International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04| Apr -2016 www.irjet.net p-ISSN: 2395-0072

Literature Review on Different Watermarking & Steganography Technique

SEEMA S. GIRARE[1], MALVIKA U. SARAF[2]

[1]Research scholar, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra,
[2]Assistant Professor, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra,

Abstract- *Now a days most of the people prefer to use internet to send data from one place to another across the world. The fast growth of Internet resulted into a major demand in transferring the information safe and accurate. However the information can be hacked while sending data over the internet. In order to transfer the data to the user at destination without any modifications, there are many techniques available like Cryptography, Watermarking and steganography. In this paper digital Watermarking and steganography technique using Least Significant Bit (LSB) algorithm is proposed to embed the message/logo into the audio file. The objective of this review is to provide a new algorithm for steganography and watermarking .This algorithm has many advantages such as it provide a better background for the use of audio file or image.*

Key words: Steganography, Data Hiding, LSB (Least Significant Bit Algorithm), digital watermarking, Embedding and Retrieving data, software metrics, PSNR.

1. INTRODUCTION

The concept of Digital watermarking mainly came into existence in 1998's .Komatsu and Tominaga was probably the first to use watermarking for hiding some data [1]. "Digital watermarking'' technique is very necessary in the world of internet. Digital watermarking technique is a key solution for avoiding illegal data transfers [2]. Digital Watermarking is the process of embedding an invisible signal (data) into the given signal (data). This invisible signal (data) is called watermark. Watermarking plays an important role in protection of copyright ownership of electronics data.

Digital watermarking embed a covert stream of bit in a file and this file could be an audio file, image file, video file or text file. Digital watermarking can also be a form steganography in which data is obscured in the message without other end user's knowledge. Generally, data hidden can be hide using three important techniques such as steganography, cryptography, watermarking as shown in figure 1.The main purpose of steganography is to communicate in a completely indiscernible manner. Steganography is acts as a science which deals with hidden information. This technique provide better security system because the watermark cannot be copied and scanned effectively. The aim of steganography is to embedded message in audio or image file, to obtained newly data d', practically it is hidden data from people, and so that hackers cannot detect the information in newly data d'.

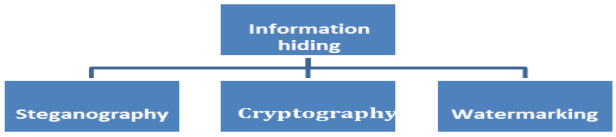


Fig -1: Classification of information hiding

The aim of steganography method is to embed a message in one-to-one communication only and the goal of watermarking is to embed message in one-to-many communications. The steganography and watermarking method have number of applications which widely helps in security system like watermark is very helpful in the examination of paper and also determining the quality of a sheet of paper. In this paper we also reviewed the previous work which had been done on digital watermarking using LSB technique and various watermarking method.

1.1 Research Objectives

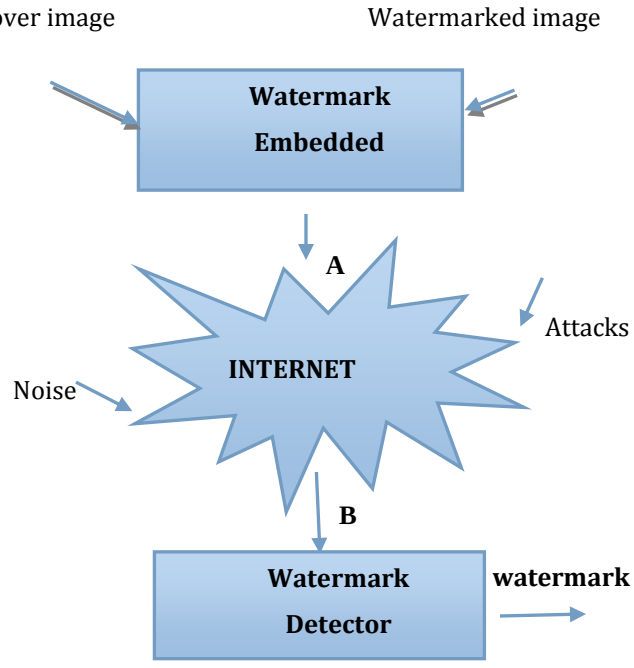
Generally two important techniques are used to hide the data and those are steganography and digital watermarking. As per the research, data hidden techniques have some limitations, the robustness of the watermark techniques and the size of the hidden data. The objectives of this research are as follows:

- To investigate the method in which the embedded watermark should protect the data from hackers using common signal processing operations and attacks.

- The second requirement is to identify the software for better audio watermarking and also find out the various methods for data security.
- To investigate the technique for high capacity rate of hiding data, robustness and imperceptibility.
- To evaluate the type of audio file that can be used to communicate securely in a complete indiscernible manner and avoid the suspicion of transmission of cryptic information.
- To carry out review of different watermarking techniques and illustrate the advantage of each method.

2. BLOCK DIAGRAM OF DIGITAL WATERMARKING TECHNIQUE

In digital watermarking data or message code can be encoded into digitized music, video, picture and audio. The main purpose of Digital watermarking is to provide protection against illegal data transmission. Watermarking consist of two types: visible watermark and invisible watermark. The information which is visible in the form of text or logo on the image, picture or videos is known as visible watermarking.



A-Watermark image ,B-Noisy Watermark image

Fig -2: Process of Digital watermarking

The working of digital watermarking begins when the encoder embeds watermark into image and thus produces watermarked image. The example of watermarking is Famous artists watermark their images or picture and if someone tries to copy the picture or image then the watermark is also copied along with the image. In invisible watermarking the detection is not easy because it is not visible or perceivable, so it is a better way of sending secret data. In the process of digital watermarking at input side the watermark is inserted in main image known as cover image because it also covers the watermark as shown in figure 2.Digital watermarking embed the data or logo into other image in an undetectable way [15]. There are various application of Digital watermarking such as owner identification, proof of ownership, data security and broadcast monitoring.

2.1 Types of Watermarking Techniques

The four categories of watermarking techniques are as follows [5]:

A) According to types of Document: They are classified into four ways [9].

• Image watermarking**:** In this technique the necessary data is embedded into image such that invisible message will attract attention of other users**.**

•Text watermarking**:** This technique only work on PDF**,** DOC and text file etc.

•Audio watermarking**:** In this watermarking the watermark is embedded only in audio file such as on internet music, MP3 etc.

•Video watermarking**:** In this watermarking the main Algorithms used for video watermarking are DFT, DCT and DWT.Video watermarking insert watermarks in a video sequence so that it will protect the video from illegal copying.

B) According to Robustness: They are classified into three ways.

• Robust: This type of watermark mainly used in copyright application. For example: Robust Private Spatial Watermarks .It is called robust if it resists selected class of transformations.

•**Fragile:** If it fails to detect after the slightest modification then this watermark is called as fragile and it is used for tamper detection.

•Semi fragile: This type of watermarking mainly used to detect malignant transformation and Blind Semi-fragile Spatial Watermarks.

C) From application point of view: They are classified into two ways.

•Source based: This watermark required to verify the identity of ownership where the owner hide a unique data/logo to the all copies which are to be distributed.

•Destination based. The main advantage of this watermark is if there is illegal reselling of copy then it will trace the buyer easily. In destination based watermark every distributed copy has a unique watermark for identifying the buyer.

D) According to working domain:

•Spatial domain: In spatial domain, watermarking can be applied by using color separation, however the watermark obtains in only one of the color bands. The algorithms which are used in above techniques are LSB, SSM Modulation [9][10].

•Frequency Domain: This technique consists of Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), in this domain watermark due to behavior of the human visual system (HVS) are good captured by the spectral coefficients [11].

2.2 Attacks on Digital Watermarking

The various possible intentional and unintentional Attacks on digital watermarking are as follows:

Watermark Attacks:

A) Active Attacks- Hacker attempts to destroy the watermark. This attacks aim for complete removal of watermarking but sometime can happen unintentionally.

B) Passive Attacks-The aim of Hacker is only to find out whether watermark is present or not and removal of watermark is not an aim of hacker. It does not actually remove the embedded watermark.

C) Forgery Attacks-In forgery attacks the hackers tries to insert a valid watermark and find a way to remove the embedded watermark data.

3. LEAST SIGNIFICANT BIT

This technique is mainly used for simple operation to insert data in image, audio or video file [6]. There are some algorithms available for digital watermarking but the simplest algorithm is Least Significant Bit (LSB) Insertion [14]. Least Significant Bit (LSB) is very simple to understand and also easy to implement. This method is based on modifications of the pixel value's (LSB).LSB technique has some advantages such as high perceptual transparency, low degradation of image quality, less distortion or noise., requires less computations, variation in choosing LSB etc. The most common technique used in steganography are least significant bit embedding, filtering, inserting. In LSB technique chose the number of bits which we want to hide in secret message.

4. STEGANOGRAPHY:

Steganography is obtained from Greek word Steganos' 'which means cryptic information and graphy means some writing or drawing [12]. Steganography is a form of science that deals with hidden messages. There are various methods are available to achieve steganography. Steganography are widely used for embedding secret data in text file, audio file and for secure communication. The main applications of Steganography are it has been used by intelligence services and also in modern printers.

4.1 Types of steganography

The steganography system is used to embed the data in an invisible manner.

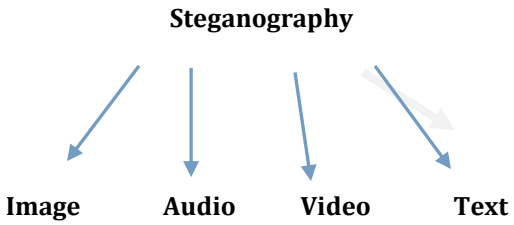


Fig -3: Types of Steganography

A.Image Steganography:

In this technique we can embed information in an image and there will not be any change in the input image.

b. Audio Steganography:

Audio Steganography can be used to embed the data in an audio file. The audio file should be indiscernible.

c. Video Steganography:

Video Steganography can be used to embed the message in video files.

d. Text files Steganography:

In this technique data is hide in text files and it is very simple method. [8]

5. REVIEW OF RELATED WORK

This literature review describes different watermark techniques used for images/audio. It present the previous work which had done on digital watermarks using LSB, including the analysis of various watermarking schemes and their results.

1] **Abdullah Bamatraf, Rosziati Abrahim and Mohd. Najib B. Mohd Salleh (2014)**

Abdullah Bamatraf, Rosziati Abrahim and Mohd. Najib B. Mohd Salleh et al [13] presented a simple and robust watermarking algorithm by using the 3rd and the 4th bit of least significant bits (LSB) technique. The proposed algorithm is more robust to hide the data in image. Figure 2 shows the framework of the proposed method. Using the proposed algorithm, two bits in the third and fourth LSB is embedded.

Advantage: Their proposed system hide the data in the image in the bit of LSB to determine coordinates, the system provide watermarked image without noticeable distortion on it and the quality of the watermarked image must be high always.

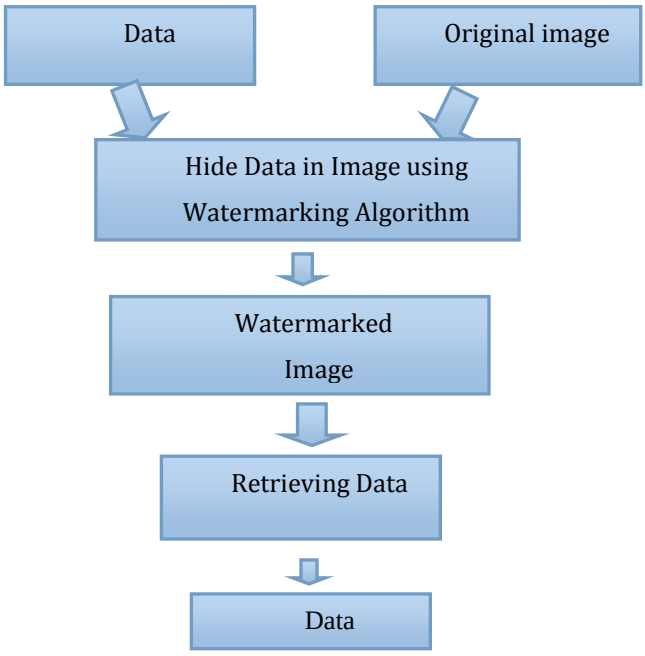


Fig -4: Proposed system frame work

[2] Puneet Kr Sharma and Rajni (2012)

Puneet Kr Sharma and Rajni et al [3] describe a method of image watermarking and evaluates LSB based watermarking method with different substitution of bit from least significant bit to most significant bit in image. After that secret data is embedded in the first bit i.e. LSB in the image and provide Watermarked Image without noticeable distortion on it. However when the data is embedded in the consequent bits the image gets distorted.

Advantage: This proposed system provide an efficient method for hiding data which provide more noise free images and the watermark (logo) was recovered perfectly and also the PSNR and MSE values are calculated.

[3] Rajni Goyal and Naresh Kumar (2014)

According to Rajni Goyal, Naresh Kumar et al [4] present the LSB watermarking technique for embedding textual information in image and also calculate the PSNR value of the given image.

Advantage*:* This proposed system provide a better security and better PSNR values.

[4] **R Sridevi, DR. A Damodaram and DR. svl.Narasimham**

According to R Sridevi, dr. a Damodaram and dr. svl.Narasimham et al [15] gives a brief idea to provide a better method for hiding the data and sent to the receiver in a safer manner.

Advantage: This proposed system is to provide a better method for embedding the data in a secret way to the output. This system will not change the original size of the input file even after inserting the data and it is also suitable for any type of audio file format.

[5] K.P.Adhiya and Swati A. Patil

According to K.P.Adhiya and Swati A. Patil propose a steganography technique to put information in audio file. In this techniques each bit of audio sample is converted into bits and then the textual information is inserted in it. The fourth last binary bit is taken into an account and also applying redundancy of the binary bit 1 or 0 used.

Advantage: 8 bitWAV and 16bitWAVaudio file are supported and the secret message can be hidden in the audio file and required less storage capacity.

[6] Manisha Rana, Rohit Tanwar (2014)

According to Manisha Rana, Rohit Tanwar et al [7] propose a steganography method for hiding text in audio file. In this paper the use of GA in Steganography is used to increase the robustness of techniques.

Advantage: To increase the Robustness GA can be used in substitution techniques while maintaining the significant data hiding capacity.

6. CONCLUSION

In previous paper the work had been done on digital watermarks which embedded the secret data in image. Now, this paper proposes a digital watermarking and steganography method using LSB algorithm for hiding text in audio such that information can reach at receiver in a safe manner without modifying the original image and the receiver extract data assigned to him. The main goal of this paper is to review digital watermarking technique, its application and different type of attacks on watermarking. Audio steganography is a new branch of this discipline. The Audio files are always larger in size than the images file is the main advantage of this technique . From the above discussion of this paper it is concluded that LSB method provides more security than other DCT or DFT techniques. We are going to use an encoding mechanism for hiding the data into the audio file.

ACKNOWLEDGMENT

The author is thankful to Professor Malvika U.Saraf, faculty of Electronics /Electronics and telecommunication for providing necessary guidance to prepare this paper.

REFERENCES

[1]Bender, W., Gruhl, D., Morimoto, N. and Lu, A (1996).: Techniques for data hiding. IBM Systems Journal, vol. 35, nos. 3&4.

[2] I.J. Cox, M.L. Miller, J.A. Bloom, Digital watermarking, Morgan Kaufmann, 2001.

[3] Puneet Kr Sharma and Rajni "analysis of Image Watermarking using least significant bit algorithm", International Journal of Information Sciences and Techniques (IJIST), Vol.2, No.4, July 2012.

[4] Rajni Goyal1, Naresh Kumar2" LSB Based Digital Watermarking Technique", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 9, September 2014.

[5] N. Cvejic, T. Seppanen "Algorithms for Audio Watermarking and Steganography", PHD thesis, Oulu University of technology, June 2004

[6] Methods of Audio Steganography, Internet publication on www.Snotmonkey.com.

[7] Manisha Rana, Rohit Tanwar, 'Genetic Algorithm in Audio Steganography", International Journal of Engineering Trends and Technology (IJETT) – Volume 13 Number 1 – Jul 2014.

[8] Stuti Goel,Arun Rana,Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography" IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) , Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48 www.iosrjournals.org

[9] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", Proceedings of International Journal of Engineering and Innovative Technology (IJEIT), March 2013Volume 2, Issue 9.

[10]Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection", Proceedings of International Conference on Intelligent Computation Technology and Automation, 2010.

[11]Manpreet Kaur, Sonia Jindal, Sunny behal, " A Study of Digital image watermarking" , Proceedings of Volume2, Issue 2, Feb 2012.

[12] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[13] Abdullah Bamatraf, Rosziati Ibrahim Mohd. Najib B. Mohd Salleh" Digital Watermarking Algorithm Using LSB"International Conference on Computer Application and Industrial Electronics (ICCAIE), December 5-7, 2014 kualu Lumpur, Malaysia.

[14] Frank Hartung, Martin Kutter (July 1999), "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1085 – 1103.

[15] R Sridevi, Dr. A Damodaram, Dr. Svl.Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced", Journal of Theoretical and Applied Information Technology.

BIOGRAPHIES

Seema S.Girare is a M.tech students of Electronics branch at Wainganga college of Engineering and Management, Nagpur, Maharashtra, India. She completed B.E in Electronics and Telecommunication branch from G.H. Raisoni Institute of Engineering and Technology for Women, from Rashtrasant Tukadoji Maharaj Nagpur University, Maharashtra in 2014. She completed diploma in Electronics and Telecommunication (ETC) from G.H. Raisoni Polytechnic in 2011. Her areas of interest are communication, Digital Design and image processing.

Malvika U.Saraf is the Head of Electronics/Electronics and Telecommunication at Wainganga college of Engineering and Management, Nagpur, Maharashtra, India.She completed M.tech from G.H. Raisoni Institute of Engineering and Technology for Women, from Rashtrasant Tukadoji Maharaj Nagpur University, Maharashtra. She has an experience of about 6 year in teaching field .She has 2 year of industrial experience. Her areas of interest are digital image processing, Digital Design.