INFORMATION SECURITY THROUGH IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM

Puneet Kr Sharma[1] and Rajni[2]

[1]Research Scholar, Deptt. of ECE, SBSCET, Ferozepur
puneet22.1981@rediffmail.com
[2]Assistant Professor, Deptt. of ECE, SBSCET, Ferozepur
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. Besides this, it is easier to modify and misuse the valuable information through hacking at the same time. In order to transfer the data/image securely to the destination without any 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

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 but the hackers might hack the network in order to access or modify 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, Stegnography and Digital Image Watermarking.

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 61–67, 2012.
 DOI : 10.5121/csit.2012.2208

Digital Image Watermarking is described as one of the promising way to close 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. This method has several implementation versions that improve the algorithm in certain aspects.

2. Watermarking Attacks

A robust watermark should survive a wide variety of attacks both incidental (Means modifications applied with a purpose other than to destroy the watermark) and malicious (attacks designed specifically to remove or weaken the watermark) [5, 6]. These watermark attacks can be categorized as follows:

Simple attacks: Simple or waveform or noise attacks are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. Examples include filtering, compression attempts like JPEG and MPEG, and addition of noise, addition of an offset, cropping, Digital to analog and analog to digital conversion.

Detection-disabling attacks: Detection-disabling or synch-ronization attacks are attacks that attempt to break the correlation and to make the recovery of the watermark impossible or infeasible for a watermark detector, mostly by geometric distortion like zooming, shift in (for video) direction, rotation, cropping, pixel permutations, sub-sampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.

Ambiguity attacks: Ambiguity or deadlock attacks are attacks that attempt to confuse by producing fake original data or fake watermarked data. An example is an inversion attack that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear which the first, authoritative watermark was.

Removal attacks: Removal attacks are attacks that attempt to analyze the watermarked data, estimate the Watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Examples are collusion attacks, de-noising, certain filter operations, or compression attacks using synthetic modeling of the image [7].

3. 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 must process both marked and 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].

4. Least Significant Bit Modification

The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [6]. Despite of its simplicity, LSB substitution suffers from many drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the Watermark. An even better attack would be to simply set the LSB bits of each pixel to one, fully defeating the Watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key[6]. Security of the watermark would be improved as the Watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant.

5. Results

The result shown below is the large watermark created for the LSB embedding algorithm, which uses the normal watermark and titles it out to full image size. Results from LSB substitution closely match with the expected one. The watermarked image shows little not noticeable degradation, while the large watermark 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 metrics used to compare image compression quality. This ratio is often used as a quality measurement 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 Subsitution

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

Figure1.Logo to be embedded in image

Figure.2.Watermarked Image with LSB

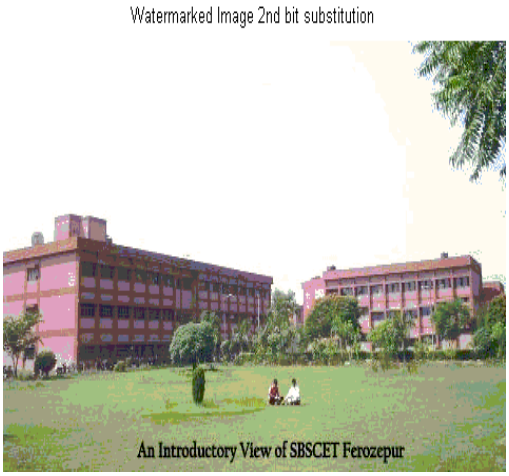

Figure.3.Watermarked Image 2nd bit substitution

Figure.4.Watermarked Image 3rd bit substitution

Figure.5.Watermarked Image 4th bit substitution

Figure.6.Watermarked Image 5th bit substitution

Figure.7.Watermarked Image 6th bit substitution

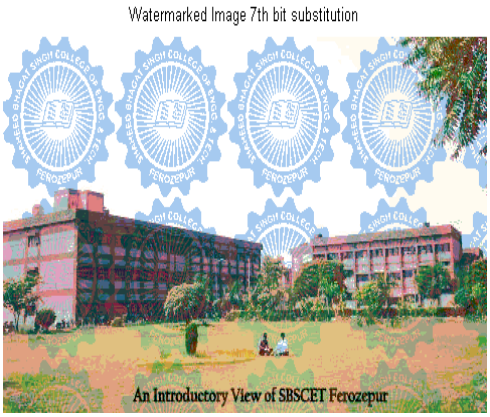

Figure.8.Watermarked Image 7th bit substitution

Figure.9.Watermarked Image 8th bit substitution

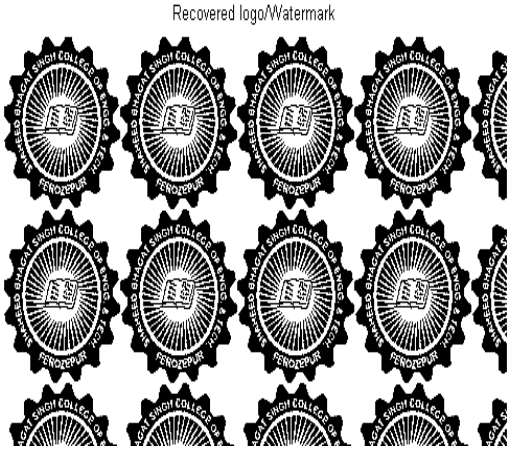

Figure.10. Recovered logo/ Watermark

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 persuing 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 teaching experience and two years of industrial experience. His area of interest includes Image processing. Digital design.