National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

An Approach of Secured data for Video Steganography

Mrs. Dipti Save[1], Mrs. Aboli Moharil[2], Mr. Bhushan Save[3]

[1]Department of Electronics & Telecommunication Engineering, Mumbai University, India
Email: diptisave050384@gmail.com
[2]Department of Electronics & Telecommunication Engineering, Mumbai University, India
Email: desaboli@gmail.com
[3]Department of Electrical Engineering, Mumbai University, India
Email: bhushansave@yahoo.com

Abstract— *Day by day the use of the internet in all domains has increased tremendously and because of this, data security has become more important. The data needs to be protected from being affected due to a virus or destroyed by the hacker. The basic idea about data security is; secret data is hidden in the cover video is nothing but steganography. Steganography not only hides the secret information but also hides the existence of the information. It is a very useful technique for secure communication. This technique is used in different fields like defense, medical, online transactions, etc. There are different types of steganography such as text, images, audio and video protocol. This paper presents various techniques available for video steganography. Video steganography techniques are classified into two main parts depend on the basis of embedding methods namely spatial domain and transform domain techniques. The performance evaluation of the proposed system is also reported in this paper.*

Keywords— embedding, LSB, PSNR, steganography, video steganography

I. INTRODUCTION

In today's life the data security is more important in all domains. It deals with the protection or security of data from corruption and unauthorized data. In today's usage of high-speed internet people are worried about data security & information being hacked by attackers. So to avoid these problems many steganography methods have been proposed. The word Steganography is nothing but Greek Origin and it means concealed writing. The Greek word stegons means covered or protected and graphy means writing. Steganography is an art and science of writing messages which are used to hide behind the original message or file. Steganography includes the combination of secret information in the carrier signal such as document file, image file, audio file, video file, program or protocol.

In this paper, the details about video steganography followed by the different techniques of it are given in section II. Our proposed work is mention in section III with algorithms & methodology in section IV. Fig 1 gives the basic block diagram of video steganography.

II. VIDEO STEGANOGRAPHY

Video Steganography is a technique that hide any kind of our secret data or files in any extension into a carrying Video file. In this technique the carrier file must be a video file. It is concerned with embedding information in a cover media in a very secure and robust manner. This system makes the files more secure. Video Steganography brings maximum possibilities of hiding a large amount of data because video is a combination of number of frames or images and sound. Therefore, image and audio Steganography techniques can also be employed in the video. Video files are a collection of images and sounds, so most of the presented techniques which are used on images and audio can be applied to video files too. The great advantage in video steganography is that the large amount of data can be hidden inside it because it is a moving stream of images and sounds.
Fig 1 shows the basic idea of video steganography. The main two terms in this are secret data and carrier video file.

National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

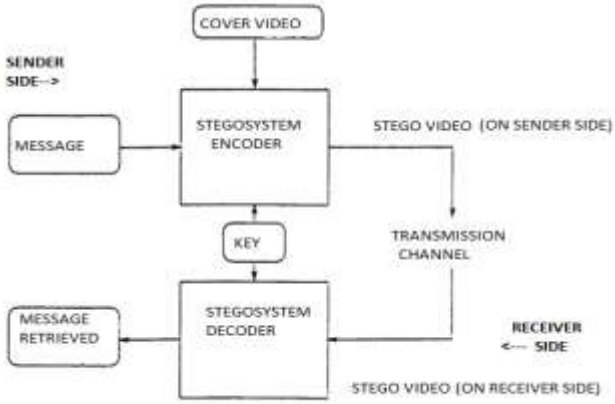

Fig 1: General Flow Diagram of Video Steganography

1.1 Techniques of Video Steganography

Video steganography techniques deal with the video as a sequence of frames with the same format. First, digital video is converted into frames as still images and then each frame is individually used as carrier data to conceal the hidden information [3]. After the embedding process, all frames are merged together to produce the stego video [3]. The most commonly used methods for video steganography are spatial domain technique and transform domain technique.

1.1.1 Spatial Domain Technique

There are many steganographic techniques that based on the spatial domain such as LSB substitution, Bit Plane Complexity Segmentation (BPCS), spread spectrum, Region of Interest (ROI), histogram manipulation, matrix encoding and mapping rule [3]. In all these methods LSB substitution is the most commonly used method. In this type, the data to be hidden is inserted into the least significant bits of the pixel information. Increase or decrease of value by changing the least Significant bit doesn't change the appearance of the image, such that the resulted stego-image looks exactly same as the cover image.

1.1.2 Transform Domain Technique

If we embed information in the spatial domain, it may be subjected to the losses if the image undergoes any image processing technique like compression, cropping, etc. To overcome this problem we embed the information in the frequency domain such that the secret information is embedded on the significant frequency values while the higher frequency part is omitted. We first apply transformations to the image then data is to be hidden by changing the values of the transformation coefficients accordingly. Different types of transform domain techniques are Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

III. PROPOSED WORK

The use of video-based steganography can be more secure than other multimedia files because of its size and complexity. While using steganography secrete data will be Huffman coded due to which data will be compressed and more secrete data can be transmitted.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

The main video file is nothing but the high-resolution AVI file which includes a sequence of high-resolution images. These images are known as frames. This video file is also called a cover video. At the first stage, the system will stream the video and collect all the frames in a bitmap format. After streaming this high-resolution AVI file into bitmap frames, the system will select one frame where data is to hide. The data which have to hide is Huffman coded and into a binary format. Then the LSB replacement method is used where the secret data in binary form is replaced with the LSB position of the cover video frame. After this, these frames are again rebuilt in a high-resolution video file.

Huffman coding is a technique used to compress files for transmission. It is a form of statistical coding. Huffman encoded bitstreams and Huffman tables both are embedded in the cover frame so that the receiver can have both information to decode the Huffman code. Here the satisfactory security should be maintain because at the decoding time secrete data cannot be extracted without knowing the decoding rules and Huffman table.

IV. ALGORITHM AND METHODOLOGY

4.1 Encryption Algorithm

This determines the message type, prepare header information to be used in the decoding stage, and sequentially encodes the message within the pixel values of the cover image. All steps for this encryption are as given below

Step 1: Determining message type & normalizing
Step 2: If message is text this will be true or false otherwise convert from ASCII to integer values.
Step 3: Encrypting using XOR key
Step 4: Preparing hiding canvas
Step 5: Hiding data
Step 6: Final output

4.2 Decryption Algorithm

This recovers a sequentially encoded messages that have been prepared using the stegancoder. This file takes in the cover image and encryption key, decodes the header file to determine the message type and length, and sequentially decodes and recovers the message from the pixel values of the cover image.

Step 1a: Recover header set
Step 1b: Header analysis – decrypt and determine message dimension
Step 2: Isolate potential message
Step 3: Decrypt step
Step 4: Message Prep
Step 5: Final output

V. PERFORMANCE ASSESSMENT METRICS

The main purpose of the steganography technique is to conceal the secret information inside the cover video data, thus the quality of the cover data will be changed ranging from a slight modification to a severe distortion [3]. Pick Signal to Noise Ratio (PSNR) is a common metric utilized to calculate the difference between the carrier and stego data [3]. PSNR is most commonly used factor to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). It is the measure of the quality of the image by comparing the cover image with the stego-image. The good perceptual quality of stego-image is depend on the PSNR. As the PSNR increases, the quality of stega image is also increases. The results of PSNR for all the techniques are in the following table

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

Table 1: PSNR Result for Steganography

Cover Frame	Size Of Message in KB					
	Text File-1KB	Text File-5KB	Text File-10KB	Text File-15KB	Text File-20KB	Text File-25KB
Frame Size (320 x 240, 225 KB)	82.3524	67.7004	64.7598	62.6356	61.4259	60.4174

We can analyze from the results that MSE for spatial domain techniques is very less than that of for transform domain technique. In case of transform domain techniques the lossy compression step of jpeg compression i.e. quantization is performed in the embedding process and hence very large MSE is produced and quality of cover image is degraded more.

Table 2: MSE Result for Steganography

Cover Frame	Size Of Message in KB					
	Text File-1KB	Text File-5KB	Text File-10KB	Text File-15KB	Text File-20KB	Text File-25KB
Frame Size (320 x 240, 225 KB)	0.0003	0.0114	0.0224	0.0365	0.0483	0.061

VI. Conclusion

The main aim of our technique is to develop a system that processes a text message by encrypting it and then hiding it behind a video file using matlab as the language for technical computing. But the project revolves basically around the frames used to hide message. This frames is further processed i.e steganography is performed so as to enhance the security provided to the message. Steganography is a really interesting subject. Day today life we are dealing with the mainstream cryptography and system administration. But it is also quite real; this is not just something that's used in the lab or an arcane subject of study in academia. The few areas which are still open in steganography are as below:

1. Wavelet transform can be used to increase the embedding capacity while maintaining the robustness of Stego-image.
2. Hamming coding or Matrix coding can be used to reduce the impact of steganography i.e. to increase the PSNR.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March- 2020]

REFERENCES

[1] SHALAW MSHIR AND PROF. ASAF VAROL, "A NEW MODEL FOR CREATING LAYER PLANES USING STEGANOGRAPHY FOR TEXT HIDING," IEEE 2019.

[2] Ms. J. Meary Jenifer, Dr. S. Raja Ratna, Dr. J. B. Shajilin Loret and Ms. D. Merlin Gethsy, "A survey on different video steganography techniques", ICOEI 2018.

[3] Ramadhan J. Mstafa, Khaled M. Elleithy and Eman Abdelfattah, "Video steganography techniques: Taxonomy, challenges and future directions," IEEE 2017.

[4] A Munasinghe, Anuja Dharmaratne and Kasun De Zoysa, "Video Steganogaphy," 2013 International Conference on Advance in ICT For Emerging Regions (ICTER):056-059.

[5] Sushmitha MC, Suresh HN and Manikandan J, "An appoarch towards novel video steganography for consumer electronics," 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia).

[6] Nematollah Zarmehi and Mohammad Ali Akhee, "Digital video steganalysis toward spread spectrum data hiding," IET Image Process, Institute of Engineering and Technology 2015.

[7] K. Rajalakshmi and Dr. K. Mahesh, "Video steganography based on embedding the video using PCF technique," International Conference on Information, Communication and Embedded Systems (ICICES 2017).s

[8] Weiming Zhang, Zhuo Zhng, Lili Zhag, Hanyi Li and Nenghai Yu, "Decomposing Joint Distortion for Adaptive Steganography," IEEE 2016.

[9] Disha and Khushil, "A Review on Video Steganography Techniques in Spatial Domain," 2017 Recent Developments in Control, Automation and Power Engineering (RDCAPE).

[10] Abhinav Thakur, Harbindar Singh and Shikha Sharda, "Different Techniques of Image and Video Steganography: A Review," RIEECE-2015.

[11] Jasleen Kour and Deepankar Verma, "Steganography Techniques – A Review Paper," International Journal of Emerging Research in Management and Technology ISSN: 2278-9359 (Volume-3, Issue-5), May 2014.

[12] Aryfandy Febryan, Tito Waluyo Purboyo and Randy Erfa Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10485-10490.