ISSN No: - 2456- 2165

A Review of Different Methodologies for Video Steganography

Sachin Jangid
M.Tech Scholar
MACERC
Jaipur, Rajasthan, India

Somesh Sharma
Professor, E.C.E Deptt.,
MACERC ,
Jaipur, Rajasthan, India

Abstract- Data protection is a basic required field in communication medium across the internet network. In this paper, we concentrate on the data protection methodology with encryption or decryption. Steganographic methods are using for hidden communication through hiding the information inside the multimedia data files. Video Steganography is also a process to cover up any type of data into a carrying Video file.

Keyword : - *Steganography, Digital watermarking, Least Significant Bit, Discrete Wavelet Transform, Discrete Cosine Transform.*

I. INTRODUCTION

Information security is a way to protect a database from harmful forces and the unwished actions from the unofficial users. Large number of private information data is being switched over the Internet (publicly open medium) because it is the most efficient and widely available way. This process also provide digital data very hard security for interception and then it is not possible for unofficial access / use and make it easy for reduce losses for the content producers and rights holders. To secure information on public channels, the protection measures need to be comprised into data communication systems over the Internet [1]. Steganography is one of the good method for provide help to attain the general goal of secure delivery of data from its source to the destination end-users. Steganography is the method of hiding a file, image, or message within another a file, image, or message. The word steganography is of Greek origin and it means "covered writing" or "concealed writing"[2]. Steganography is varying the digital media in a mode in which just the sender and the receiver is capable to detect the message sent by it. On the other side steganalysis is the science of detection hidden message [3]. The target of steganalysis is to divide steganography arrangement and that condition is met if an algorithm can judge whether a given image contains a secret message. To decrease the possibility of attacks, protection requires to be hold hidden i.e. invisible security. The important data can be introduced into multimedia documents in a way that can't be patched. Digital Watermarking method is applied to better the imperceptibility (i.e. invisibility) and robustness. Digital watermarking can be applied on any digital image, audio file or text file. Digital watermarking is the method of introducing a digital signal or pattern (indicative of the owner of the content) into digital content. The signal (also known as a watermark) can be applied to describe the owner work, to tracing illegal copies and to authenticate the subject of the work. Steganography and watermarking are differ in a number of ways including use, specification and detecting/extraction techniques. The basic difference is that the target of communication in watermarking is the host signal with the embedded information which allowing copyright security. In steganography, the target to be transmitted with the embedded message and the cover signal attends as an chosen fairly arbitrarily by the user supported on its technological suitability. The third party cannot find the message in stego media but in watermarking, the third party cannot take or replace the message. It basically prevents the illegal copy. Further, the creation of the watermark is extracted openly and any effort to remove or avoid the embedded content renders the host useless. The vitally significant demand for steganography is perpetual and algorithmic undetectability. Robustness versus malicious attacks and signal processing is not the basic concern as it is for watermarking.

II. STEGANOGRAPHY

Steganography is converting the digital media in a direction that only the transmitter and the intended recipient is capable to observe the message sent by it. The following method allows a very generic description of the pieces of the steganographic method [4]:

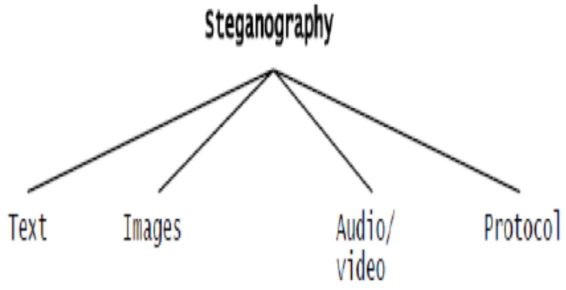

Fig 1: Categories of steganography

cover_medium + hidden data + stego_key = stego_medium

In this context, the cover_medium is the data file in which it is applied to hide the information, which may be encoded using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium).

Almost all digital data file formats can be used for steganography, but the formats that are more appropriate are those with a high degree of redundance. The redundant bits of an object are those bits that can be adapted without the alteration being observed easily. Video and image files specially comply with this demand that can be applied for data hiding. In fig 1, shows the four main categories of file formats that can be used for steganography.

In text, hiding data is historically the most significant technique of steganography. This technique use to hide a private content in every nth letter of every word of a text content. In video steganography, a digital video consists of a set of frames (images) that are played back at positive frame rates which based on the video standards. Video steganography covers the message in any one of the frames/images, after hiding, iI is very hard to examine in which the data/message is invisible [5].

III. LITERATURE REVIEW

In 2014 Kamred Udham Singh submitted a research paper for the development of high-speed computer networks and Internet which has increased the easiness of data Communication. In contrast with Analog media and Digital media allow several another advantages like as high quality, simple editing, high dedication copying, and authenticity. But in the area of data communication, this type of development has raised the fear of sneaking the data while transmitting information from the transmitter to the receiver. Due to this reason data Security is the primary problem for information Communication. Steganography acts an significant role in the field of data Security. Video and images are the basic options for hiding data. It is very significant for effective and successful embedding method to select suitable pixels in the video frames, which are applied to store the secret data. We use video supported Steganography because of big size and memory demands. Hiding data in a carrier file they use Least Significant Bit (LSB) insertion method. In the Least Significant Bit (LSB) insertion method, for hiding data, they convert LSB of the video file with the data bits.This paper will focus on hiding data in particular frames of the video and in the specific position of the frame by LSB exchange [1].

In 2013 Vipula Madhukar Wajgade[et.al] submitted a paper for data security which has to get the area of touch as a result of widespread apply for communication medium over the internet. This paper concentrates on the information security techniques as joint with encryption and steganographic methods for private communication by hiding it inside the multimedia system files. The high results are accomplished by allowing the protection to information before broadcasting it over the internet. The files such as images, audio, video carry collection of bits that can be further transformed into images, audio, and video. The files composed of insignificant bits or fresh areas which can be applied for overwriting of other information. This paper explains the proposed technique by use video steganography for increase information security [2].

In 2014 Shivani Khosla[et.al] presented a paper for the fast development of data exchange by the internet which makes it simple to transport the data accurate and more quick to the destination. Besides this, anybody can change and misuse the useful data by the hack it. This paper presents video steganography with digital watermarking methods as an effective and robust tool for security. This paper is a combination of Steganography and watermarking; which allows a solid backbone for its protection. Here considers video as the set of frames or images and any alterations in the output image by hidden information is not visually identifiable. This suggested system not only covers the big volume of information within a video; but also bounds the perceivable distortion that might occur while working it [3].

In 2012 A. Swathi[et.al] Presented a paper for Video Steganography which is a method to hide any files into a carrying Video file. The use of the video based Steganography can be more desirable than other multimedia system files, because of its sizing and memory demands. The Least Significant Bit (LSB) insertion is an significant approach for planting data in a carrier file. Least significant bit (LSB) insertion method works on LSB bit of the media file to cover the data bit. In this project, a data hiding scheme will be built up to hide the data in specific frames of the video and in particular location of the frame by LSB substitution using polynomial equation [4].

In 2012 Syeda Musfia Nasreen[et.al] presented a paper for Data hiding methods which take a big role with the fast growth of intensive transfer of multimedia content and secret communications. The method of Steganography is applied to deal the data secretly and securely. It is the science of planting secret data into the cover media with the modification to the cover image, which cannot be easily known by human eyes. Steganography algorithms can be used in audio, video and image file. Hiding secret data in the video file is called video steganography. Video Steganography signifies, hiding a secret message that can be either a secret text message or an image For hiding secret data in the video, there are lots of Steganography methods which are additionally explained in this paper along with some of the research works done in some fields under video steganography by some authors. The paper shows the progress in the area of video Steganography and signifies to give the comparison between its different uses and methods [5].

In 2015 Kedar Nath Choudry[et.al] presented a paper for handle the information on internet against intruders. Data is normally in the form of text, audio, video and image. Steganography is single good technique to share the data secretly and securely. Steganography methods can be employed for audio, video and image file. Secret data may in the form of text, image or even in the form of video and audio. Hiding secret data in the video file is known as video steganography. In this paper, a review on different video steganography methods has been submitted. Various spatial domain and transform domain techniques of video steganography have been discussed in this paper [7].

In 2015 Swetha V[et.al] presented a paper for Digital data communication which has get an inbuilt part of infrastructure nowadays. In this tech era, with the maximizing popularity of the internet and the quick communicating methods, the security and the confidentiality of the sensitive information has got the prime concern. This has resulted in an occasional growth in the field of data hiding. Cryptography and steganography are the two standard techniques which are free to allow protection. One hides the existence of the message and the other distorts the message itself. Steganography is a method to hide secret data in some other media without allowing any apparent evidence of information alteration. It comes under the assumption that if the feature is open, the point of attack is evident, thus the aim of steganography is always to hide the secret data. This paper allows a state-of-the-art survey and analysis of the different existing techniques of video steganography and also covers classification and applications [8].

In 2014 Jasleen Kour[et.al] presented a paper for Steganography which is formed as the study of transparent communication. Steganography normally deals with the ways of covering the existence of the communicated data in specified a way that it remains confidential. It keeps privacy between two communing parties. In image steganography, privacy is attained by embedding data into cover image and getting a stego-image. There are different types of steganography methods each has their strengths and weaknesses. In this paper, we review the different protection and data hiding methods that are applied to implement a steganography such as LSB, ISB, MLSB etc [9].

In 2015 Abhinav Thakur[et.al] presented a paper for Steganography which is the practice of hiding a file, message, image, or video within different file, message, image, or video. It can also be specified as an hidden communication that hides the existence of the communicated message so that the message does not appeal the attention from eavesdroppers and attackers. The main target of steganography are robustness against various image processing attacks, capacity of the invisible data and undetectability. This paper explores the various methods of image and video steganography that are applied to hide the message in digital carriers [10].

IV. CONCLUSION

Steganography is the method that allows secret communication between two parties. In this paper, main methods of video steganography are discussed. Each steganography method must satisfy the three main targets (imperceptibility, capacity, and robustness). In video steganography, it has been found that frequency based methods are more robust as compared to spatial domain methods.

References

[1]. Kamred Udham Singh," Video Steganography: Text Hiding In Video By LSB Substitution ", in Kamred Udham Singh Int. Journal of Engineering Research and Applications, Vol. 4, Issue 5(Version 1), May 2014.

[2]. Vipula Madhukar Wajgade, Dr. Suresh Kumar," Enhancing Data Security Using Video Steganography ", in International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.

[3]. Shivani Khosla,Paramjeet Kaur," Secure Data Hiding Technique Using Video Steganography and Watermarking ", in International Journal of Computer Applications, Volume 95– No.20, June 2014.

[4]. A. Swathi , Dr. S.A.K Jilani, " Video Steganography by LSB Substitution Using Different Polynomial Equations", in International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, 2012.

[5]. Syeda Musfia Nasreen , Gaurav Jalewal, Saurabh Sutradhar," A Study on Video Steganographic Techniques ", in International Journal of Computational Engineering Research (IJCER) , Volume, 05 , Issue, 10, October – 2015,

[6]. Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa," Video steganography: a comprehensive review", in Multimed Tools Appl , 2014.

[7]. Kedar Nath Choudry, Aakash Wanjari," A Survey Paper on Video Steganography", in International Journal of Computer Science and Information Technologies , Vol. 6 (3) , 2015.

[8]. Swetha V, Prajith V," Data Hiding Using Video Steganography -A Survey", in IJCSET, June 2015.

[9]. Jasleen Kour, Deepankar Verma," Steganography Techniques –A Review Paper ", in International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May 2014.

[10]. Abhinav Thakur1, Harbinder Singh2, Shikha Sharda," Different Techniques of Image and Video Steganography: A Review", Volume 2, Spl. Issue 2 (2015).