International Journal of Trend in Research and Development, Volume 3(3), ISSN: 2394-9333
www.ijtrd.com

Image Watermarking Using Least Significant Bit (LSB) Algorithm

[1]Ms. Patil V. A. and [2]Ms. S. S. Tamboli,
[1,2]Assistant Professor, Department of Electronics & Telecommunication Engineering,
Annasaheb Dange College of Engineering & Technology, Ashta, Maharashtra, India

Abstract-- The rapid advancement of internet has made it easier to send the data/image accurate and faster to the destination. But this advantage is also accompanied with the disadvantage of modifying and misusing the valuable information through intercepting or hacking. So In order to transfer the data/image to the intended user at destination without any alterations or modifications, there are many approaches like Cryptography, Watermarking and Steganography. This paper presents the general overview of image watermarking and different security issues. In this paper, Image Watermarking using Least Significant Bit (LSB) algorithm has been used for embedding the message/logo into the image. This work has been implemented through MATLAB.

Keywords-- *Least Significant Bit (LSB), Digital Watermarking, Peak Signal to Noise Ratio (PSNR)*

I. INTRODUCTION

Privacy is the ability of an individual or group to insulate them or information about themselves and thereby reveal them selectively [1]. Data privacy is the relationship between collection and dissemination of data, technology, the public anticipation of privacy, and the legal issues [2]. Data privacy or data protection has become increasingly important as more and more systems are connected to the internet [2]. In order to circumvent the problem of the security attacks in data transfers over the internet, many techniques have been developed like: Cryptography, Stegnography and Digital Image Watermarking.

The concept of Image watermarking mainly came into existence in 1990s because of the widespread of the Internet. At that time an invisible watermark message was inserted into a image which is to be transfered such that the invisible message will survive intended or unintended attacks. The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying music works. In year 1988, Komatsu and Tominaga was probably the first to use the term "digital watermarking" [1]. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. The information/logo are embedded in image is called a digital image watermark. The information/logo where the watermark is to be embedded is called the host image [2, 3].Watermarking is a pattern of bits inserted into a digital image, audio or video file that specifies the file's copyright information such author, rights and so on [3]. Thus, watermarking approach is used to make sure of the protection of the data. However, watermarking is also designed to be completely invisible. The actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and tampered [4]. Thus, the watermarking must be robust enough so that it can withstand normal changes to the file such as attacking by adding noise [5].

Contrast to printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that is completely invisible [6]. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data [7]. Media watermarking research is a very active area and digital image watermarking became an interesting protection measure and got the attention of many researchers since the early 1990s [8].

Digital image watermarking technique provides perceptibility. A watermarking system is of no importance to anyone if it degrades or distract the cover image to the extent that it being useless, or highly distracting to its intended user. An ideal watermarked imaged should appear indistinguishable from the original image even if one uses highest quality equipment. The ideal watermark must be highly robust so as to be highly resistant to any distortion that can be introduced during normal use (unintentional attack), or a deliberate effort to remove or alter the watermark present in the data/image being transferred (intentional attack). Integrity and Security are also two essential requirements of ideal watermarking [4, 5]. A robust watermark is one which can withstand a wide variety of attacks both incidental and malicious.

The rest of this paper is organized as follows: Section 2 describes classification while section 3 briefs the techniques of watermarking. Watermarking process is described in section 4. Section 5 describes least significant bit technique in detail. Results and conclusion is given in Section 6 and 7 respectively.

A. Classification of Watermarking

Digital Watermarking techniques can be classified as:

1. Text Watermarking
2. Image Watermarking
3. Audio Watermarking
4. Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

1. Visible watermark
2. Invisible-Robust watermark
3. Invisible-Fragile watermark

B. Techniques of Watermarking

a. Frequency Domain Watermarking

These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture.[11]

b. Spread Spectrum

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [10].

c. Spatial Domain Techniques

Techniques in spatial domain class generally share the following characteristics:

1. The watermark is applied in the pixel domain.
2. No transforms are applied to the host signal during watermark embedding.
3. Combination with the host signal is based on simple operations, in the pixel domain.
4. The watermark can be detected by correlating the expected pattern with the received signal.

Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame. Let us denote a picture to be watermarked by P and values of its pixel color samples by Pi , a watermarked version of picture P by P * and values of its pixel color samples by P * i . Let us have as many elements of watermark W with values Wi as number of pixels in picture P. Watermark W hereby covers the whole picture P. Further, it is possible to increase the watermark strength by multiplying watermark element values by weight factor a. Then the natural Formula for Embedding Watermark W into Picture P Is:

P*i = P i +aWi .

The most common algorithm using spatial domain watermarking is LSB.

d. Process of Watermarking

The process of watermarking begins when the encoder inserts watermark into image, producing watermarked image. The decoder extracts and validates the presence of watermarked input or unmarked input. If the watermark is visible, the decoder is not needed. Otherwise, the decoder may or may not require a copy of decoder to do this job. If input image and/or watermarked image are used, the watermarking system is called a private or restricted-key system; otherwise, the system is public or unrestricted-key system.

The decoder is so designed to process both marked as well as unmarked image. Finally, the decoder needs to correlate the extracted watermark with original image and compare the result to a predefined threshold that sets the degree of similarity accepted as a match. If the correlation matches the threshold value, then watermark is detected i.e. original image belong to the user otherwise the data does not belong to the user [8, 9].

Digital image watermarking is similar to the concept of watermarking physical objects with the difference that the watermarking technique is used for digital content instead of physical objects. In digital image watermarking a secret information or logo is embedded in another image in an impercitible manner. This secret information or logo is called watermark and it contains some metadata, like security or copyright information about the main data/image. The main image in which the watermark is embedded is known as cover image since it covers the watermark. The digital image watermarking system essentially consists of a watermark embedder and a watermark detector as shown in figure 1.

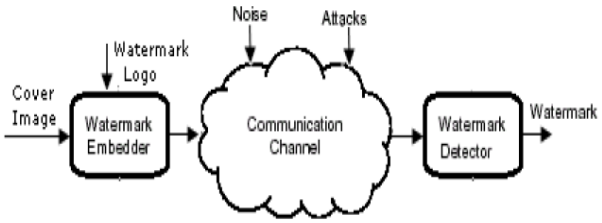

Figure 1: Digital Image watermarking

The watermark embedded inserts a watermark onto the cover image and the watermark detector detects the presence of watermark information/logo. Sometime a watermark key is also used during the process of embedding and detecting watermarks. The watermark key has a one-to-one relation with watermark information. The watermark key is private and known to only intended users and it ensures that only desirable set of users can detect the watermark.

II. Least Significant Bit Modification

There are many algorithms available for invisible digital watermarking2 3. The simplest algorithm is Least Significant Bit (LSB) Insertion, 4in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. [9]Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times.[9].In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image .Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications.

III. RESULTS

Figure 2: Original and watermark image

Figure 3: Watermarked image and recovered watermark

CONCLUSION

This paper investigates the classification and methods of image watermarking and evaluates LSB based digital watermarking scheme. After we have embedded the secret data in the first bit i.e. LSB in the image we got Watermarked Image without noticeable distortion on it. However when we embed the data in the consequent bits i.e. second towards last MSB bit, the image start distorted.

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] Saraju Prasad Mohanty (January 1999) "Watermarking of Digital Images", Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012

[3] Katzenbeisser, S. and Petitcolas, F(1999).: Information hiding techniques for steganography and digital watermarking. Artech House Books.

[4] Van Dijk, M. and Willems, F(May 15-16, 2001).: Embedding information in grayscale images. Proc. 22 nd Symposium on Information and Communication Theory in the Benelux, pp. 147-154, Enschede, the Netherlands.

[5] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi(Oct. 2001), "A survey on watermarking application scenarios and related attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993.

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

[7] Brigitte Jellinek(Jan 2000), "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17.

[8] K. Watermarking digital Image and video data. *IEEE Signal Processing Magazine*, 17:20–46, 2000

[9] C. Rey and J.L. Dugelay(2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing*, 6:613–621.

[10] Avani Bhatia, Mrs. Raj Kumari"Digital Watermarking Techniques".

[11] Chiou- Ting Hsu; Ja-Ling Wu; Consumer Electronics "DCT-based watermarking for video", IEEE Transactions on Volume 44, Issue 1, Feb. 1998 Page(s):206 – 216