Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image Watermarking Using LSB (Least Significant Bit)

Gurpreet Kaur*
M.Tech(Computer Science)
Shri Guru Granth Sahib World Univeristy, India.

Kamaljeet Kaur
Assistant Professor(Computer Science)
Shri Guru Granth Sahib World Univeristy, India.

Abstract: With the rapid development and wide use of Internet, information transmission faces a big challenge of security. People need a safe and secured way to transmit information. Digital watermarking is a technique of data hiding, which provide security of data. This paper presents a watermarking technique which least significant bits (LSB), its steps and its process with matlab images.

Keywords: Watermarking, spatial domain, Frequency domain, Spread spectrum, LSB

I. INTRODUCTION

Watermarking is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work [10,2]. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. Digital watermarking involves embedding a structure in a host signal to "mark" its ownership [12]. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party [8]. While some watermarks are visible [5], most watermarks are invisible. [11].

II. CLASSIFICATION OF WATERMARKING

Digital Watermarking techniques can be classified as:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

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

I. Visible watermark
II. Invisible-Robust watermark
III. Invisible-Fragile watermark

III. 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.[4]

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 [1].

C. Spatial Domain Techniques

Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.
- 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.

IV. LEAST SIGNIFICANT BIT

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.

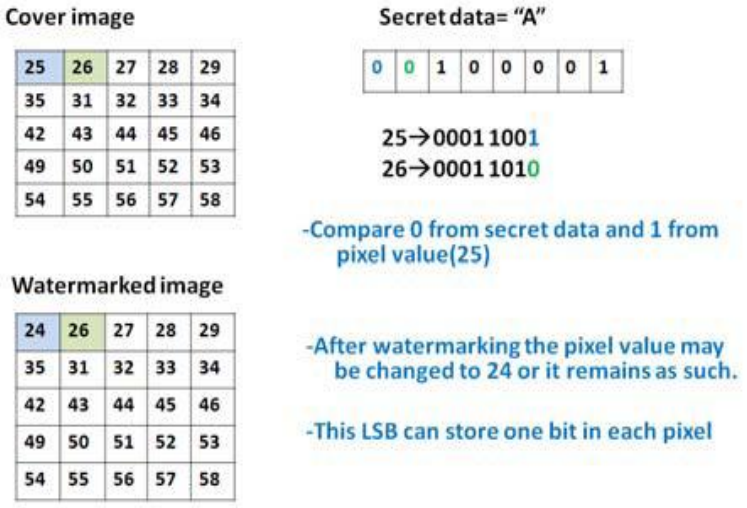

Figure 1 An example of 1 bit LSB[11]

The algorithm proposed by Kurah and McHughes [7] to embed in the LSB and it was known as image downgrading [13]. An example of the less predictable or less perceptible is Least Significant Bit insertion. This section explains how this works for an 8-bit grayscale image and the possible effects of altering such an image. The principle of embedding is fairly simple and effective. If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures [7].For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel. [11].

Features of LSB (Least-Significant-Bit)

a. It is simple to understand
b. Easy to implement
c. It results in stego-images that contain hidden data yet appear to be of high visual fidelity.[3]

V. STEPS OF LEAST SIGNIFICANT BIT

1) Convert RGB image to gray scale image.
2) Make double precision for image.
3) Shift most significant bits to low significant bits of watermark image.
4) Make least significant bits of host image to zero
5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

VI. PROCESS OF LSB

A. Remove Noise

First we use DWT and other techniques to remove the noise

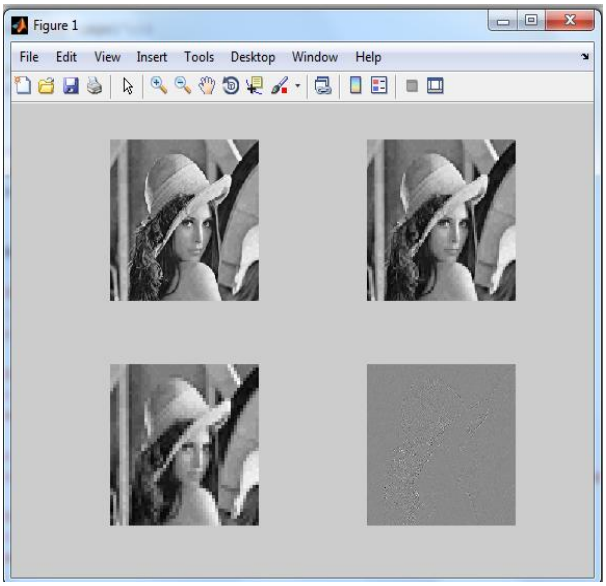

Figure 2 Remove noise from original image

B. Apply Watermark

Then we apply watermark to the original image or hide some information to the image.

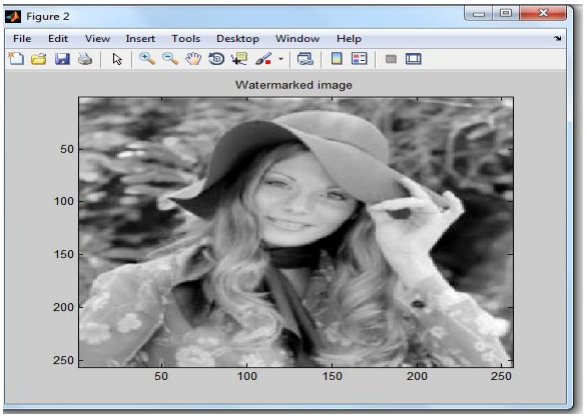

Figure 3 watermark image

C. Apply LSB

Apply LSB on watermark image for security of the image.

Figure 4 LSB image

VII. CONCLUSIONS

There are different techniques used in watermarking for security of images. Frequency domain, Spatial domain and spread spectrum. In this paper we use spatial domain method LSB for security of images, which is easy and simple and more effective method. Process of LSB is simple when we used LSB in MATLAB. A different image in MATLAB tells different process steps and their result. In future LSB may also use for other type of data and test on different type of images.

REFERENCES

[1] Avani Bhatia, Mrs. Raj Kumari"Digital Watermarking Techniques".
[2] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011
[3] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.
[4] 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
[5] Cox, Miller and Bloom, "Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher
[6] DarshanaMistry "Comparison of Digital Water Marking methods"(IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 09, 2010, 2905-2909
[7] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", AlpVision, Switzerland, pp 1 – 4M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116.
[8] H.Arafat Ali, "Qualitative Spatial Image Data Hiding for Secure Data Transmission", GVIP Journal,Volume 7,Issue 2 , pages 35- 37, 2, August 2007
[9] Max Sobell"LSB Digital Watermarking",CPE 462
[10] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518
[11] R.AARTHI, 2V. JAGANYA, &3S.POONKUNTRAN "Modified Lsb Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012
[12] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.
[13] Yeuan-Kuen Lee1, Graeme Bell2, Shih-Yu Huang1, Ran-Zan Wang3, And Shyong-JianShyu "An Advanced Least-Significant-Bit EmbeddingScheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009

