*IOSR Journal of Computer Engineering (IOSRJCE)*
*ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41*
*www.iosrjournals.org*

# Lsb Based Digital Image Watermarking For Gray Scale Image

Deepshikha Chopra[1], Preeti Gupta[2], Gaur Sanjay B.C.[3], Anil Gupta[4]
[1,2]*(CSE Department, Jodhpur Institute of Engineering & Technology Jodhpur, RTU, India)*
[3]*(ECE Department, Jodhpur Institute of Engineering & Technology Jodhpur, RTU, India)*
[4]*(CSE Department, M.B.M. Engineering College, JNVU Jodhpur, India)*

***ABSTRACT :*** *In recent years, internet revolution resulted in an explosive growth in multimedia applications. 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. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity.*
*In this paper an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented.*

*This paper presents the general overview of image watermarking and different security issues. Various attacks are also performed on watermarked images and their impact on quality of images is also studied. 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*** *- Watermarking, Least Significant Bit (LSB), JPEG (Joint Photographic Experts Group), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).*

## 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 [1, 3]. 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 [4]. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party [5]. While some watermarks are visible [6], most watermarks are invisible.

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.

## II. BASIC MODEL

Basic model of watermarking with four stages as shown in figure 2.1 below: [5, 8]

- Generation
- Embedding
- Distribution and attacks
- Detection and Recovery.

Explanation about the Generation, Embedding and Detection stage is presented together.

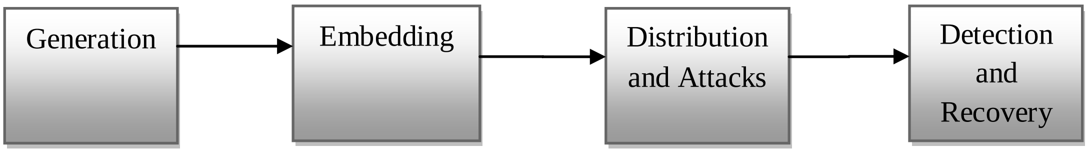


Figure 2.1 Basic Model

In Generation stage watermark is created and its contents should be unique and complex such that it is difficult to extract or damaged from possible attacks.

In Embedding stage watermark is embedded in cover media. Embedding is directly related to extraction algorithm. Hence Embedding algorithm is combination of watermark with chosen media, so the result is equivalently:

$$WM= E\ (CI, WI)$$

Where CI is original image, WI is watermark, E is embedding function and WM is the watermarked media.

The Distribution process can be seen as transmission of signal through watermark channel. Possible attacks in broadcast channel may be intentional or accidental.

Detection process allows owner to be identified and provides information to the intended recipients. There are two kinds of detection: Informed detection and Blind detection.

To insert a watermark we can use spatial domain, transform domain.

### 2.1 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

### 2.2 CLASSIFICATION OF WATERMARKING ATTACKS

Many operations may affect the watermarking algorithms and destroy it. Those operations that destroy watermark data are called attacks [7]. Here are some of the best known attacks.

- **Simple attacks:** (other possible names include “waveform attacks” and “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.
- **Detection-disabling attacks:** (other possible names include “synchronization 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, subsampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.
- **Ambiguity attacks:** (other possible names include “deadlock attacks,” “inversion attacks,” “fake watermark attacks,” and “fake-original attacks”) are attacks that attempt to confuse by producing fake original data or fake watermarked data.
- **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.
- **Cryptographic attacks:** The above two type of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security.

## III. 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.

### 3.1 REVIEW OF LSB

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 [4],[7]. Tirkel et. al were one of the first used techniques for image watermarking. 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.

The algorithm proposed by Kurah and McHughes [9] to embed in the LSB and it was known as image downgrading [2]. 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.

### 3.2 Watermark Embedded and Extraction

All images are 256*256 Pixels by 8 bit per pixel gray scale image.

Select an image CI to be used as base image or cover image in which watermark will be inserted. Select an image to be used as watermark Reading images WI which will be added to base image.

n: integer

n=no. of least significant bits to be utilized to hide most significant bits of watermark under the base image

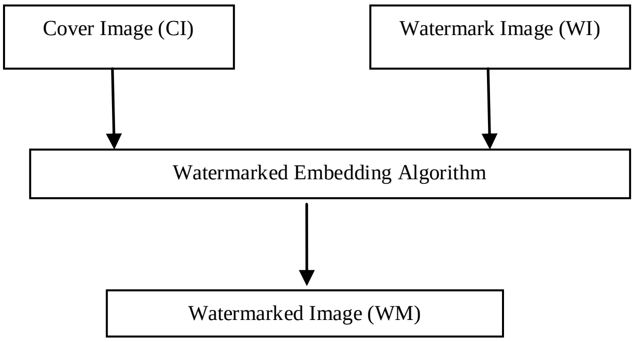


Figure 3.1 Watermark Embedded

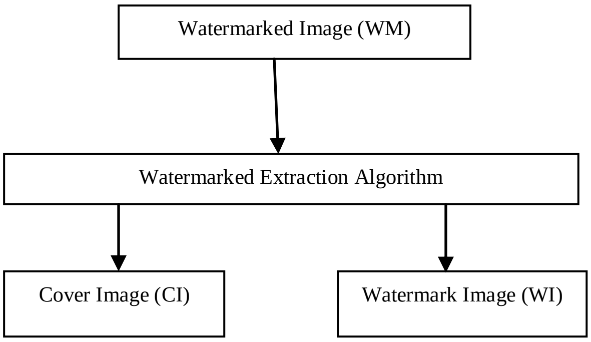


Figure 3.2 Watermark Extraction

### Watermark Embedded

```
For each pixel in base, watermark, watermarked_image
        Do
                Base_image:set n least significant bits to zero
                Watermark:shift right by 8-n bits
                Watermarked-image : add values from base and watermark
        Enddo
End
```

### Watermark Extraction

```
In watermarked image for each pixel in watermarked image and extracted image
Do
        Watermarked image:
                Shift left by 8-n bits
        Extracted image:
                Set to the shifted value of watermarked image
```

The technique used will be LSB technique which is a form of spatial domain technique.

This technique is used to add an invisible and visible watermark in the image by varying the number of bits to be replaced in base image.

## IV. Experimental Results

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 watermarked image. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality.

MSE is a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors.

Suppose that x = { $x_i$ |i = 1, 2, · · ·, N} and y = { $y_i$ |i = 1, 2, · · · , N} are two finite-length, discrete signals (e.g., visual images), where N is the number of signal samples (pixels, if the signals are images) and $x_i$ and $y_i$ are the values of the i th samples in x and y, respectively. The MSE between the signals x and y is

$$MSE(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2$$

In the MSE, we will often refer to the error signal $e_i$,= $x_i - y_i$, which is the difference between the original and distorted signals. If one of the signals is an original signal of acceptable (or perhaps pristine) quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality.

MSE is often converted into a peak-to-peak signal-to-noise ratio (PSNR) measure

$$PSNR = 10\log_{10}\frac{L^2}{MSE}$$

Where L is the dynamic range of allowable image pixel intensities. For example, for images that have allocations of 8 bits/pixel of gray-scale, L = $2^8 - 1$ = 255. The PSNR is useful if images having different dynamic ranges are being compared, but otherwise contains no new information relative to the MSE.

Cover Image CI (Flower)

Watermark Image WI (logo)

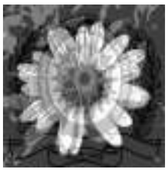
1st bit substitution

2nd bit substitution

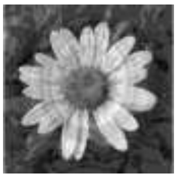
3rd bit substitution

4th bit substitution

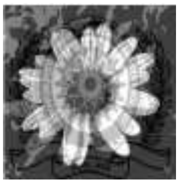
(Invisible Watermarked Image)



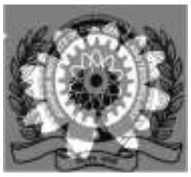
5th bit substitution



6th bit substitution



7th bit substitution



8th bit substitution

(Visible Watermarked Image)

The figure 4.1 shows various images, WI, upon which the algorithm was implemented and their corresponding watermarked copy WM. Values for mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. Table 4.1

| Method | PSNR | MSE |
|---|---|---|
| LSB or 1st Bit Substitution | 54.87 | 0.21 |
| 2nd Bit Substitution | 45.54 | 1.83 |
| 3rd Bit Substitution | 38.25 | 9.80 |
| 4th Bit Substitution | 31.68 | 44.50 |
| 5th Bit Substitution | 25.42 | 188.28 |
| 6th Bit Substitution | 19.28 | 772.72 |
| 7th Bit Substitution | 13.21 | 3129.01 |
| MSB or 8th Bit Substitution | 14.3467 | 2.3900e+003 |

TABLE 4.1 PSNR & MSE for Different Bit Substitution

## V. IMAGES WITH DISTORTIONS

Here we have applied different types of distortion to the watermarked image and the Mean Squared Error (MSE) for the images is calculated. The traditional error measuring techniques are mainly MSE and Peak Signal to Noise Ratio (PSNR). These are widely used because they are simple to calculate and are independent of viewing conditions and individual observers.

### VARIOUS ATTACKS ON THE WATERMARKED IMAGE

**1. Salt and Paper Noise**

| Bit Substitution | Watermarked Image | | Salt and Paper Noise | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| Bit=1 | 141.40 | 142.25 | 26.63 | 140.33 |
| Bit=2 | 143.97 | 142.11 | 26.64 | 137.59 |
| Bit=3 | 148.73 | 139.83 | 26.71 | 134.84 |
| Bit=4 | 145.69 | 136.52 | 26.53 | 144.24 |
| Bit=5 | 143.86 | 136.65 | 26.81 | 149.50 |
| Bit=6 | 131.87 | 132.88 | 26.93 | 135.00 |
| Bit=7 | 136.97 | 133.00 | 26.93 | 138.74 |
| Bit=8 | 184.13 | 187.42 | 25.44 | 180.95 |

**2. Gaussian Noise**

| Bit Substitution | Watermarked Image | | Gaussian Noise | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| Bit=1 | 205.67 | 203.96 | 25.07 | 204.85 |
| Bit=2 | 206.11 | 205.22 | 25.04 | 203.76 |
| Bit=3 | 204.74 | 204.71 | 25.05 | 207.45 |
| Bit=4 | 205.57 | 205.86 | 25.03 | 207.47 |
| Bit=5 | 205.40 | 205.40 | 25.04 | 207.62 |
| Bit=6 | 204.45 | 207.13 | 25.00 | 207.14 |
| Bit=7 | 197.64 | 198.67 | 25.18 | 199.47 |
| Bit=8 | 193.72 | 190.94 | 25.36 | 194.93 |

**3. Poisson Noise**

| Bit Substitution | Watermarked Image | | Poisson Noise | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| Bit=1 | 34.06 | 34.57 | 32.78 | 33.70 |
| Bit=2 | 34.27 | 34.09 | 32.84 | 34.74 |
| Bit=3 | 34.62 | 34.47 | 32.79 | 34.81 |
| Bit=4 | 34.81 | 34.89 | 32.74 | 34.51 |
| Bit=5 | 35.78 | 35.23 | 32.70 | 35.39 |
| Bit=6 | 33.64 | 33.92 | 32.86 | 33.65 |
| Bit=7 | 37.52 | 38.00 | 32.37 | 38.23 |
| Bit=8 | 36.24 | 35.96 | 32.61 | 36.28 |

**4. Speckle Noise**

| Bit Substitution | Watermarked Image | | Speckle Noise | |
|---|---|---|---|---|
| | PSNR | MSE | PSNR | MSE |
| Bit=1 | 49.75 | 49.57 | 31.21 | 49.26 |
| Bit=2 | 49.45 | 49.83 | 31.19 | 49.56 |
| Bit=3 | 49.70 | 50.33 | 31.15 | 50.11 |
| Bit=4 | 50.51 | 50.31 | 31.15 | 49.82 |
| Bit=5 | 50.84 | 51.13 | 31.08 | 51.10 |
| Bit=6 | 48.52 | 48.78 | 31.28 | 48.75 |
| Bit=7 | 56.21 | 55 62 | 30.71 | 56.15 |
| Bit=8 | 75.30 | 74.26 | 29.46 | 74.85 |

**Noise on 'Bit=1'**

**Speckle Noise**

**Poisson Noise**

**Gaussian Noise**

**Salt and Paper Noise**

## VI CONCLUSION

The increasing amount of digital exchangeable data generates new information security needs. Multimedia documents and specifically images are also affected. Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an integrity service adapted to images and more general way to multimedia documents.

The tool used for the execution of this algorithm was 'Matlab'. The aim of the program is to replace the LSB of the base image with the MSB of the watermark.

## REFERENCES

**Journal Papers:**

[1] 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

[2] Manpreet Kaur, Sonika Jindal, Sunny Behal, *"A Study of Digital Image Watermarking", IJREAS ,Volume 2, Issue 2 (Febru ry 2012) pp-126-136*

[3] B Surekha, Dr GN Swamy, *"A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011*

[4] 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.*

[5] H.Arafat Ali, *"Qualitative Spatial Image Data Hiding for Secure Data Transmission", GVIP Journal,Volume 7,Issue 2 , pages 35-37, 2, August 2007*

[6] Cox, Miller and Bloom, *"Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher*

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

[8] Lu, C-S., Liao, H-Y., M., Huang, S-K., Sze, C-J., *"Cocktail Watermarking on Images", 3rd International Workshop on Information Hiding, Dresden, Germany, Sep 29-Oct. 1, 1999*

[9] 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.*

[10] J.J.K.O. Ruanaidh, W.J.Dowling, F.M. Boland, *"Watermarking Digital Images for Copyright Protection", IEEE ProcVis. Image Signal Process. Vol. 143, No. 4, pp 250 - 254. August 1996.*

**Thesis:**

[11] Mitra Abbasfard *"Digital Image Watermarking Robustness: A Comparative Study"*, Delft University of Technologyrertre , 2009: *74 pages*

[12] Harpuneet Kaur , *"Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data" Thapar Institute of Engineering & Technology , Patiala , India ,May 2006 : 79 pages*

[13] K. Vanwasi, *"Digital Watermarking - Steering the future of security" Edition 2001, available at http://www.networkmagazineindia.com/200108/security1.html*

[14] Saraju Prasad Mohanty, *"Watermarking of Digital Images", Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999*

**Books:**

[15] *Andreas Koschan, Mongi Abidi, " Digital Colour Image Processing" Published by John Wiley & Sons, Inc., Hoboken, New Jersey,Published simultaneously in Canada.*