Optimization of Secure Data for Steganography and Digital Watermarking Scheme

Amit Dubey[1], Neha Tripathi[2]

[1]*Assistant Professor,* [2]*M. Tech. Scholar*

Department of Computer Science and Engineering

OCT, Bhopal

Abstract-Steganography technique plays an important role in information hiding in any digital cover object. Security of information on internet against unauthorized access has become a prime problem. Due to this, steganography technique becomes more popular. Steganography is the science which includes secret communication in an appropriate digital cover objects viz. audio, image, text and video files. The main objective of steganography technique is to hide the presence of the embedded information in carrier file and other objectives are robustness, Un-detectability and capacity of the concealed data. Steganography is separate from other related techniques viz. watermarking and cryptography in term of robustness and Un-detectability of information. Watermarking is a technique that hides information in digital image to protect intellectual properties and copyright, such as logo for proving ownership. Steganography and watermarking are important techniques to conceal important data in cover object an undetectable and irremovable way. Both techniques are the fast developing area of information hiding. This paper delivers a comparative study on digital images steganography and watermarking techniques and significant research growths are also discussed.

Keywords-Steganography, watermarking, Carrier, robustness and information

I. INTRODUCTION

Nowadays multimedia data has been moved expeditiously and broadly to the destinations through the internet into various forms such as image, audio, video and text. In digital communication over the internet, everything is visible and accessible to every user. Therefore, security of information is a necessary and important task. There are three goals of network or information security such as confidentiality, integrity and availability (CIA) [1]. Confidentiality means that information is secure and not available to the unauthorized person. Integrity refers to the accuracy of information and availability means that information is in time access to authorized person. Network security is not sufficient for reliable communication of information like text, audio, video and digital images. There are many techniques to secure images including encryption, watermarking, digital watermarking, reversible watermarking, cryptography, steganography etc. In this paper a review on encryption, steganography and watermarking is presented [2]. In this research study we proposed a hybrid security approach that is a fusion of encryption, steganography and watermarking. A brief introduction of each technique has been discussed in the following sections..

Video based stenographic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, images are transformed to frequency components by using FFT, DCT or DWT and then messages are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the message can be inserted in intensity pixels of the video in LSB positions. The advantage in the method is that the amount of data (payload) that can be embedded is more in LSB techniques. However most of the LSB techniques are prone to attack as described in [5] and [6]. This makes research fraternity interested in designing new methods. Techniques other than LSB substitution also exist in literature and have been discussed in the next section. In this paper a hash based LSB Techniques is proposed in spatial domain. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium.

II. STEGANOGRAPHY

Steganography technique is the art of concealing information imperceptibly in a digital cover medium such as image, audio, and video. The word Steganography derived from the Greek words which mean covered writing in any object [7]. The main objective of steganography is to conceal the existence of the information in the cover medium. Steganography, Cryptography and Watermarking are mostly used to hide the message in image and these techniques are closely related to each other [8]. The strong point of steganography over cryptography is that the hidden messages do not attract attention of third party when it transmitted to the desired recipients because of robustness and undetectably. As observed, during the last several decades, an exponential growth of use of multimedia data over the Internet in the form of Digital Images, Video and Audio files. The rise of digital data on the internet has further enhanced the research work devoted to steganography. The several applications of steganography like secure multimedia watermarking, military communications and fingerprinting applications

for the authentication determination to control the problem of digital piracy. Many steganographic algorithms can be used for these tasks but these are not perfect applications of steganography.

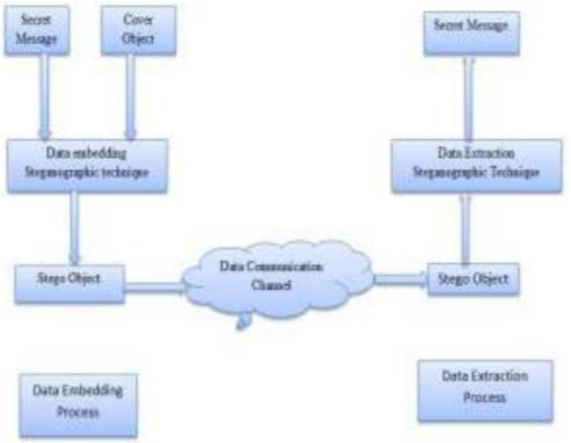

Figure 1: Steganography system

In Steganography, generally some secret data embed into an innocuous looking simple image as a cover image and create a Stego image file. The Stego image visually seems to be same as cover image but hides the secret data inside it and transmitted to the recipients over the communication channels. When the desired recipient receives the Stego image, then follow the data extraction process to recover the secret data.

TYPES OF STEGANOGRAPHY:-

The sender composes a harmless message and after that covers a mystery message on a similar bit of paper. The principle objective of steganography is to impart safely in a totally imperceptible way and to abstain from attracting doubt to the transmission of concealed information. It isn't to shield others from knowing the shrouded data, yet it is to shield others from suspecting that the data even exists. The information can be obvious in fundamental configurations like: Audio, Video, Text and Images and so forth. These types of information are perceptible by human stowing away, and a definitive arrangement was Steganography. The different kinds of steganography include:

Image Steganography: The Image Steganography is method in which we shroud the information in a picture so that there won't be any adjustment in the first picture.

b. Audio Steganography: Sound Steganography can be utilized to shroud the data in a sound document. The sound record ought to be imperceptible.

c. Video Steganography: Video Steganography can be utilized to conceal the data in video records. The video records ought to be imperceptible by the aggressor.

d. Text files Steganography: Text Steganography is used to hide the information in text files. The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text as a source.

III. DIGITAL WATERMARKING

Watermarking system mainly consist of two modules; Watermark embedding, Watermark extraction Watermark embedding and extraction process has a cryptographic key which could be either a public key or a secret key. The key is used for security reasons, which prevent it from unauthorized parties [4]. Cover object is the original image to be watermarked. Watermark is another image use for watermarking on the cover image. Watermarked data is an output data which is obtain by superimposing of original image and watermark image. Embedding process of watermark image is shown in figure 2.

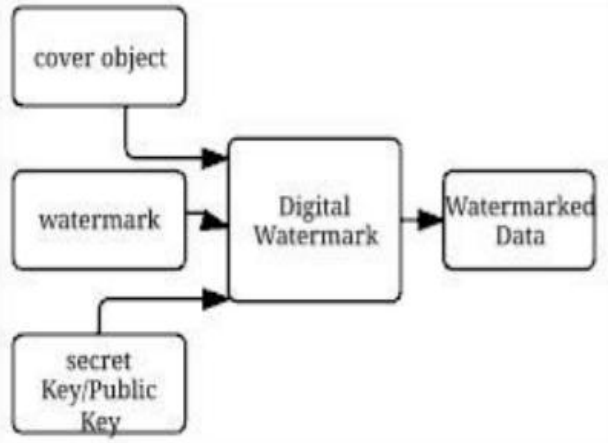

Figure 2: Digital watermarking: Embedding process

Watermark, cover object and secret key or public key are given as the input to watermark embedding process. Either a text or an image can be used as a watermark object. The output data received is the extracted watermark data. Extraction process of digital image watermarking is shown in Figure 3.

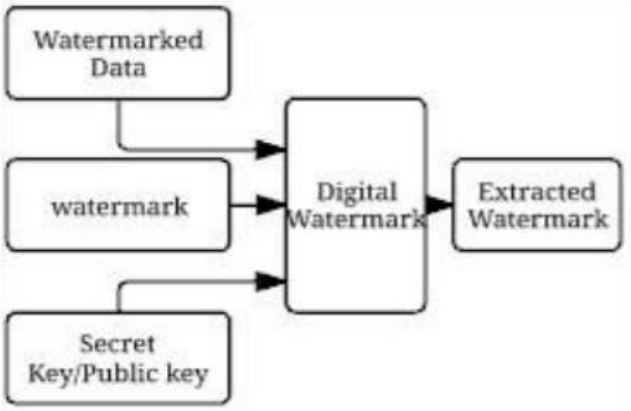

Figure 3: Digital Watermarking: Extraction process

For extraction process Watermark or the original data, the Watermarked data and the secret key or the pubic key are the input data. The output is recovered watermark.

Characteristics of Digital Watermarking:-

Digital watermarking system has following properties.

Robustness: Robustness means the watermark embedded in a data can survive under various attacks and processing operations like rotation, scaling, compression etc. It should be robust against different geometrical and non-geometrical attacks.

Non-perceptibility: Watermark object can neither be seen by a human eye nor be caught by a human ear, it can only be find out through special processing or dedicated circuits. The watermark should be processed in such a way that it does not affect the quality of embedded data.

Security: Only the authorized users can detect, extract and modify the watermark and thus an owner can achieve the purpose of copyright protection.

Payload capacity: The payload limit of watermark portrays greatest measure of information that can be installed as a watermark into an advanced media. The span of the implanted data is frequently essential the same number of frameworks require a major payload to be inserted. As a big payload also provide a security to a digital media.

Verifiability: The watermark should be embedded in such a way that it able to give the full and reliable proof of the ownership of copyright protected information products. It can be used for protecting data from illegal distribution as the data is being protected by the watermark. It is also used for identifying the authenticity.

Fidelity: When we add a watermark into an image there is a large possibility that it will affect the quality of original image. We must keep this property of the image's quality to a minimum, so that the fidelity of an image should be maintained.

Applications of Digital Watermarking:-

Watermarking system can be used in different areas and some of the application of digital watermarking are:

Broadcast Monitoring: The Broadcast monitoring system can protect commercial advertisements and valuable TV products. This application of digital watermark identifies that when and where works are broadcasted by identifying watermark embedded in these works. There are different technologies which can monitor playback of sound recorded during transmission. The digital watermarking is an alternative to these technologies due to its reliable automation detection.

Data Hiding: In digital watermarking data hiding is one of the most common applications. Data hiding is the method in which data is sent secretly in such a way that no unauthorized person can detect it.

Proof of Ownership: To prevent the unauthorized modification of data, the authorized person identification is watermarked into the original data.

Data Authentication: The image can be easily meddled without even being detected. The Watermark like text, signature, and set of words can be embedded into the image to avoid this temper and to maintain the originality. Meddling of image can easily be identified now, as the pixel value of the embedded data would change and does not match with the original pixel values.

IV. COMBINED WATERMARKING AND STEGANOGRAPHY

To protect the authenticity of the document, watermarking can be applied to it. This watermarked document can be embedded in cover image using a stego-key and transmitted over the communication medium. At the receiver end, the information can be first decrypted using the reverse procedure and then it can be validated for its authenticity using the watermarking. This combined approach will satisfy all four goals of data hiding: security, capacity, robustness and perceptibility.

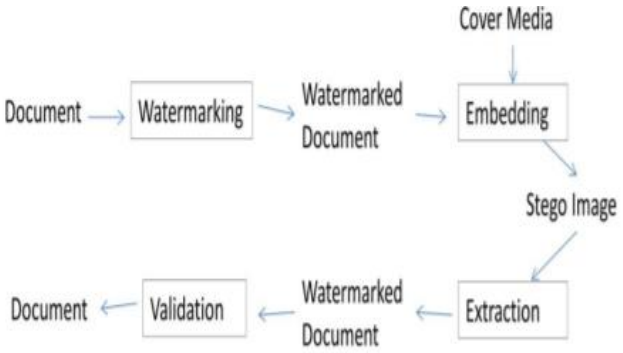

Figure 4: Watermarking with Steganography

Pure steganography – it does not require the exchange of cipher such as a stego-key but the sender and receiver must have access to embedding and extraction algorithm. The cover for this method is c hosen such that it minimizes the changes caused by embedding process. These systems are not very secure as the security depends on the presumption that no other party is aware of this secret message.

Secret key steganography – this method uses a key to embed the secret message into the cover. The key is only known to sender and the receiver and is known prior to communication. Also, the key should be exchanged in a secure medium. The disadvantage of this approach is that it is susceptible to interception.

Public key steganography – it utilizes two keys, open key put away out in the open database and is utilized for installing process and the mystery key is known just to correspondence parties and is utilized to reproduce the first message [8].

V. METHODOLOGY

Cover-Image: A picture in which the mystery data will be covered up. The expression "cover" is utilized to depict the first, pure message, information, sound, still, video and so forth. The cover picture is some of the time called as the "host".

Stego-Image: The medium in which the data is covered up. The "stego" information is the information containing both the cover picture and the "inserted" data. Legitimately, the handling of concealing the mystery data in the cover picture is known as inserting.

Payload: The data which is to be covered. The data to be covered up in the cover information is known as the "inserted" information.

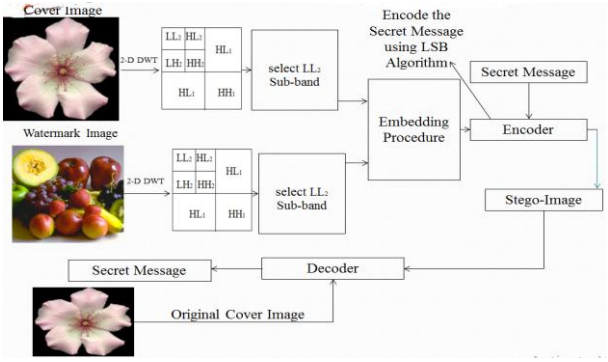

Figure 5; Flow Chart of Methodology

This system works best when the record is longer than the message document and if picture is grayscale.

While applying LSB method to every byte of a 24 bit picture, three bits can be encoded into every pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

$$S(i, j) = C(i, j)-1, \text{ if LSB } (C(i, j)) = 1 \text{ and } SM = 0$$

$$S(i, j) = C(i, j)+1, \text{ if LSB } (C(i, j)) = 0 \text{ and } SM = 1$$

$$S(i, j) = C(i, j), \text{ if LSB } (C(i, j)) = SM$$

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and “SM” id the next message bit to be embedded. S(i, j) is the Stego image.

VI. CONCLUSION

The importance of data hiding techniques comes from the fact the there is no reliability over the medium through which the information is send, in other words the medium is not secured. So, some methods are needed so that it becomes difficult for unintended user to extract the information from the message. The presented a comparative study of steganography and watermarking which are widely used for the confidential data transmission. Generally watermarking used for copyright the image. Combination of two technique steganography and cryptography produce most secure data hiding technique and also enhance the security, security is the main challenge of data over internet.

REFRENCES

[1] N. Senthil Kumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[2] Aase, S.O., Husoy, J.H. and Waldemar, P., A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[3] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[4] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[5] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[6] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.

[7] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp. 86-106.

[8] Baaziz, N., Zheng, D. and Wang, D. (2011) Image quality assessment based on multiple watermarking approach, IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5.

[9] Bao, F., Deng, R., Deing, X. and Yang, Y. (2008) Private Query on Encrypted Data in Multi-User Settings, Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.

[10] Barni, M. and Bartolini, F. (2004) Watermarking systems engineering: Enabling digital assets security and other application, Signal processing and communications series, Marcel Dekker Inc., New York.