

# Improvement of Binary Based Watermarking Technique

MOHAMED EASSA<sup>1</sup>, YAHIA HAMDY ELBASHAR<sup>2\*</sup>

<sup>1</sup>Department of Basic Science, Thebes Higher Institute for Engineering, Cairo, Egypt

<sup>2</sup>Department of Basic Science, EL Gazeera High institute for Engineering and Technology, Cairo, Egypt

\* Corresponding author: [y\\_elbashar@yahoo.com](mailto:y_elbashar@yahoo.com)

## Abstract

In this paper, a new invisible digital watermarking technique that using intermediate significant bit (ISB). The proposed algorithm embedded the message in other significant bit to make the technique more robust than standard technique (least significant bit). The technique is developed to enhance quality of watermarked images in spatial domain through reducing noise imposed by the watermark. Experimental results show a significant enhancement of quality of watermarked image on the expense of extracted message quality and robustness of the proposed technique to a range of attack types.

**Keywords:** Digital watermarking, other significant bit, LSB, PSNR, SSB.

## 1. Introduction

Over the past decade, image authentication comes to the front, and there has been significant development of the World Wide Web and digital technology, leading to an exponential increase of sharable multimedia data such as digital images and photographs. However, owners were rejected to display and distribute their images, as digital images can be easily distributed without the owner's consent. Digital watermarking emerged as a way to tackle this important issue and discourage copyright violations. It also helps to prove ownership of digital images. This work is a technique for hiding an invisible watermark in an image with aim of proving its ownership is introduced and tested, [1]. Most of the research focused on frequency domain (transform domain) technologies for their strong robustness property against attack. But the spatial domain technology which utilizes the least significant bit (LSB) of the image to embed a large amount of data has good visual imperceptibility, and extreme ease of implementation [2]. Different techniques were proposed including watermarking the images with either visible or invisible watermarks. Visible watermarking purposely distorts images while invisible watermarking is supposed to leave no visible distortions [3]. However, as data of the watermark is inserted into the image data, it leaves distortion from the original evaluated through calculation of Peak Signal to Noise Ratio (PSNR). Many techniques were proposed for that purpose with different implementation levels' ease and difficulty, different levels of quality and robustness.

## 2. Literature review

Recently, techniques that used both spatial and transform techniques are introduced. In [4], a technique-based least significant bit (LSB) is proposed. This algorithm used LSB by inverting the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of the image before embedding the watermark. If the length of the watermark text is more than  $((M \times N)/8)-2$ , the extra of the watermark text is embedded in the second LSB. Also, they showed the experimental results when combining different positions of LSB such as the second LSB, the third LSB, the fourth LSB, and the combination between them. This algorithm improved the quality of the watermarked image; however, it suffers from the robustness of watermarked image. In [5], a technique based on the multiple transform method, discrete wavelet transform (DWT), and discrete fractional random transform (DFRNT) is proposed. It selects a two-dimensional (2D) barcode for hiding the information and applies the block code encoding and generates a watermark through them. The generated watermark image is embedded into DWT-DFRNT using the quantization technique. This technique achieves robustness; however, it suffers from the low quality of the watermarked image. In [6], a hybrid steganography technique is presented which is an integration of both spatial and transforms domains. Both the cover image and payload are divided into two cells each and RGB components of only the cover image cell 1 are transformed into the frequency domain using DWT/DCT and retaining Cell 2 in the spatial domain. Embedding a secret image ( $128 \times 128$ ) into a cover image ( $512 \times 512$ ) shows that DWT has better PSNR compared to DCT as well as individual transform domain techniques. However, the robustness issue of watermarked images is not discussed. In [7], a technique for watermarked images based on DWT, DCT, Singular Value Decomposition (SVD), and a semi-blind algorithm (Trigonometric function) is introduced. The trigonometric function is used to closely relate the singular values of the original image and the watermarked image. This technique is robust against several attacks like cropping, noise, rotation, filtering, and translation. However, the quality of the watermarked image is not discussed. In [8], a semi-blind watermarking technique that combines and uses DWT and Singular Value Decomposition (SVD) algorithm is proposed. It is used a grayscale image as a watermark to hide in another grayscale image as a cover image. The cover image is modified and divided into the number of blocks of size  $n \times n$ . This algorithm provided robustness for various attacks (average filtering, median filtering, additive Gaussian noise, cropping, rotation, pixilation, wrapping, motion blur) equalization, and sharpening. The only drawback of this technique is that the PSNR shows the low quality of the watermarked image. In [9], a technique for image steganography based on DWT and Huffman Encoding is presented. Two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image and Huffman encoding is performed on the secret messages before embedding. Then, each bit of the Huffman code of the secret message is embedded in the high-frequency coefficients resulting from Discrete Wavelet Transform. This technique improved the quality of the watermarked image. In [10], a hybrid non-blind technique based on discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) is introduced, which applies SVD to the LL sub-band, then the LL sub-band coefficients are reconstructed with modified singular values and inverse DWT is applied to obtain the watermarked image. This technique achieves robustness and reliability via embedding a ( $256 \times 256$ ) pixels binary image into a ( $512 \times 512$ ) pixels cover image. In [11], a robust image watermarking technique based on 1-level DWT (Discrete Wavelet Transform) is proposed. This method embeds the invisible watermark into salient features of the original image using the alpha blending technique. The experiment result shows that the embedding and extraction of the watermark are dependent only on the value of alpha. All the results obtained for the recovered images and watermarks are identical to the original images. In [12], presents a technique based on discrete wavelet

transform (DWT) and singular value decomposition (SVD). The singular values of the binary watermark are embedded in singular values of LL3 (low frequency 3-level) sub-band coefficient of the host image by making use of multiple scaling factors (MSFs). This technique utilized Firefly algorithm to achieve the balance between imperceptibility and robustness via embedding a  $(32 \times 32)$  pixels binary image into  $(256 \times 256)$  pixels cover image, however, the watermark was small compared to the cover image.

### 3. Standard technique

#### 3.1- Least Significant Bit

LSB is the simplest technique of spatial domain techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes, [13].

**General advantages of spatial domain LSB technique are:**

1. There is less chance for degradation of the original image, [14].
2. More information can be stored in an image, [13].

**Disadvantages of LSB technique are:**

1. It is not very robust against attacks, [14].
2. The watermark can be easily destroyed by simple attacks, [13].

**The embedding procedure in LSB, [15]**

A= Original Image

B= Watermark

C= Watermarked Image

A: 10000100 00100101 10001000 01010001...

B:           1           0           0           1...

C: 10000101 00100100 10001000 01010001...

#### 3.2- Other Significant Bit (OSB)

In this technique, the particular significant bit of the image's digital data is altered in the embedding operation, [16].

**Advantage:** That is more robust about the attack than the LSB, [17] [18].

**Disadvantage:** increase the amount of noise in the watermarked image. And this problem has no solution till now, [19] [20].

## The embedding procedure in other significant bit

### Original pixel 8-bit value

1	0	1	1	0	1	1	1
---	---	---	---	---	---	---	---

Value = 183

### Embedding 1 in 4-SB (standard technique)

1	0	1	1	1	1	1	1
---	---	---	---	---	---	---	---

Value = 191

Error = 191 - 183 = 8

## 4. Proposed technique

In this technique, we increase the security and robustness of watermarked image by embedding the watermarked in other significant bits but also it increases the image quality more than the standard technique. The optimization is carried out by considering a new pixel value with all bits equal to zero, changing the required embedding bit to the new watermarked image pixel value, then optimizing the other bits starting from the highest significant bit. To achieve that every bit is considered to have values of 1, and 0, and the bit value is optimized through comparison between the corresponding pixel value of watermarked image and cover image. Finally, the bit value that produces the lowest error is selected by cycling through all the bits aside from the embedding bit, the total value of the pixel is optimized and the lowest error of embedding is achieved.

### Original pixel 8-bit value

1	0	1	1	0	1	1	1
---	---	---	---	---	---	---	---

Value = 183

### Step 1

The watermark bit is embedded in the required nth bit of cover image byte like competitive techniques, using the following steps:

a - Consider a new watermarked pixel value is zero (all bits are zeros).

0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---

b - Write the watermark bit to the corresponding new bit of watermarked pixel.

### Embedding 1 in 4-SB (proposed technique)

0	0	0	0	1	0	0	0
---	---	---	---	---	---	---	---

### Step 2

The rest of the bits of the watermarked byte are optimized by changing their values to reduce distortion resulting from the watermark embedding (reducing the error), using the following steps:

c - Consider the value of the highest significant bit to be 1 and evaluate the pixel value.

1	0	0	0	1	0	0	0
---	---	---	---	---	---	---	---

**Byte value =  $128+8 = 136$**

d - Consider the value of the highest significant bit to be 0 and the value of other significant bits to be 1.

0	1	1	1	1	1	1	1
---	---	---	---	---	---	---	---

**Byte value = 127**

e - Compare the two values with the cover image's pixel and evaluate the absolute errors.

**Error (of c) =  $183 - 136 = 47$**

**Error (of d) =  $183 - 127 = 56$**

f - Choose the bit value that achieved the lowest error.

**Bit 8 value selected is 1**

g - Go through all bits aside from embedding SB and repeat the procedures (c to f) then the rest of the bits' values are optimized.

1	0	1	1	1	0	0	0
---	---	---	---	---	---	---	---

h - The value of the pixel is evaluated and considered as the watermarked pixel value

**The new pixel value = 184**

**Error =  $184 - 183 = 1$**

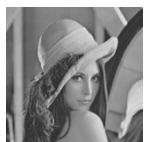
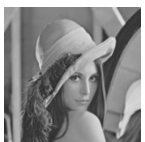
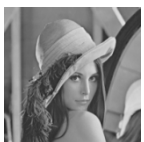









## 5. Experimental results

The results show an improvement in PSNR of the proposed technique when compared to the standard LSB without adding much processing load.

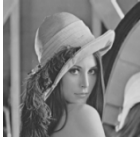



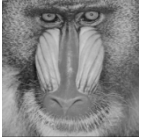







1-We present the result of embedding the watermark in other significant bits by standard method and proposed method using PSNR, Table 1-8.

*Note: All images are  $512 \times 512$  pixels.*

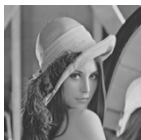
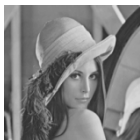
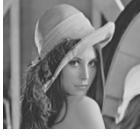









**Table 1.** The message Embedded in the first significant bit 1SB (LSB)

Host Image	Original image	Standard Watermarked image	PSNR	proposed Watermarked image	PSNR	message
Lena			51.1528		51.1528	M
Baboon			51.1459		51.1459	M
Peppers			51.1513		51.1513	M
Jet			51.1551		51.1551	M




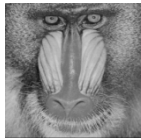

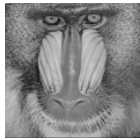






**Table 2.** The message Embedded in the second significant bit (2SB)

Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	Message
Lena			45.1250		51.1406	(M)
Baboon			45.1157		51.1320	(M)
Peppers			45.1250		51.1433	(M)
Jet			45.0946		51.1152	(M)

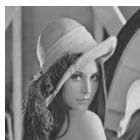

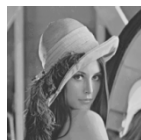









**Table 3.** The message Embedded in the third significant bit (3SB)

Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			39.0758		47.1345	(M)
Baboon			39.0988		47.1599	(M)
Peppers			39.1487		47.2053	(M)
Jet			38.9703		46.9944	(M)

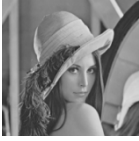

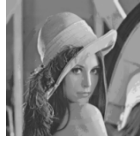
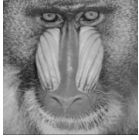



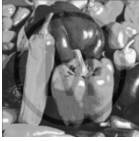




**Table 4.** The message Embedded in the fourth significant bit (4SB)

Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			33.0645		42.3765	M
Baboon			33.0812		42.3567	M
Peppers			32.9449		41.9674	M
Jet			33.0982		42.3160	M




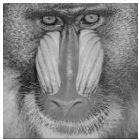
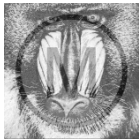


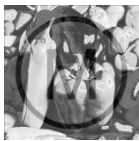
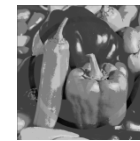



**Table 5.** The message Embedded in the fifth significant bit (5SB)

Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			27.2383		37.3367	M
Baboon			27.1761		37.1706	M
Peppers			26.8901		35.6229	M
Jet			27.3965		37.3675	M

**Table 6.** The message Embedded in the sixth significant bit (6SB)





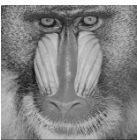

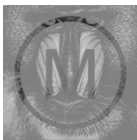









Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			20.9673		31.3378	(M)
Baboon			21.3470		31.7450	(M)
Peppers			20.6656		28.8013	(M)
Jet			19.7299		29.2105	(M)

**Table 7.** The message Embedded in the seventh significant bit (7SB)

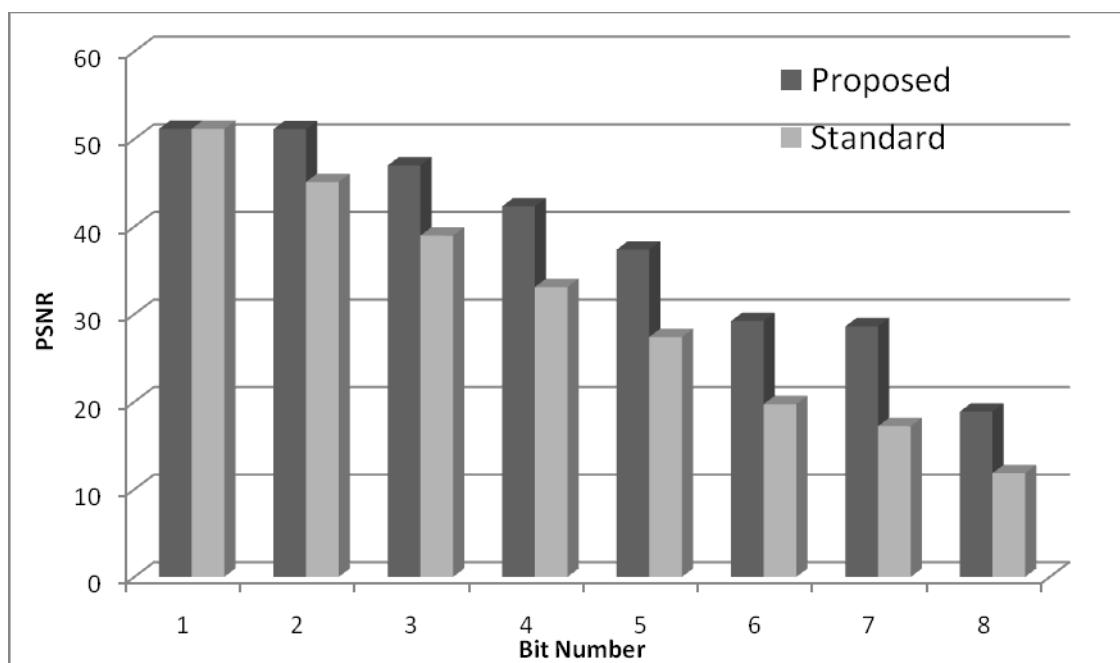
Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			14.6778		25.7421	(M)
Baboon			14.7609		25.4603	(M)
Peppers			14.1278		21.5177	(M)
Jet			17.2123		28.6154	(M)



**Table 8.** The message Embedded in the eighth significant bit (8SB)

Host Image	Original image	Standard Watermarking technique	PSNR	proposed Watermarking technique	PSNR	message
Lena			9.0153		17.5842	
Baboon			8.9124		18.0315	
Peppers			8.6845		13.7971	
Jet			11.8435		18.8701	

The histogram of PSNR is displayed in Figure 1, as it shows how superior the proposed technique is to the standard technique.



**Figure 1.** The histogram of PSNR

2- We present the comparison between proposed method and Jitendra Jain's method, [21]. The (Jitendra Jain, et al) work shows the embedding of watermark into the nth significant bit

of original image. The result illustrates that PSNR of proposed method is enhanced compared to Jitendra Jain's method, Table 9.

**Table 9.** Comparison between the proposed method and Jitendra Jain's method

Significant Bit	(Jitendra Jain, et al) PSNR	(Proposed method) PSNR
<b>1SB (LSB)</b>	51.1440	51.1448
<b>2SB</b>	45.1193	51.1316
<b>3SB</b>	39.1116	47.1320
<b>4SB</b>	33.1051	42.3737
<b>5SB</b>	26.9516	37.3769
<b>6SB</b>	21.6501	31.2901
<b>7SB</b>	15.1870	25.5488
<b>8SB (MSB)</b>	10.6623	17.5822






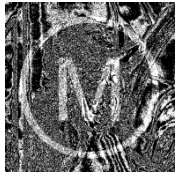

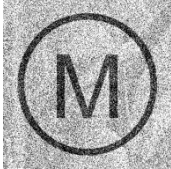
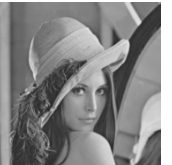


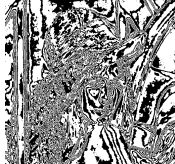
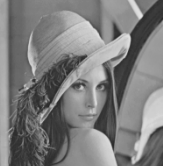



Original image  
(512×512) pixels




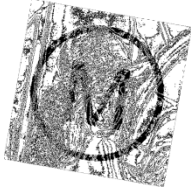

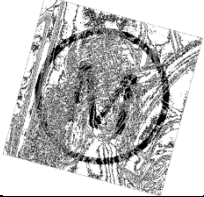

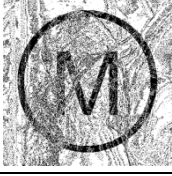
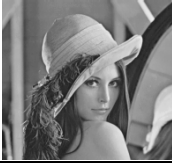





Message (512×512) pixels

3. We present the result of some attacks on the watermarked image and its effect on the watermark, table 10.

**Table 10.** Some types of attacks at 4SB (mid-range of SB) proposed

Attacks type	Watermarked image after attack	Message
<b>Cropping</b>		
<b>Brightness</b>		
<b>Random noise 50%</b>		
<b>Soften</b>		
<b>Blurring</b>		
<b>Resize double</b>		
<b>Resize 0.5</b>		

Attacks type	Watermarked image after attack	Message
Rotate 5%		
Rotate 10%		
Rotate 15%		
Sharpen		
Contrast		
Median filter		

## 6. Conclusion

In this paper, we have presented an improved LSB technique (proposed technique) to embed the message in the cover image to get the watermarked image. This technique aims at increasing the quality and robustness of watermarked image at the same time by embedding the watermarked in a deeper significant bit layer but without sacrificing the image quality. This technique gets the balance between quality enhancement and robustness against attacks of the watermarked image.

## 7. References

- [1] Kaur M., Jindal S., and behal S. (2012). A Study Of Digital Image Watermarking, *International Journal of Research in Engineering & Applied Sciences*, 2(2), 126-136.
- [2] Sun J., li Y., Zhong X., and Li J. A. (2020). Scheme of LSB Steganography Based on Concept of Finding Optimization Pixels Selection, *Springer-Verlag Berlin Heidelberg*, 155-160.

- [3] Singh N., and Rani S. (2010). Embedding Watermark: the way to improve Security, *International Journal of Electronics and Computer Science Engineering*, 492-496.
- [4] Bamatraf A., Ibrahim R., and Salleh M. N. M. (2011). A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit, *JOURNAL OF COMPUTING*, 3(4), pp. 1-8.
- [5] Kim M., Li D., and Hong S. (2014). A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method, *International Journal of Multimedia and Ubiquitous Engineering*, 9(1), 369-378.
- [6] Shiva K. B., Raja K. B., and Pattnaik S. (2019). Hybrid Domain In LSB Steganography, *international journal of computer application*, 19(7), 35-40.
- [7] Saxena H., Saxena P., and KIMT S. R. (2014). DWT-DCT-SVD based semi-blind reference image watermarking scheme using trigonometric function, *International Journal of Conceptions on Computing and Information Technology*, 2(2), 14-18.
- [8] Murty S., Bhaskar M. U., Babu P. N., and Kumar P. R. (2011). A Semi-Blind Reference Watermarking Scheme Using DWT-SVD for Copyright Protection, *The International Journal of Multimedia & Its Applications (IJMA)*, 3 (3), 61-70.
- [9] Nag A., Biswas S., Sarkar D., and Sarkar P. P. (2010). A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, *International Journal of Computer Science and Security, (IJCSS)*, 4(6), 561-570.
- [10] Jane O., Elbasi E., and Lik H.G. (2014). Hybrid Non-Blind Watermarking Based on DWT and SVD, *Journal of Applied Research and Technology*, 750-761.
- [11] Shing A. P. and Mishra A. (2011). Wavelet Based Watermarking on Digital Image, *Indian Journal of computer Science and Engineering*.
- [12] Agarwal C., Nishra A., Sharma A., and Bedi P. (2014). Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm, *Expert Systems with Applications*, 1-10 .
- [13] Hussian M., and Hussian M. (2013). A Survey of Image steganography Techniques. *International Journal of Advanced Science and Technology*, 54, 113-124.
- [14] Singh P., and Chadha R. S. (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks, *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9), 165-175.
- [15] Bhalla J. S., and Nagrath P. (2013). Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm, *International Journal of Scientific and Research Publications*, 3(4), 1-6.
- [16] Bamatraf A., Ibrahim R., and Salleh M. N. (2011). A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit, *JOURNAL OF COMPUTING*, 3(4), 1-8.
- [17] Jayaraman S., Esakkirajan S., and Veerakumar T. (2009). *Digital Image Processing, McGraw-Hill*.
- [18] Eassa M., Selim I. M., Dabour W., and Elkafrawy B. (2021). Automated classification technique for edge-on galaxies based on mathematical treatment of brightness data, *Research in astronomy and astrophysics*, 21, 264-272.
- [19] Pan J., Huang H. C., and Jain L. C. (2004). *Intelligent Watermarking Techniques, World Scientific*.
- [20] Eassa M., Selim I. M., Dabour W., and Elkafrawy P. (2022). Automated detection and classification of galaxies based on their brightness patterns, *Alexandria Engineering Journal*, 61, 1145-1158.
- [21] Jain J., and Johari P. (2014). Digital Image Watermarking Based on LSB for Gray Scale Image. *International Journal of Computer Science and Network Security (IJCSNS)*. 14(6), 108-112.