

ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM

Puneet Kr Sharma¹ and Rajni²

¹ Research Scholar, Deptt. of ECE, SBSCET, Ferozpur
puneet22.1981@rediffmail.com

² Assistant Professor, Deptt. of ECE, SBSCET, Ferozpur
rajni_c123@yahoo.co.in

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), JPEG (Joint Photographic Experts Group), MPEG (Moving Picture Experts Group), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR)

1. INTRODUCTION

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 transferred 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].

Digital image watermarking technique provides **perceptibility**. A watermarking system is of no importance to anyone if it degrades or distracts the cover image to the extent that it being useless, or highly distracting to its intended user. An ideal watermarked image 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 (Means modifications applied with a

purpose other than to hamper the watermark) and malicious (attacks aimed typically to remove or weaken the watermark) [6].

In the current trends of the world, due to the advancement in technologies, most of the individuals prefer to use the internet as the primary medium to transfer data from one end to another across the world. The data transmission is made very simple, fast and accurate using the internet. However, security threat is the main issue while sending data over the internet. The private/confidential data can be hacked in many ways. Therefore it becomes mandatory to take data security into consideration. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data alteration. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet [1, 2]. Information security consists of the measures adopted to prevent the unauthorized use or change of data or capabilities [3, 4]. Information security is the protection of information, system and hardware that use, store, and transmits this information. The data is transmitted from source to destination to the intended user but the hackers might hack the same data in order to access or manipulate the original data. These types of attacks are formally known as Security Attacks. In order to circumvent the problem of the security attacks in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and Digital Image Watermarking.

Digital Image Watermarking is one of the prominent method to fulfill the gap between copyright issues and digital distribution of data. It is mainly based on Steganographic techniques and enables useful safety mechanisms. It acts as a very good medium for copyright issues as it embeds a symbol or a logo in the form of a Watermark, which cannot be altered manually. One critical factor, which is to be kept in mind while using Watermarking, is to avert any alterations to the originality of the image after embedding the data. When the image with the secret data is transmitted over the internet, unauthorized parties may want to hack the data hidden over the image or change it. If the originality of the image has been altered, then it will be easier to hack the information by unauthorized persons. In order to improve the security, the Digital Watermarks are predominantly inserted as transformed digital signal into the source data using key based embedding algorithm and pseudo noise pattern. The best known Watermarking method that works in the spatial domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information.

2. 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 imperceptible 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 1.1.



Figure 1.1 Digital Image Watermarking

The watermark embedder 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. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital image watermarking techniques should be resilient to both noise and security attacks [7].

3. Least Significant Bit Modification

The most common method of watermark embedding is to embed the watermark into the least-significant-bits of the cover object [6]. Despite being a simple method, LSB substitution suffers from many drawbacks. Although it can survive transformations like cropping, any addition of undesirable noise or lossy compression but a more sophisticated attack that could simply set the LSB bits of each pixel to one can fully defeat the Watermark with negligible impact on the cover object. Once the algorithm is known to a hacker, the embedded watermark could be easily modified by him without any difficulty.

A more sophisticated approach over conventional LSB method would be to use a pseudo-random number generator which determine the pixels to be used for embedding watermark based on a given key [6]. Security of the watermark would be enhanced greatly as the Watermark could now be no longer is easily viewable to the hackers or any other unintended user. Although this algorithm is still vulnerable to replacing the LSB's with a constant value.

4. Results

The result shown below are of the large watermark embedded into a original image using LSB embedding algorithm, which uses the logo as watermark and spreads it out to full image size. Results from LSB substitution closely match with the expected one. The watermarked image shows slight but unnoticeable degradation, while the watermark (logo) was recovered perfectly. In this method consider the binary value of an image pixel as

```
00100111    11101001    11001000    00100111    11001000    11101001
11001000    00100111
```

We will hide a binary value for say 10000011 by changing only the LSB of the above mentioned image pixel value. The result will be as following

```
00100111    11101000    11001000    00100110    11001000    11101000
11001001    00100111
```

In this way a watermark is being embedded in the image data by changing only the LSB of the image data. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error measurement methods which are used to compare image compression quality. This ratio is used as a quality measurement benchmark between the original and a compressed image. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower will be the error. To compute the PSNR, the mean-squared error is first calculated using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m, n) - I_2(m, n)]^2}{M * N}$$

Where M and N are the number of rows and columns in the input images, respectively and $I_1(m, n)$ is the original image, $I_2(m, n)$ is the Watermarked image. The PSNR is calculated using the following equation:

$$PSNR = 10 \log_{10} \left[\frac{R^2}{MSE} \right]$$

Where R represents maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number.

TABLE 1. PSNR & MSE for Different Bit Substitution

Method	PSNR	MSE
LSB or 1st Bit Substitution	55.8784	0.1680
2 nd Bit Substitution	49.7986	0.6811
3 rd Bit Substitution	43.9396	2.6249
4 th Bit Substitution	37.8535	10.6593
5 th Bit Substitution	31.9717	41.2961
6 th Bit Substitution	26.0475	161.5588
7 th Bit Substitution	19.8117	679.0598
MSB or 8 th Bit Substitution	14.3467	2.3900e+003

Logo to hide



Figure1. Logo to be embedded in image

Watermarked Image with LSB



Figure.2. Watermarked Image with LSB

Watermarked Image 2nd bit substitution



Figure.3. Watermarked Image 2nd bit substitution

Watermarked Image 3rd bit substitution



Figure.4. Watermarked Image 3rd bit substitution

Watermarked Image 4th bit substitution



Figure.5. Watermarked Image 4th bit substitution

Watermarked Image 5th bit substitution



Figure.6. Watermarked Image 5th bit substitution

Watermarked Image 6th bit substitution



Figure.7. Watermarked Image 6th bit substitution

Watermarked Image 7th bit substitution



Figure.8. Watermarked Image 7th bit substitution

Watermarked Image 8th bit (MSB) substitution



Figure.9. Watermarked Image 8th bit substitution

Recovered logo/Watermark

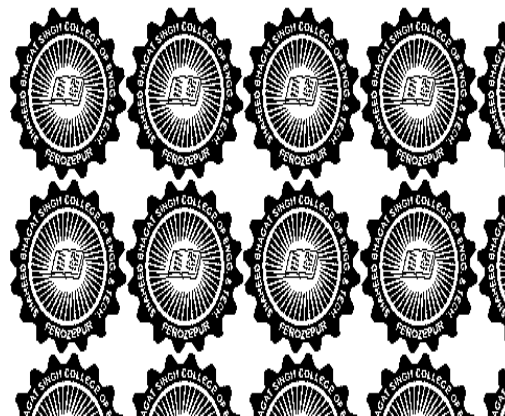


Figure.10. Recovered logo/ Watermark

6. CONCLUSIONS

This paper investigates the classification, attacks and methods of image watermarking and evaluates LSB based digital watermarking scheme with different bit substitution from LSB to MSB in image. 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. The PSNR and MSE values are calculated and shown in Table1.

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.,

- [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. 22nd 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.

Authors

Mrs. Rajni is currently Assistant Professor at SBS College of Engineering and Technology, Punjab, India. She has been pursuing PhD from SLIET, Longowal. She has completed her M.E. from NITTTR, Chandigarh, India, B.Tech. from NIT, Kurukshetra, India. She has about fourteen years of academic experience and two years industrial experience. Her areas of interest includes Wireless communication, Antenna design.

Mr. Puneet Sharma is student at SBS College of Engineering and Technology, Punjab. He has done M.B.A from G.J.U, Hissar ,Haryana ,B.tech from P.T.U, Jalandhar,India. He has about nine years of academic experience and two years of industrial experience. His area of interest includes Image processing. Digital design.