Hiding Text in Video Using Steganographic Technique - A Review

Jaspreet Kaur , Jagroop Kaur
Deptt. of CE, Punjabi University, Patiala.
Jaspreetkhurmi40@gmail.com,Jagroop_80@rediffmail.com

ABSTRACT
This paper presents the hiding of text in video using haar wavelet transform in particular frame and BCH codes. Haar wavelet transform is applied to get the low frequency sub-band in an image to hide data. The frequency sub-bands are (LL, LH, HL and HH). BCH codes are used to encrypt the data. The work of various researchers is discussed about video steganography and their techniques for embedding and extraction of data. With the advancement of technology and multimedia information, Videos and digital images are increasing very quickly. Steganography is hiding private or secret data within a carrier in invisible manner. A lot of information can be stored in video files. It contains number of frames played over a period of time. .Information can be stored in any or number of frames. Moreover, Attacker or Human eye cannot detect the presence of message in video because video frame is only visible for a fraction of time.
Keywords: Steganography, Cryptography, Encryption Algorithm.

I. INTRODUCTION

Video Steganography is a very important task in real life where the users want to keep data secret. Data is the heart of computer communication and over the years, different methods have been proposed and created to accomplish the goal of using steganography to hide data.
The problem occurs when Traditional Text and Image Based Steganography techniques is not plentiful .They are able to carry only small files. So there is a problem, how to get much enough files to hide our message. This becomes a very tedious task for carry large amount of data. Here, comes the need of Video Steganography. The use of video as a carrier cover for the secure message is overcame the capacity problem. Information can be hidden in any frame of video. Video has a large Capacity to store information. Added small enhancement to the security aspects. The integration

of Steganography and cryptography techniques provided powerful systems for sharing secure messages.

II. LITERATURE SURVEY

Now a days, for secret and secure communication video steganography has become a well liked option. The performance of any steganography algorithm is based on some parameters. In this paper, the author proposed a novel video steganography algorithm based on the KLT tracking algorithm and BCH codes in the wavelet domain. The proposed algorithm encompasses four distinct steps. First, in the encryption process the secret message is preprocessed, and secret message is encoded by applying BCH codes (n, k, t). Second, to identify the facial regions of interest, face detection and face tracking algorithms are applied on the cover videos. Third, In the Embedding process embeds the encoded secret message into the high and middle frequency wavelet coefficients of all facial regions are achieved. Forth, In the extraction process, extracting the secret message from the high and middle frequency wavelet coefficients for each RGB components of all facial regions is accomplished. Experimental results of the proposed video steganography algorithm have demonstrated a more embedding efficiency and a more embedding payload. [1]
Present day, Researches are usually focused on Linguistic steganography. This paper proposed a new steganographic method with an Indian local language, Malayalam. The proposed method is based on custom Unicode technique with embedding based on indexing, i.e. firstly the original message is

encoded to Malayalam text with custom UNICODE values produced for the Malayalam text. The comparison of the proposed method against an existing method depicts that, the proposed steganography methods is more accurate in the encoding as well as in decoding process. [2]

Steganography is a technique that is used to hide data and that data is cannot be detected by attacker. Steganography is basically used for data securing applications. Steganography hides the existence of the message so that attacker cannot identify the presence of message and unable to decrypt it. In this paper, multiple color images are hidden into a single color image using the Discrete Wavelet Transform. The cover image is split up into R, G and B planes. Secret images are embedded into these planes. An N-level decomposition of the cover image and the secret images are done and some frequency components of the same are combined. Secret images are then extracted from the stego image. Here, the appearance of both stego image and the original image is almost same with high overall security. [3]

In this literature, an image steganography technique is proposed that is used to hide audio signal in image in the transform domain using wavelet transform. The audio signal in any format i.e. MP3 or WAV or any other type is encrypted and carried by the image. Viewer cannot recognize the existence of signal. Whenever the secret information is hidden in the carrier the result is the stego signal. In this paper, the quality of the stego image is measured by some parameters i.e. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Universal Image Quality Index (UIQI). The quality of secret audio signal that is extracted is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC). The results describe good values for these parameters. The results show good quality stego signal and the stego signal is analyzed for different attacks. This technique found robust and it can hold out against the attacks. [4]

In this literature, the author proposed an efficient video steganography algorithm based on the binary BCH codes to improve the security and efficiency. With the help of private key, First the pixels positions of the video frames components are arbitrary permuted. Furthermore, the bits positions of the secret message are also permuted by using the same private key. Next , to preserve the message from being read. The secret message is encoded by applying BCH codes (n, k, t), and XORed with random numbers before the embedding process. The preferred embedding area in each Y, U, and V frame components is randomly chosen, and will vary from frame to frame. After that the embedding process is accomplished by hiding each of the encoded blocks into the 3-2-2 least significant bit (LSB) of the YUV pixels that was selected. Experimental results indicates that the proposed algorithm have a high embedding efficiency, high embedding payload, and resistant against hackers. [5]

In this paper, the Author presents a secure information hiding technique that uses random key encoding function for video images. Secret information is embedded into the random Red Green Blue (RGB) pixel values of the cover-video images using an encryption key. To avoid overflow/underflow the cover-video images are pre-processed. Experimental results depicts that the information that is extracted are without any errors. The performance of the proposed scheme is verified in terms of (Peak signal noise ratio) PSNR values and security. [6]

Here, the Author developed a system to embed any kind of file in another file, which is called carrier file or carrier media. The carrier media must be a video file for video steganography. Along with steganography we use Cryptography to make the files more secure. This technique is used for secure transferring of data. In Cryptography the data is encrypted into unreadable form and is hidden but more securely. Without any modification required in the host signal range while hiding data the algorithm that is used is called Forbidden Zone Data Hiding algorithm .The secret data should not be extremely degraded and should be as imperceptible as possible. The embedded data should be as unaffected to modifications from attacks. [7]

In this paper, the algorithm elaborated with the aim to hide a “secret” color video sequence within another color video sequence with the help of wavelet transform in order to split up the cover video sequence and then replace the less noticeable wavelet band with “secret” video frames has been implemented and tested. On the receiver side, to recover the hidden color video from stego color video

the process is reversed. Proposed algorithm has been implemented using MATLAB and PSNR and MSE error parameters are used to evaluate the quality of both video sequences. [8]

In this paper a method for hiding of information on the poster or advertising board is presented. It is generally known that encryption give secure channels for communicating entities. Here, an author proposes a new form of steganography, on-line hiding of information on the output screens of the instrument. This method can be used for notify a secret message in public place. It can be extended to other means such as electronic billboard around sports stadium, railway station or airport. This steganographic method is very close to image steganography and video steganography. Here, symmetric key steganography technique and LSB technique is used for hiding the secret information for Private marking system. [9]

In this paper, we present a new self adaptive algorithm in color images for segmenting human skin regions. Due to high variance and low specificity of human skin color such models are used for pixel based classification, but its efficiency is finite. So, skin model adaptation and spatial analysis were described to upgrade the final segmentation outcome; Though, little attention has been paid to merge these two improvement directions. To determine the seeds for the spatial analysis our main focus lies in learning a local skin color model on the fly, which is finally applied to the image. Moreover, we also take a choice of textural features for computing local propagation costs that are used in the distance transform. The outcome of this thorough study indicates that the proposed method is highly competitive, particularly for finding hand regions in color images. [10]

At present, steganography in digital media is the most fruitful approach to embed the payload while decreasing a well defined distortion function. The Expert's aim is to design the distortion to attain a technique with a high empirical mathematical detectability. The only task that is left to the steganographer is the design of the distortion since effective practical codes exist that embeds near the payload distortion bound. In this paper, author propose a universal distortion design called universal wavelet relative distortion (UNIWARD) that can be applied for embedding in an randomly domain. Then the embedding distortion is calculated as a sum of respective changes of coefficients in a directional filter bank while perform decomposition of the cover image. The portions of the cover object those are tough to model in multiple directions, such as textures or noisy regions or clean edges then the directionality forces the embedding changes to such portions. It is determined experimentally using rich models as well as targeted attacks that steganographic methods produced using UNIWARD match or out perform the current state of the art in the spatial domain, JPEG domain, and side informed JPEG domain. [11]

In this paper, the author proposes a novel video steganography technique for efficient and effective information hiding. Today, video is considered to be an effective and important tool for communication. Video steganography uses video that act as a container for embedding secret information. In this paper, A 3-3-2 LSB based scheme has been used as a base technique for video steganography. To decide the goodness of any steganographic scheme two key parameters i.e. Imperceptibility and video quality is used. Thus the base technique is raised or increased using Genetic Algorithm (GA) which succeeds to get best imperceptibility of hidden information. An anti-steganalysis test is used to check for the quality of the frame with respect to original frame. Experimental results show a significant improvement in the Peak Signal Noise Ratio (PSNR) and Image Fidelity (IF) values after optimization over the base technique. Complexity analysis of the proposed technique is also described in this paper. [12]

Video Steganography is a process of hiding secret data or information within a video. Here, Video is a cover medium. In this paper, a spatial domain hash based least significant bit (LSB) technique has been presented in which the secret information is embedded in the LSB of the cover frames. A hash function is used to find out the position of insertion in LSB bits and that LSB positions are used to hide data. 8 bits of the secret information is divided into 3, 3, 2 and embedded into the RGB pixel values of the cover frames correspondingly. The performance of the proposed method is analyzed in terms some metrics i.e Peak Signal to Noise Ratio (PSNR) as well as the Mean Square Error (MSE) and estimation of embedding capacity is measured between the original and steganographic files. Image Fidelity (IF) is

also measured and the results represent least reduction of the steganographic video file. The proposed technique is compared with existing LSB based steganography technique and the results are found to be promising. [13]

Video Steganography is a method to hide any kind of secret files into a Video file. The use of video as a carrier cover for the secure message overcame the capacity problem. Information can be hidden in any frame of video. The least significant bit (LSB) insertion is an essential approach for embedding information in a cover file. In this literature, a data hiding scheme will be presented to hide the secret data in particular frames of the video and in particular location of the frame by LSB substitution using polynomial equation. [14]

In this paper, the LSB technique is used to hide images within the video file, evidently safe images. An encrypted image or files may quiet hide information using steganography, so when the encrypted file is decoded, the hidden message is not seen. The LSB approach is used in conjunction with the Transformations techniques, Masking- Filtering and to hide the secret image or any other files. [15]

In this work we propose a novel technique of digital video encryption that is expanded into a novel type of digital video steganography where it is viable to camouflage a given video with another video. So, there are so many algorithms for digital video encryption and we introduce an extended classification of digital video encryption along with advantages over currently available scheme. Therefore, the proposed method is tested on the basis of security and performance aspects and the results describes that the method is efficient and secure from a cryptographic perspective. Although the method is right now suitable only for a certain class of video sequences and video codecs, the method is encouraging and future analysis might notify its vast suitability. [16]

III. ENCRYPTION AND EMBEDDING PROCESS

The secret message is encrypted through BCH codes.BCH codes are multiple error correcting codes which were invented by Bose, Chaudhuri, and Hocquenghem. The embedding process takes a cover video and a secret message as the inputs.

Step 1: First take an original video as cover video. Then convert it into number of frames or images. Select n as the input cover image.

Step 2: Apply Haar Wavelet Transform to decompose into different frequency sub-bands.

Step 3: Select LL sub-band to hide data. Add a key for more security.

Step 4: Load a secret text which embed into the cover image.

Step 5: Apply the steganography algorithm based on wavelet transform and BCH code to hide the data.

Step 6: Get the resultant stego video.

IV. EXTRACTING PROCESS

It basically follows the reverse process of the hiding algorithm to obtain the secret message. Following steps are carried out to recover the hidden information:

Step 1: Load the stego video.

Step 2: Apply inverse wavelet and BCH algorithm to recover the secret code.

Step 3: Compare the extracted code with original.

Step 4: Compute psnr, mse and other parameters for algorithm efficiency.

CONCLUSION AND FUTURE SCOPE

This work is a review work and covers various techniques for data/text embedding in a given video. The robustness of the steganography algorithm is evaluated by computing the psnr, mse and other statistical parameters that are computed from the extracted code from the stego input. The robustness of the algorithm is evaluated by extracting the secret code form the stego input by using different existing technique like LSB, wavelet and dct etc. and then comparing the recovered secret code with the original

code. In Future, the security, robustness and efficiency finds potential room for improvement. The enhanced and robust algorithm for steganograpgy is in development stage and the results of the same are expected soon.

REFERENCES

1. Mstafa, Ramadhan J., and Khaled M. Elleithy. "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes." Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015.
2. Vidhya, P. M., and Varghese Paul. "A Method for Text Steganography Using Malayalam Text." Procedia Computer Science 46 (2015): 524-531.
3. Baby, Della, et al. "A Novel DWT Based Image Securing Method Using Steganography." Procedia Computer Science 46 (2015): 612-618.
4. Hemalatha, S., U. Dinesh Acharya, and A. Renuka. "Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image." Procedia Computer Science 47 (2015): 272-281.
5. Mstafa, Ramadhan J., and Khaled M. Elleithy. "An Efficient Video Steganography Algorithm Based on BCH Codes." (2015).
6. Ramalingam, Mritha, and Nor Ashidi Mat Isa. "A steganography approach over video images to improve security." Indian Journal of Science and Technology8.1 (2015): 79-86.
7. Satpute, Snehal, et al. "An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding)." (2015).
8. Kolakalur, Anush, Ioannis Kagalidis, and Branislav Vuksanovic. "Wavelet Based Color Video Steganography." International Journal of Engineering and Technology 8.3 (2016): 165.
9. Jenifer, K. Steffy, G. Yogaraj, and K. Rajalakshmi. "LSB Approach for Video Steganography to Embed Images." International Journal of Computer Science and Information Technologies (2014).
10. Kawulok, Michal, et al. "Self-adaptive algorithm for segmenting skin regions."EURASIP Journal on Advances in Signal Processing 2014.1 (2014): 1-22.
11. Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014.1 (2014): 1-13..
12. Dasgupta, Kousik, Jyotsna Kumar Mondal, and Paramartha Dutta. "Optimized Video Steganography Using Genetic Algorithm (GA)." Procedia Technology 10 (2013): 131-137.
13. Dasgupta, Kousik, J. K. Mandal, and Paramartha Dutta. "Hash based least significant bit technique for video steganography (HLSB)." International Journal of Security, Privacy and Trust Management (IJSPTM) 1.2 (2012): 1-11.
14. Swathi, A., and Dr SAK Jilani. "Video Steganography by LSB Substitution Using Different Polynomial Equations." MadanapalliInstitude of Technology and science (2012).
15. Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data."arXiv preprint arXiv:0912.2319 (2009).
16. Socek, Daniel, et al. "New approaches to encryption and steganography for digital videos." Multimedia Systems 13.3 (2007): 191-204.