

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 2 ISSUE : 4 Print / Issue Publication Date: 31-Mar-2017

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 275-278
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)



HIDING TEXT IN VIDEO USING STEGANOGRAPHY - A REVIEW

Er. Gursukhmanipreet Kaur
CU, University Gharaun

Er. Sandeep Kaur
GVIET, Banur, Punajb, India

Abstract— **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

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphical " means "writing" . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia objects like audio, video, images are used as a cover sources to hide the data. Video steganography is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Video Steganography is the art of hiding information in ways that avert the revealing of hiding messages in videos. Actually message like text, image, audio, video and etc. The major work of video Steganography is hide secret message without affecting the visual quality, structure and content of the video file. Video Steganography deals with hiding secret data or information within a video. It is a technique of hiding any kind of files or data into digital video format. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files. It is focused on spatial and transform domain. Spatial domain algorithm directly embedded information in the cover image with no visual changes with good quality. The result of algorithms has the advantage in Steganography capacity. Transform domain algorithm is embedding the secret information in the transform space. This kind of algorithms has the advantage of good stability, but the disadvantage of small capacity. Video steganography is combination of both images and audio.

Video:- Video is the technology of electronically recording, transmitting, storing, capturing, and reconstructing a sequence of still images representing scenes in motion.

Steganography:-Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphial " means "writing".

Characteristics of Video Steganography

Following are important characteristics of the video.

Frame Rate: - The number of still pictures per unit of times of video the ranges from six or eight frames per second (frame/s).

Size: - The Size of a video image is measured in pixels for digital video. Horizontal scan lines and vertical lines of resolution for analog video**.**

Aspect Ratio: **-** It describes the dimensions of video screens and video picture elements.

Video Formats: **-** All popular video formats are rectilinear, and so can be described by a ratio between width and height.

Video Quality: **-** It can be measured with formal metrics like PSNR or with subjective video quality using expert observation.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 275-278
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)



Advantages 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 REVIEW

Now a day, 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 algorithms encompass 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 a middle frequency wavelet coefficient of all facial regions is 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].

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 [3].

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 [4].

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 [5].

In this paper,the main focus of an authors is on rising data security with the help of dual steganography. In this steganography the secret information is firstly inserted into cover medium and then the produced stego-object will be one more time inserted into other cover medium. Proposed paper also gives a measureable evaluation of dual steganography which depicts decline in the mean square error (MSE) and raises the peak signal to noise ratio (PSNR) between actual files and produced stenographic files. An initial result displays the large imperceptibility of the proposed technique in addition to the hiding capacity of discovered technique [6].

It examined just video steganography. In case of video steganography technique the secret information is enclosed within a video to make it harmless from attackers. In this paper, Author importantly considers basic concepts, performance metrics and protection feature of video steganography. Special techniques are used for protecting secret information with the help of video as cover medium are discovered. Contrasts between other video steganography methods are also displayed. This paper also depicts Steganalysis in concise [7].

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 4, ISSN No. 2455-2143, Pages 275-278
Published Online February-March 2017 in IJEAST (http://www.ijeast.com)

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 [8].

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 [9].

Image Steganography plays a vital role to hide information interior an image. The main objective of this steganography approach is to hide data within a stego-image by reducing the number of bit flips. In this paper, the author has been proposed a new steganography technique with the help of Graphical codes and also comparison with steganography technique using BCH codes and with other techniques [10].

III. ENCRYPTION AND EMBEDDING PROCESS

The embedding process takes a cover video and a secret message as the inputs.

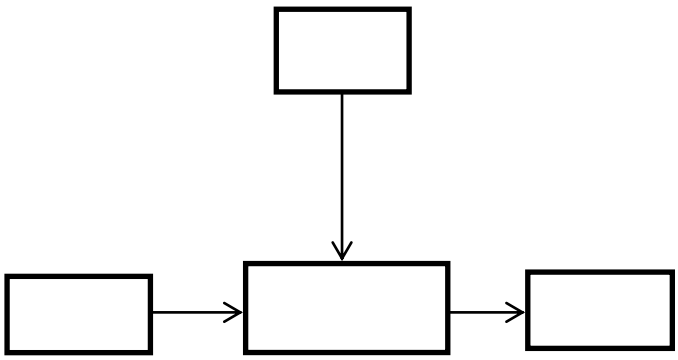
Step 1: First take an original video as cover video. Then convert it into number of frames or images. Then select a particular frame/image; this will act as cover image.

Step 2: Add a password graphically for more security.

Step 3: Load a secret text which embed into the cover image.

Step 4: Then apply any Technique to get a stego-image.

Step 5: At last, have a stego video. This video is ready for the transmission through the internet.



IV. EXTRACTING PROCESS

It basically follows the reverse process of the hiding algorithm to obtain the secret message.

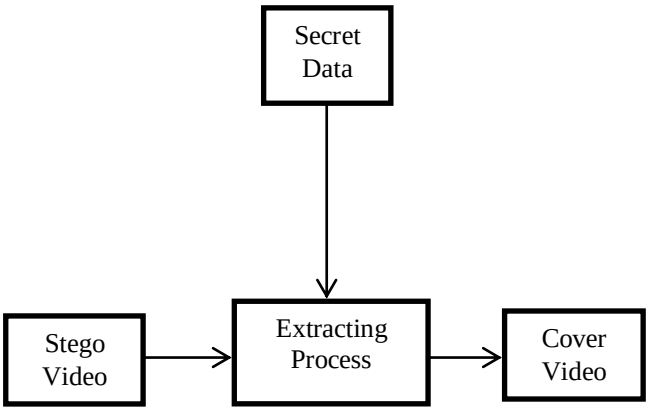
Steps to recover the hidden information:

Step 1: Load the stego video.

Step 2: Enter the password to get the secret message.

Step 3: Apply technique that we have used in embedding Process on the stego image.

Step 4: Get the secret message and original video.



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

VI. REFERENCES

[1]. Ramadhan J. Mstafa, Khaled M. Elleithy, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes," 978-1-4577-1343-9/12/$26.00 ©2015 IEEE.

[2]. Vidhya P.Ma,Varghese Paulb,*, "A Method for Text Steganography Using Malayalam Text," Procedia Computer Science 46 (2015) 524 – 531.

[3]. Anush Kolakalur, Ioannis Kagalidis, and Branislav Vuksanovic, "Wavelet Based Color Video Steganography," IACSIT International Journal of Engineering and Technology, Vol. 8, No. 3, March 2015.

[4]. K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi, "LSB Approach for Video Steganography to Embed Images,"



International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 319-322, ISSN:0975-9646.
[5]. A.Swathi, "Video Steganography by LSB Substitution Using Different Polynomial Equations,"International Journal Of Computational Engineering Research Vol. 2 Issue. 5, September 2012.
[6]. Jigar Makwana, S.G Chudasama. . "Dual Steganography: A New Hiding Technique for Digital Communication.." Vol. 5, Issue 4, April 2016
[7]. 3 Bharti Chandel, Dr.Shaily Jain. . "Video Steganography: A Survey.." IOSR Journal of Computer Engineering (IOSR-JCE) Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17.
[8]. Baby, Della, et al. "A Novel DWT Based Image Securing Method Using Steganography." Procedia Computer Science 46 (2015): 612-618.
[9]. 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.
[10]. Sensarma, Debajit, and Samar Sen Sarma. "Data Hiding using Graphical Code based Steganography Technique." arXiv preprint arXiv: 1509.08743(2015).

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

Er. Gursukhmanipreet Kaur

Er. Sandeep Kaur

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com

www.ijeast.com

India

2455-2143