steganography because of its simple file structure and small size and popularity in video hosting websites. They also describe software implementation and research in the field of video Steganography [10].

In 2011, Samir Kumar bandyopadhyay and Biswajit Dutta modified LSB technique. They altered 1st lsb layer and then 4th LSB layer under certain conditions. Still they did not see any difference between original and cover file [10].

In 2016, Mansi Dave and Hinal Somani proposed advanced LSB approach for embedding the data. they improves Steganography performance in terms of visual quality and robustness unlike other methods advanced LSB method does not directly embed the bit of message in video. In the proposed method in embedding process depends on the message bit and the parity which is produced by the LSB of each color component. This method based on odd even parity rules hence it provides High robustness and visual quality [5].

Non-uniform rectangular partition

In 2011, Shen Dun Hu et al. presented non-uniform rectangular partition for Video Steganography. They used uncompressed videos. The cover video and hiding secret video are of same size. Encoded each frame of secret video is portioned into non-uniform rectangular part.

Four leftmost least significant bits of each frame of cover videos are used for hiding the secret video stream. This technique shown no distortion in the result and PSNR values were larger than 28 db of the frames [9].

Lazy Lifting Wavelet Transformation

In 2013, Khushaman Patel et al. have proposed encoding technique based on lazy lifting wavelet transformation. In this technique first video is transform by using LLWT then LSB in sub-bands of the video that has been achieved. This video Steganography techniques use both visual and audio components. Visual frames uses lazy wavelet transform and data is stored in the coefficients of the visual component. LSB hides up to length stored data in the audio component. This proposed scheme does not affect higher and lower ends of the frequency distribution of the signal. By using this technique we get high payload capacity and very low computational requirements [7].

5. RELATED WORK

In 2014,R Shantakumari and Dr .D. S. Malliga taken AVI video format stream for Video Steganography and used LSB Matching Revisited Algorithm. In their proposed paper, firstly they split cover video into frames and then message embedded into multiple frames. After that all nine frames are grouped together for making the stego video. At receiver side again split frames for extracting the hidden message. LSBMR algorithm has very few replacement rates. Hence MSE is low and PSNR values decreases when increases the embedding. Finally resulted LSBMR is more secured than LSB algorithm [9].

In 2014, kelash et al. proposed technique based on histogram constant value they hide secret message within part of frame or in whole frame. Random from selection increases secrecy and embedding capacity and in each frame reduced faded pixel [1].

In 2014 Jennifer et al. presented advertising board for hiding information. It known that encryption provide the secure channels for communication, here author proposed online hiding of information output screens of instrument are used for finding the data. This method used in showing a secret message in public place. This method can be used in railway station or airport this method is very close to both image and video Steganography. They used two technique for hiding the data namely symmetric key Steganography technique and lsb technique for private marking system [11].

In 2015, Yugeswari Kakde et al. researchers used audio video file for hiding the data in frames of a video and audio at the time of hiding the data in audio file the first 2 bits of the 16 bits WAV file were converted into decimal. They provide the insertion position of the secret information in the LSB bit by bit by repeating the process until all the text bit were substituted which hiding an image or frames is a frame is selected from the video using DWT and SVD. The LSB method recovers the text and DWT and SVD reverse The Secret image [12].

In 2017, Sunil K. Moon et al. proposed BPCT and LSB techniques to embed the secret data. Data may be text, image and audio for video Steganography. Natural video shows good result because of it's sharply define border. The BPCT algorithm is used for hiding The Secret data inside the selected frame of video and LSB technique is used to hide the data in audio for audio video Steganography. It provides more security and improves embedding capacity [8].

In 2013,Hemant Gupta et al. have chosen method for replacing one, two or three least significant bit of each pixel in video frame and the apply AES because of this it becomes very ambiguous to detect the image which hide into the video [7].

In 2013, B. Suneetha et al. proposed video Steganography with encryption of hidden data with ASCII code. It provides extra secrecy layer for hiding the data [12].

6. CONCLUSION

In this paper, we have studied Bit Plane Complexity Segmentation Technique (BPCS), Non-uniform Rectangular Partition, Least Significant Bit (LSB), Discrete Cosine Transform, and Lazy Lifting Wavelet Transform video steganographic techniques for data hiding. Different authors proposed different techniques and also measure the performance of the techniques using parameters like peak signal to noise ratio(PSNR) and mean square error(MSE).If PSNR value is more and MSE value is less then this technique is good for hiding the data. We can conclude that using LSB technique we can hide more data than BPCS and Lazy Lifting Wavelet Transform techniques.

7. REFERENCES

1. Sahil Gupta , Jyoti Saxena and Sukhjinder Singh "Design of Random Scan Algorithm in Video Steganography for Security Purposes" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. I (Sep - Oct .2015), PP 14-20

2. A. Rasmi, M. Mohanapriya, "An Extensive Survey of Data Hiding Techniques" European Journal of Applied Sciences 9 (3):pp 133-139, 2017 ISSN 2079-2077

3. Namrata Singh,Virendra Kumar Yadav ," Trends in Digital Video Steganography: A Survey", International Journal of computer Applications (0975 – 8887) Volume 169 – No.7, July 2017,pp 6-18

4.Kedar Nath Chaudhari et al, "A Survey Paper on Video Steganography" ISSN: 0975-9646 International Journal of Computer Science and Information Technologies, vol.6 (3), 2015, pp 2335-2338

5. Mansi Dave, Hinal Somani, "A SURVEY ON DIGITAL VIDEO STEGANOGRAPHY TECHNIQUES USED FOR SECURE TRANSMISSION OF DATA" Vol-2 Issue-6 2016 IJARIIE-ISSN (O)-2395-4396,pp 479-485

6. Bharti Chandel , Dr.Shaily Jain, "Video Steganography: A Survey" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17

7. Ankita Patel, Ajay Barot "Survey Paper on Video Steganography", IJSRD - International Journal for Scientific Research & Development Vol. 3, Issue 12, 2016 ISSN (online): 2321-0613,pp 170-173

8. Sunil k. Moon et al. "Innovative Data Hiding Security Model using Forensic Audio Video Crypto-steganography", ISSN: 2229-6948(ONLINE) ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, DECEMBER 2017, VOLUME: 08, ISSUE: 04, pp 1633-1639

9.Syeda Musfia Nasreen , Gaurav Jalewal, Saurabh Sutradhar "A Study on Video Steganographic Techniques" International Journal of Computational Engineering Research (IJCER) ISSN (e): 2250 – 3005 Volume, 05 Issue, 10 ,October – 2015, pp 30-34

10. Amba Mishra, Prashant Johr, "A Review on Video Steganography using GA" International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue September 2015, pp 120-124
11. Jaspreet Kaur, Jagroop kaur "Hiding Text in Video Using Steganographic Technique - A Review", An International Journal of Engineering Sciences, January 2016, Vol. 17 ISSN: 2229-6913 (Print), ISSN: 2320-0332 (Online),pp 578-582
12. Kunal Hossain ,Ranjan Parekh," An Approach Towards Image, Audio and Video Steganography", Second International Conference on Research in Computational Intelligence and Communication networks, 978-1-5090-1047-9/,2016,pp 302-307