RESEARCH ARTICLE OPEN ACCESS

Hiding an Image Data into Video Stenography Using Different Algorithm and MATLAB: A Review

Anchal Chander Lekha [1]
Monika Gautam [2] HOD
Department of Electronics & communication Engineering
L.R Institute of Engineering &Technology Solan
HP-India

ABSTRACT

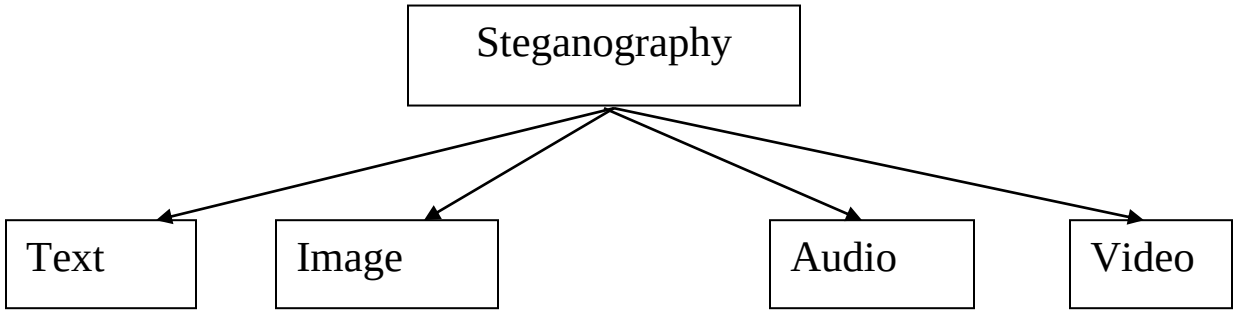
Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner and is an art of hiding information in ways that avert the revealing of hiding messages.The secure data transmission over internet is achieved using Steganography. Video files are generally a collection of images. so most of the presented techniques on images and audio can be applied to video files too.[1] [5] 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. The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Cryptography, on the other hand obscures the content of the message. We propose a high capacity data embedding approach by the combination of Steganography and cryptography.[6][3]

Keywords:- Steganography, Data hiding, File Security, Frame Extraction, Consumer Videos, LSB Technique etc

I. INTRODUCTION

Development in networking and technology has posed serious threats to obtain secured data communication. This has driven the interest in computer security researchers to overcome the serious threats for secured data transmission. The one method of providing more security to data is information hiding. The approach to secured communication is cryptography, which deals with the data encryption at the sender side and data decryption at the receiver side. The main difference between steganography and cryptography is the suspicion factor. The steganography and cryptography are implemented together, the amount of security increases. The steganography make presence of secret data appear invisible to eaves droppers such as key loggers or harmful tracking cookies where the users keystroke is monitored while entering password and personal information. The Steganography is used for secret the data transmission. Steganography has been derived from the Greek word steganos which means “covered” and graphia which means “writing”, therefore Steganography means “covered-writing”. In steganography the secret image is embedded into the cover image and transmitted in such a way that the existence of information is undetectable and unreadable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, images or cipher text etc. The steganography method provides embedded data in an imperceptible manner with the high payload capacity. Encrypting data provides data confidentiality, authentication, and data integrity.

Types of Steganography:



Text: In this only text data in hiding. For text we generally prefer cryptography rather then steganography

Image: For Image steganography data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image

Video: In this type information will be hiding in video. Several new approaches are developed in video data is in the form for .mpeg, avi, .mp4. A Steganography technique such as LSB, DCT, DWT and Vector embedding is generally used. Most of times Video data is contain both the video and audio information.

Audio: In audio steganography, the basic spread spectrum (SS) method attempts to spread secret Information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound.

Steganography is the practice of masking messages or information within other non-secret text or data. Hiding of information or message is achieved through hiding information in other information, thus hiding the existence of the transmitted information.

II. RELATED WORK

H S ManjunathaReddyet al. [1] proposed secure data transmission over internet is achieved using Steganography with High Capacity and Security Steganography using discrete wavelet transforms (HCSSD). The capacity of the proposed algorithm is increased as the only approximation band of payload was considered. A**mitavaNaget et al. [2]** focuses on major importance is given on the secrecy as well as the privacy of information as Image Steganography. Embedded of embedding process is hiddenunder the transformation (DWT and IDWT) of cover image. These operations provide sufficient secrecy.**Mazdak Zamani et al. [3]** described steganography technique by modifying an audio signals. They have developed their using genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness.**SherlyA P et al [4]** discussed about a novel steganographic approach called tri-way pixel-value differencing (TPVD) is used for embedding. All the processes are defined and executed in the compressed domain.**Poonam V Bodhak et al [5]** designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applied imperceptible modification. This Stego system implements steganography in video image and reveal process without restarting a different application. Also this system is Platform Independent application with high portability and high consistency.**KousikDasgupta et al [6]** proposed hash based LSB technique for video steganography. The Proposed Method isanalyzed in term of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames.**Nitin Jain et al [7]** shown steganography process with edges of images can be used to hiding

text message. This is done with help of edge detection filters. By using the edge detection approach along with least significant bit method leads to high security even with a little object as an image, the embedded image is just like the original one.**A. Swathi at al [8]** describes a data hiding scheme was be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. In this information was embedded based on the stego key.**Shamim Ahmed Laskar et al. [9]** proposed a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access.**Ashish T. Bhole et al. [10**] describes steganography over Video File using Random Byte Hiding and LSB Technique. Authors have given comparative analysis of video steganography techniques, encryption and decryption time and hiding data ratio (per frame) in tabular form.

III. ALGORITHM

a. TPVD Algorithm

A steganographic algorithm for compressed video is introduced here, operating directly in compressed bit stream. In a GOP, secret data's are embedded in I frame, and in P frames and in B frames. This proposed secure compressed video Steganographic architecture taking account of video statistical invisibility.[1] The frame work is shown in the Figure 1

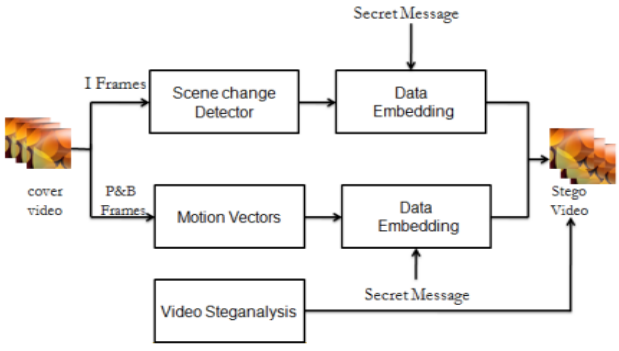


Figure 1: Block diagram of the proposed System

This architecture consists of four functions: I P and B frame extraction, the scene changedetector, motion vectors calculation and the data embedder and steganalysis. The first section explains the extraction of I P and B frames from MPEG video. In the next section, scene change detector analyzes the frames with maximum scene change.[8][9] I frames in MPEG standard is coded in intra frame manner, we can obtain the DC picture with abstracting the DC coefficients from the DCT coefficient codes. below describes the compare method between two conjoint I frames.

b. Random Byte Hiding Technique

In this technique, the information is hiding in each line of the video frame at the different place. For example, if the line begins with the pixel value of 'zz', the information is stored over the 'zz'+x location, where x is only known to the authorized receiver. So, when unknown person view the video, he sees it as normal video, while the person knowing the steganography can detect the hidden message. The same kind of technique can be implemented by using 'y-zz' where y must be taken above the 256 (a bit higher than logical high level) so that 'y-zz' does not go negative. The similar technique can be implemented over the column line also.[1] [3] The lossless steganography requires storing the hidden information in a specific location and will requires some time to run the algorithm and to find the specific location where hidden information will be stored. Thus, in real time application, the lossless algorithm is becoming tougher to implement, and that depends on the system specifications. The proposed framework shows that how the agreement is made. There may be many variations can be done in this agreement and the different steganography technique can be generated. The location of pixel whose D0 bits are going to affect, the frame wise location changing, the sequence of storing etc. are the properties of the algorithm which can modify to generate different algorithm. Method for the data hiding is based on video steganography where we have used the AES

algorithm to make the steganography more secure and robust.

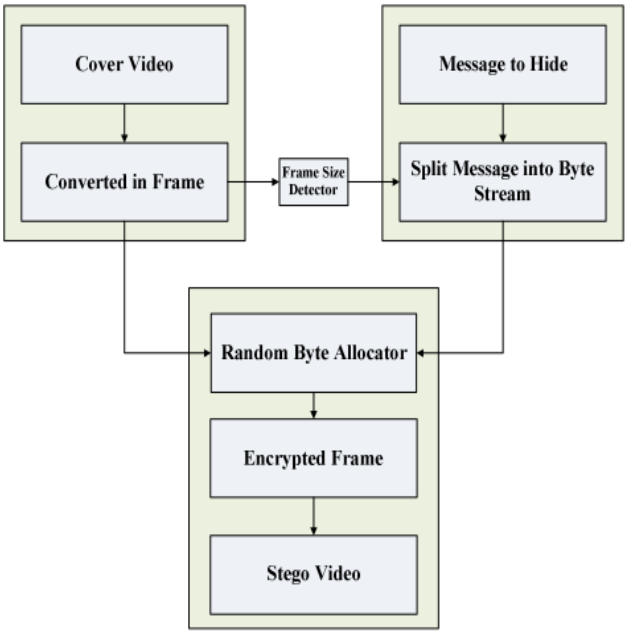


Figure 2:Proposed Framework for Video Steganography Encoding for Random Byte Hiding Technique

The video steganography is achieved by embedding the video files with the secret data that is to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end.

c. LSB Technique

Least Significant Bit (LSB) insertion is a common, simple 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[6]. 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. We implemented our project such that it can accept and video of any size. For example a grid for 3 pixels of a 24 bit image can be as follows: [1][2][4]

(00101101 00011100 11011100)

(10100110 11000100 00001100)

Algorithm to embed text message:-

Step 1: Read the cover image and text message which isto be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixels of cover image.

Step 4: Replace LSB of cover image with each bit ofsecret message one by one.

Step 5: Write stego image Algorithm to retrieve textmessage:-

Step 1: Read the stego image.Step.

2: Calculate LSB of each pixels of stego image. Step

3: Retrieve bits and convert each 8 bit into character.

IV. RELATED WORK

H S ManjunathaReddyet al. [1] proposed secure data transmission over internet is achieved using Steganography with High Capacity and Security Steganography using discrete wavelet transforms (HCSSD). AmitavaNaget et al. [2] focuses on major importance is given on the secrecy as well as the privacy of information as Image Steganography. Embedded of embedding process is hidden under the transformation (DWT and IDWT) of cover image. Mazdak Zamani et al. [3] described steganography technique by modifying an audio signals. They have developed their using genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness.Sherly A P et al [4] discussed about a novel steganographic approach called tri-way pixel-value differencing (TPVD) is used for embedding . All the processes are defined and executed in the compressed domain. Thoughdecompression is not required.Poonam V Bodhak et al [5] designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method.KousikDasgupta

et al [6] proposed hash based LSB technique for video steganography. The Proposed Method isanalyzed in term of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. As result with proposed technique is compared with existing LSB based steganography and the results are found to be encouraging.Nitin Jain et al [7] shown steganography process with edges of images can be used to hiding text message. This is done with help of edge detection filters.A. Swathi at al [8] describes a data hiding scheme was be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. In this information was embedded based on the stego key. Shamim Ahmed Laskar et al. [9] proposed a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access.Shikha Mohan et al. [13] In this paper, Survey, classification and application of various methods of steganography were discussed. Most of the techniques work on the least significant bits of the pixel values. Results shows that LSB based steganography perform better than others. DWT domain shows promising results and outperforms DCT embedding especially in terms of compression survival.

REFRENCES

[1] Reddy, HS Manjunatha, and K. B. Raja. "High capacity and security Steganography using discrete wavelet transform." International Journal of Computer Science and Security (IJCSS) (2009).

[2] Nag, Amitava, et al. "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding." International Journal of Computer Science and Security (IJCSS) (2009).

[3] Zamani, Mazdak, et al. "An approach to improve the robustness of substitution techniques of audio Steganography." Computer Science and Information Technology, 2009.ICCSIT 2009.2nd IEEE International Conference on.IEEE, (2009).

[4] Sherly, A. P., and P. P. Amritha. "A compressed video steganography using TPVD." International Journal of Database Management Systems (IJDMS) (2010).

[5] Bodhak, Poonam V., and Baisa L. Gunjal. "Improved protection in video Steganography using DCT & LSB." International journal of engineering and innovative technology (IJEIT)(2012).

[6] Dasgupta, Kousik, J. K. Mandal, and ParamarthaDutta. "Hash based least significant bit technique for video steganography (HLSB)." International Journal of Security, Privacy and Trust Management (IJSPTM) (2012).

[7] Jain, Nitin, SachinMeshram, and ShikhaDubey. "Image Steganography Using LSB and Edge–Detection Technique." International Journal of Soft Computing and Engineering (IJSCE) (2012).

[8] Swathi, A., and Dr SAK Jilani. "Video Steganography by LSB Substitution Using Different Polynomial Equations." international Journal Of Computational Engineering Research (IJCER) (2012).

[9] Laskar, Shamim Ahmed, and KattamanchiHemachandran. "High Capacity data hiding using LSB Steganography and Encryption." International Journal of Database Management Systems (IJDMS) (2012).

[10] Bhole, Ashish T., and Rachna Patel. "Steganography over video file using Random Byte Hiding and LSB technique." Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on.IEEE, (2012).

[11] Sharma, Vipul, and Sunny Kumar. "A New Approach to Hide Text in Images Using Steganography." International Journal of

Advanced Research in Computer Science and Software Engineering (2013).

[12] Jenifer, K. Steffy, G. Yogaraj, and K. Rajalakshmi. "LSB Approach for Video Steganography to Embed Images." International Journal of Computer Science & Information Technologies (2014).

[13] Shikha Mohan and Satnam Singh "Image Steganography: Classification, Application and Algorithms", International Journal Of Core Engineering & Management (IJCEM) Volume 1, \Issue 10, January 2015.