www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13760-13764

Review Paper on Various Data Hiding Techniques

Ramandip singh[1], sukhmeet kaur[2]

[1] M. Tech Scholar, CSE, CGC Jhanjeri, Punjab, India
[2] Assistant Prof. , CSE, CGC Jhanjeri, Punjab, India

Abstract- The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is an art of hiding the secret message in a cover object without leaving a remarkable track on the original message. It is used to increase the security of message sent over the internet. In contrast to cryptography, it is not used to scramble the data but it is used to conceal the data in digital media. Thus, this paper reviews various data hiding techniques and briefly explain Steganography.

Keywords- Data hiding, security, DCT, DWT, PSNR, Steganography, least significant bit, Cryptography.

I. Introduction

Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice. Data Hiding is the methodology of furtively implanting data inside a data source without transforming its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that nobody seperated from the sender and intended recipient even realizes there is a hidden message [1]. This apparent message is sent through the network to the recipient, where the actual message is separated from it.

In today's world, Data handling is very risk in internet against intruder. In this case, data means like text, image, audio, video etc. Thus, Stegnography is one of the best methods for secret and securely sharing data's. Genuine significance for Steganography is the art of concealing the message from sender to receiver very secure method [2]. Secure video Steganography is a testing undertaking of sending the embedded data to the receiver without being identified. Basically Steganography utilizing text, image, audio, video.

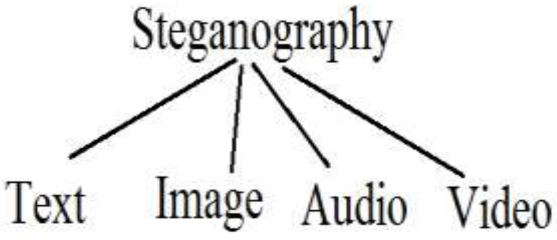

Fig. 1: Areas of Steganography

Steganography is one of the method in which the data is hidden in the cover object with the use of secret key. The extractor should have secret key to extract the data. The secret key designed in such a manner that it can't be find out by an unusual user. In Steganography systems following terms are used:

Cover Media: The cover media is the medium in which message is embedded to hide the presence of secret data.
Stego: The media through which the data is hidden.
Secret data: The data to be hidden or extract.
Steganalysis: The process by which secret data is to be extracted.

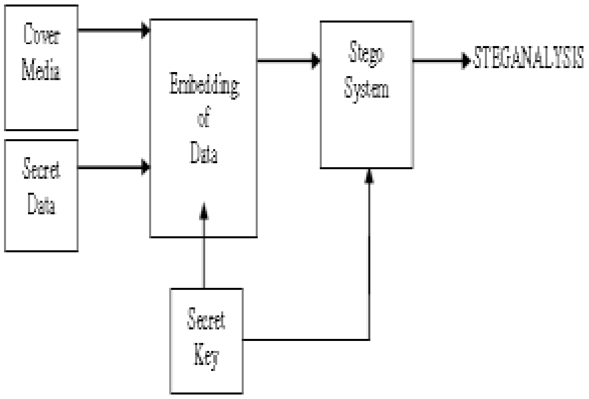

Figure 2: Steganography System

II. Requirements of Data Hiding

Video data hiding presents various issues. Because of a lot of information and natural redundancies between edges, Video indicators are exceptionally vulnerable to theft strike, including casing averaging, edge dropping, casing swapping, factual examination, and so on. To build the power of the plan, we propose a few mixture approaches.

Thus, these systems can be characterized by a number of defining properties including embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, robustness, security, and watermark keys, modification and multiple watermark, cost, tamper resistance, unobtrusiveness, ready detection, unambiguous, sensitivity, and scalability [2]. The relative importance of each property is dependent on the requirement of the application and the role the watermark will play. Some of them are common to most practical applications. In this section, such general requirements are listed and briefly discussed.

a) Robustness

Robustness refers to the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression. Unintentional strikes include changes that are generally connected to pictures throughout typical use, for example, editing, resizing, differentiation improvement and so forth. The utilization of music, pictures and feature motions in computerized structure, ordinarily includes numerous sorts of twists, for example, lossy packing, or, in the picture case, separating, resizing, differentiation upgrade, trimming, turn etc. The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.

b) Reliability

Reliable communication is one of the vital properties of the internet. The internet should guarantee the reliable delivery of the information to the intended recipient.

c) Fault-Tolerance

Fault-tolerance means the ability of the system to operate normally even in the events of failure. Internet should exhibit fault-tolerance so that it keeps on functioning even when there is failure in some part of the internet.

d) Quality of Service Support

Quality of Service (QoS) is one of the crucial properties in terms of communication. Inter should provide QoS support to various applications and sensitive data and should prioritize them depending on the nature of the data.

e) Payload Capacity

It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.

f) Security

An alternate property of a perfect framework is that it actualize the utilization of keys to guarantee that the methodology is not rendered futile the minute that the calculation gets known. It might likewise be an objective that the framework uses a lopsided key framework, for example, openly/private key cryptographic frameworks. Albeit private key frameworks are decently simple to actualize in watermarking, unbalanced key sets are for the most part not. The danger here is that inserted frameworks may have their private key uncovered, destroying security of the whole framework. This was precisely the situation when

DOI: 10.18535/ijecs/v4i8.24

a solitary DVD decoder usage left its mystery key decoded, rupturing the whole DVD duplicate insurance system.

g) PSNR (Peak Signal to Noise Ratio)

It is characterized as the degree between the maximum greatest conceivable power of a signal and the power of corrupting noise that influences the loyality of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.

III. Steganography

The Steganography, Cryptography and Digital Watermarking strategies can be utilized to obtain security and privacy of data. The steganography is the art of concealing information inside another information, for example, cover medium by applying dinstictive steganographic strategies. While cryptography brings about making the data human unreadable form called as cipher, hence, cryptography is scrambling of messages. Though the steganography brings about exploitation of human awareness so it remains imperceptibly and undetected or intact. It is conceivable to utilize all file medium, digital data, or files as a cover medium in steganography. Generally steganography technique is applied where the cryptography is inefficient [3].

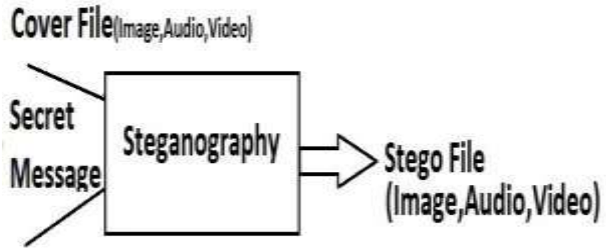

Fig. 3: Steganography

The steganography framework comprises of the cover file (image, audio, video etc) and the secret message that is hidden inside the cover file by applying steganography the secret message is shrouded and stego file is created which is same as cover image and go undetected or unaltered.

Analysts have executed different methodologies for information and data security to accomplish secret communication. Steganography is a strategy of concealing the secret messages into the carrier medium such as image, audio, video etc. Steganography technique is generally characterized into three main types namely, technique exploiting image format, method embedding in frequency domain and method in spatial domain[4].Stego is a greek word which implies hidden.The ancient people utilized different procedures to send the secret messages amid the war time. The assessment of steganography technique is done with three parameters such as capacity, robustness and security[5].The framework ought to be fit for concealing the information into cover media, it should be robust to the changes and it ought to be sufficiently secured enough from eavesdroppers or assailants that has a tendency to distinguish or alter the contents of the secret data[6].

IV. Video Steganography techniques:

Several new approaches are studied in video data Steganography literature. In this section, some of the most well-known approaches have been discussed.

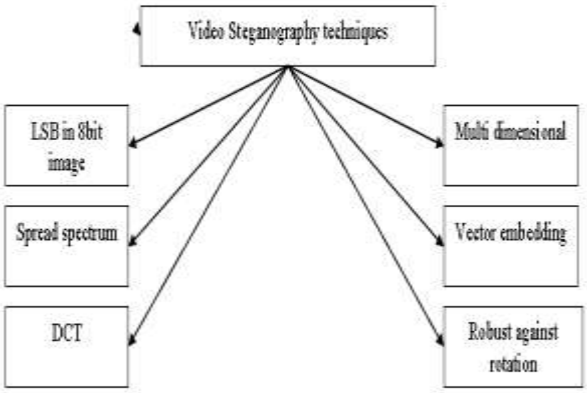

Fig. 4: Techniques of video steganography

- **Spatial Domain Methods**

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based. i) LSB: this method is most commonly used for hiding data. In this method the

DOI: 10.18535/ijecs/v4i8.24

embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image. ii) BPCP: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data iii) PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area. Least Significant Bit method (LSB) which hide secret data into the least significant bits of the host video. This method is simple and can hide large data.

- **Spread Spectrum Technique**

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication. This method satisfies the robustness criterion. The amount of hidden data lost after applying some geometric transformations is very little. The amount of hidden lost is also little even though the file is compressed with low bit-rate. This method satisfies another criterion is security.

- **Transform Domain Technique**

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits.

A technique for high capacity data hiding using the Discrete Cosine Transform (DCT) transformation. Its main objective is to maximize the payload while keeping robustness. Here, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of frames [14]. A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2) .This method embeds audio information to pixels of frames in host video [15].

- **Distortion Techniques**

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

- **Masking and Filtering**

These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

V. Conclusion

In the past few years, Steganography has become an interested field of data hiding techniques. This paper provides an overview of different steganography methods that satisfy the most important factors of steganography design. There are many kinds of steganography techniques are available among them hiding data in video by LSB substitution is a simple method. Here the information will be embedded based on the stego key. Key is used in the form of polynomial equations with different coefficients. By using this, the capacity of embedding bits into the cover image can be increased.

REFERENCES

[1] Yuting Su, Chengqian Zhang, and Chuntian Zhang, “A video steganalytic algorithm against motion-vector-based steganography,” Signal Process, vol. 91, pp. 1901–1909, Aug. 2011.

[2] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad (2013), ‘Video Watermarking Techniques for Copyright protection and Content Authentication’, International Journal of Computer Information Systems and Industrial Management Applications(2013), Volume:5, pp. 652–660, ISSN: 2150-7988

[3] Nutzinger,M.C.Fabian, and M.Marschalek. ”Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”. In Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP), 2010 Sixth International Conference.

[4] Abbas Cheddad,Joan Condell,Kevin Curran, Paul Kevitt, ”Enhancing Steganography In Digital Images”. Proc. Canadian Conference on Computer and Robot Vision.

[5] B. Dunbar. A Detailed look at steganographic techniques and their use in an Open-Systems Environment,Sans Institute,1(2002).

[6] Alain,C.Brainos,”A study of Steganography and Art Of Hiding Information,”East Carolina University.

[7] Dipti Kapoor Sarmah, Neha Bajpai.”Proposed System for data hiding using Cryptography and Steganography”. Proc.International Journal of Computer Applications,Vol 9,Isuue2,2010.

[8] Bender,W,Grulh,D,Morimoto,N. & Lu,A.,”Techniques for Data Hiding”,IBM Systems Journal,Vol 35,1996.

[9] Dunbar,B.,”Steganography Techniques and their use in an Open-Systems environment”,SANS Institute,January 2002.

[10] Marvel,L.,M.,Boncelet Jr.,C.G.& Retter,C., ”Spread Spectrum Steganography”, IEEE Transactions on Image Processing,1999.

[11] Wang,H & Wang,S,”Cyber Warfare:Steganography vs. Steganalysis”, Communications of the ACM, 47:10,October 2004.

[12] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking,Artech House, Boston. London,2000.

[13] Jamil,T.,”Steganography:The art of Hiding Information is Plain Sight”,IEEE Potentials,18:01,1999.

[14] Bodhak V. and Gunjal L., “Improved protection in video Steganography using DCT & LSB” international journal of engineering and innovative technology (IJEIT) vol. 1, issue 4, April 2012.

[15] Hussein A. Aly “, Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error” IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.