Performance Analysis of Least Significant Bit Based Watermarking Technique Under Various Types of Attacks

Afkar Ali Hasan, Majid Jabbar Jawad, Mohammed Abdullah Naser

Computer Science Department, College of Science for Women University of Babylon, Babil, Iraq.

hassanafkar5@gmail.com

Abstract. Digital information transferred through internet should be protection from unauthorized and attack resource using one of the information security system method, one of these methods was digital watermarking was used in order to prevent information from various types of attack adversary since it satisfies all security system requirements (authentication, integrity and confident). Digital watermarking is used digital image for several purposes such as authentication, copyright, and many purposes. This paper we embedded (number of bits) MSB of watermark image in the (number of bits) LSB of cover image by proposed embedding algorithm, where the ratio of appearing information of the watermark in the watermarked image depends on a number bits embedded. Such that increasing the number bits increase the information display. The performance of the algorithm for watermarking and quality of reconstructed image have been measured in terms of MSE and PSNR. This paper produced performance analysis of image watermarking technique depend on least significant bit against several attacks (Gaussian, salt and pepper noise, Poisson and Speckle). The result of the attack appears that salt and pepper attack give best result than other types when it applied on the original image and watermarked image. Simulation results show that best results were achieved against Salt and Pepper attack in terms of less MSE and high PSNR. MATLAB language is used for implementing the suggested Algorithm.

Keywords. Digital watermarking, Least Significant Bit, Mean Square Error, Peak Signal to Noise Ratio, watermarking’s attacks, watermark applications.

1. Introduction

The recent development that done in the information technology and communication network, make all digital data can be distributed. There are several types of attacks may challenge the digital data through its distributed [1]. Several methods suggested for protecting networks against attacks. Cryptography, steganography, digital watermarking is among them. Digital watermark is the most widely used method for securing the original data from unauthorized manipulation and dissemination [2].

Firstly, applied the watermark by TIRKEL in 1993, where TIRKEL supplied watermarking strategies to hide the watermark facts in the photos. Also, can apply this technique with text, audio, and video [3]. In generally, the watermarking technique is utilized to cover up data or distinguishing information within digital multimedia. Our paper will center mainly on the digital images watermarking. Digital watermarking is a method to embed some information called watermark into several media form called cover, which cannot be effortlessly recovered by the third party [4].
1.1. Related Works
This section reviews several works related to our suggested approach:

Abdullah Bamtraf, et al. (2011) [5] presented new algorithm depend on the combination of LSB Reverse the watermark text binary values and move the watermark to the odd or even number of pixel object coordinates before embedding the watermark. This depended on the length of the text of the watermark. If the watermark text size is greater than ((MxN)/8)-2. Suggested algorithm keeps the watermarked goodness.

Kamal deep Joshi, et al. (2016) [6] The scaling factor methodology was analyzed using DWT with different scaling factors and pictures of grayscale. Using the Discrete Wavelet Transformation (DWT) additive method, the watermark power of the grayscale picture was used. Where, the host picture of the grayscale is divided into four sub-bands: (Low-Low), (High-Low), (Low-High), (High-High) and the (Low-Low) sub-band covered with DWT technique.

Nasrin M. Makbol, et al. (2016) [7] proposed a block-based mechanism using the human visual system with along SVD and DCT. Entropy and Edge entropy are utilized as HVS properties to choose significant blocks to embed the watermark. Through the proposed mechanism.

Khalid Ahmed Youssif Ibrahim Al-Afandy (2017) [8] proposed two methods for providing the security using digital watermark. The first method is Homomorphic Particular Value Deterioration watermarking in Discrete Wavelet Change space, second method based on 3-level Discrete Stationary Wavelet Change within the Discrete Cosine Change space.

Anamika Upadhyay, et al. (2018) [2] used quad tree with digital watermarking utilizing LSB and DES. This method selects position in an original image for inserting the hidden text in variable sized quad tree blocks. A threshold and a minimal block volume are used to control the number of blocks obtained for an original image.

Nazir A. Loan, et al. (2018) [9] presented a novel approach that could be applied to color as well as grayscale images that were based on a chaotic encryption and was named as blind digital image watermarking approach. Before the watermark is embedded within the host image, Discrete Cosine Transform (DCT) is applied.

Abdulaziz Shehab, et al. (2018) [10] A new approach has been proposed novel for medical applications for providing image authentication and self-recovery. The image tampering is localized and the original image is recovered by proposing this new fragile watermarking based on approach.

Maimaitiming mamuti, et al. (2019) [11] improved watermarking scheme for medical image uses Red, Green, and Blue color channels of the color image. RGB original image is first invalid into Red, Green, Blue channels, then Discrete Cosine Transform on G channel and LSB on B channel, Discrete Wavelet Transform is implemented on R channel, Medical image is treated with Arnold Scrambling before being embedded. With combination of conventional and widely used watermarking algorithms such as LSB, DWT and DCT, and application of Arnold scrambling technique the new watermarking scheme proves to be more hardness as it is evident from the experimental result.

2. Materials and Methods

2.1. DIGITAL WATERMARKING FUNDAMENTALS
As mentioned, the idea of the watermarking is hidden additional data may be text, logo, image inside another object such as image, software code, video, signal without effect on the quality of the host object [12]. Therefore, the following two primary processes can be described which are illustrated in Figure (1).
Figure 1. General idea of digital watermarking.

- Watermark Embedding.
- Watermark Extraction.

The watermarking processes can be described. By embedded a watermark information into a cover, to build watermarked. The watermark distortion is defined between a cover and watermarked. In order to improve the safeness, usually encoded the watermark data using a secret key [12].

After inserting the watermark, intentional and unintentional distortions such as compression, conversions, and noise can be placed on the watermarked cover [12]. Also, it’s techniques can be classified according to domain criteria as:

- Spatial Domain.
- Transform Domain.
- Multiple Domain.

The watermarking method which works in the spatial domain, that is the Least Significant Bit method, we used in this paper to cover the least significant bits of pixels chosen to mask the data. This method has several implementing versions which in some aspects boost the algorithm. Data in a digital image can be directly inserted into all bits of image data [4].

From the other side, there are three main approaches for watermark detection [12]:

- Blind watermarking the cover need not be identified by the watermark.
- Semi blind watermarking the watermark needs to be detected using some cover data.
- Non blind watermarking the watermark must be identified using the cover and the watermarked manipulated.

Also, can be divided watermarking methods into three methods:

- Robust digital watermarking that even under danger and harmful distortions discovers the watermark.
- Semi-fragile digital watermarking discovered under just unintentional distortions by the watermark.
- Fragile digital watermarking This will only discover the watermark if there are no intentional or unintentional distortions [12].

2.2. Requirements of Digital Watermarking

1. Robustness: the watermarked object, may be exposed to several manipulation operations such as compression, addition...etc., under international and un international attack, the extracted watermark varies less from the initial watermark.

2. Capacity: Capacity or payload means how many information bits can be embedded in digital object.

3. Imperceptibility: The watermark ought to not be recognizable to the watcher. Imperceptibility can be communicated by measuring quality or devotion. There are two tests accessible for devotion and quality estimations counting subjective and objective.

4. Tamper Resistance: The watermark system's resistance for threatening attacks. Each application depends on several kinds of tamper resistance for several types of attacks such as (active attacks, passive attacks, collusion attacks, forgery attacks).
5. Computational Cost: The watermarking method should be less complex to reduce computational cost [7]. It is referred to as dollar cost and speed requirements for both watermarks embedding and extraction processes [12].

2.3. Applications of Digital Watermarking

Digital watermarking is applied in several applications [12] such as:
1. Copyright protection.
2. Digital right management.
3. Broadcast monitoring.
4. Forensics and Piracy Deterrence
5. Medical application.
6. Document and Multimedia Security.
7. Authentication.
8. Fingerprinting [1]
9. Indexing [1]

2.4. Watermarking Attacks

There are many attacks that may be performed on the watermarked image possible malicious intentional or unintentional. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is preventing the watermark from performing its intended purpose [8]. Various types of attacks are:
- Removal Attack
- Interference attack
- Geometric attack
- Low pass filtering attack
- Forgery attack

2.5. PERFORMANCE Measures

The following measures or benchmarks are usually used to measure image deterioration and to test the extracted watermarks with and without attacks

2.5.1. Mean Square Error

MSE could be signal devotion degree. The objective of signal constancy degree is to compare two signals by giving a quantitative score that depicts the level of mutilation between them. More often than not, it is assumed that one of the signals may be an original, whereas the other is mutilated or sullied by blunders.

The MSE between two digital images is [13]:

\[
MSE = \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} [I(m,n) - \hat{I}(M, N)]^2
\]  

(1)

2.5.2. Peak Signal to Noise Ratio

MSE is often transformed into a PSNR (Peak-to-Peak) measure [14].

\[
PSNR = 20 \log_{10}(MAX) rew - 10 \log_{10}(MSE)
\]  

(2)

Where MAX is the dynamic range of agreement image pixel density. For instance, for images with 8 bits / pixel gray-scale allocations, L = 28−1 = 255. The PSNR is valuable when comparing pictures with diverse dynamic ranges, but something else does not contain any new data relative almost the MSE [14].
2.6. Proposed System
This part will explain the principle work for the digital image watermarking based on three parts:

- Watermark Embedding
- Attacks on Watermarked Image
- Watermark Extracting

The first part that based on the construct the watermarked image using the proposed algorithm by embedded watermark image $W$ with cover image $C$. where we proposed algorithm for cover most significant $n$ bit (n MSB) from the watermark in (n LSB) of the cover image, where the result of the appearing for the watermark based on the value of $n$ bit.

We applied our paper in the special domain of grayscale image (pixel), That represent each value in it with 8 bits, there for the value of $n$ must be between (1 to 8).

In the second part, Different types of manipulation have been added to the watermarked image and the mean square error is measured for the images. MSE and PSNR are the standard methods for error calculation. These are commonly used because they are easy to calculate and independent of visual conditions and particular analysts.

In the third part, we inverse the embedded algorithm to extract the watermark from the watermarked image, where it used the watermarked image and (n) number of bits, that used for embedded.

Now, can we describe our paper with the following figure (2).

Figure 2. Framework of proposed watermark

We can be described each step with the corresponding algorithm, where the first step that represents embedded, take the cover and watermark and $n$: number of hidden bits.

After then take the $n$ bits from the most significant bit in the watermark and put it in LSB of the original image(cover).

**Embedding Procedure**
The algorithm 1 illustrates the main steps for the embedding procedure

**Algorithm (1): Main Embedding Procedure**

**Input:**
Cover Image, Watermark image, n: number of bits want embedding.

**Output:**
Watermarked Image.

**Start**
Step 1: load cover image.
Step 2: load watermark image.
Step 3: read value n: number of embedded bits.
Step 4: convert cover and watermark to gray scale
\[ CI \leftarrow \text{convert to gray(cover)} \]
\[ WI \leftarrow \text{convert to gray (watermark)} \]
Step 5: for each pixel in CI
Set n LSB to zero
Step 6: for each pixel in WI
Shift (8-n) to right
Step 7: for each pixel in watermarked
\[ Wm=\text{adding (CI, WI)} \]
Step 8: save Wm matrix to image

**End**

**Extraction Procedure**
The watermark can be retrieved in reverse of the embedded algorithm's work, where we receive the watermarked image Wm and number of embedded bit as input, after then shifted each pixel to the (8-n)left, that make it as the MSB in same pixel, and sets another bits to construct value of pixel for the extracted image (that must be represented watermark image). can be described in details as the following procedure:

The algorithm (2) illustrates the main steps for the Extraction procedure.

**Algorithm (2): Main Extraction Procedure**

**Input:**
Watermarked image WM
The number of embedded bits n.

**Output:**
Extracted Watermark Image (EWI).

**Start**
Step 1: Wm=convert to the matrix (watermarked image);
Step 2: input number of bit (n)
Step 2: for each element in the Wm
shift left by (n) bits
Set the shifted value to a watermark.
Step 3: get the extracted watermark (EWI)

**End**

**Attacks on Watermarked Image**
Between the embedding operation and the extracting operation, the watermarked image may be exposed to the intentional or unintentional distortion that what’s known as an attack.

In the suggested paper, we used noise attack and calculate the ratio of the error using "mean square error, peak signal to noise ratio". that we measured for four types of attack (Gaussian, salt and pepper, passion, speckle), where we applied with all watermarked images that generated from the different values of n bits (1 to 8).

The algorithm (3) illustrates the main steps for the Attack procedure.

Algorithm (3): Main Attack Procedure

| Input:          |
|----------------|----------------|
| WM: Watermarked Image. |
| AT: Attacking Type |
| Output:         |
| AWM: attacked Watermarked Image. |

Start

Step 1: Input attacking type (AT)
Step 2: AWM= attacking (AT, WM).
Step 3: Get attacked watermarked image (AWM)

End

3. Experimental Results and Discussion
In this part, we will discuss the results of embedding the original images (cover) with the secret image (watermark), using n bits (1 to 8). Then, evaluating the results using two measurement tools: MSE and PSNR.

| No. of bits | Cover image | Watermark image | Watermarked image | Extracted watermark image | MSE   | PSNR  |
|-------------|-------------|-----------------|-------------------|---------------------------|-------|-------|
| 1           | ![Image 1](image1.png) | ![Image 2](image2.png) | ![Image 3](image3.png) | ![Image 4](image4.png) | 0.5968 | 50.3725 |
| 2           | ![Image 5](image5.png) | ![Image 6](image6.png) | ![Image 7](image7.png) | ![Image 8](image8.png) | 1.9498 | 45.2308 |
| 3           | ![Image 9](image9.png) | ![Image 10](image10.png) | ![Image 11](image11.png) | ![Image 12](image12.png) | 10.7195 | 37.8291 |
when we applied four types of attacks (Gaussian, salt and pepper, Poisson, speckle), on the cover image can see the result in figure (3)

![Figure 3](image-url)  
*Figure 3. results of applied types of attacks on the cover of test 1*
### Table 2. Results of Gaussian attack and Salt and Pepper attack on the watermarked of test 1

| No. of bits | Attacked Gaussian on the watermarked image | MSE    | PSNR  | Attacked Salt and pepper watermarked image | MSE    | PSNR  |
|------------|------------------------------------------|--------|-------|-------------------------------------------|--------|-------|
| 1          |                                          | 84.8568| 28.8439 |                                            | 6.2731 | 40.156|
| 2          |                                          | 84.7954| 28.8263 |                                            | 6.35   | 40.1031|
| 3          |                                          | 84.3553| 28.8697 |                                            | 6.5186 | 39.9893|
| 4          |                                          | 84.4709| 28.8637 |                                            | 6.2907 | 40.1438|
| 5          |                                          | 85.2619| 28.8233 |                                            | 6.1937 | 40.2113|
| 6          |                                          | 85.0026| 28.8365 |                                            | 6.2037 | 40.2043|
| 7          |                                          | 83.8921|        |                                            | 6.0392 | 40.321 |
| 8          |                                          | 85.0858| 28.8322 |                                            | 6.0189 | 40.3356|

### Table 4. Results of Poisson attack and speckle attack on the watermarked of test 1

| No. of bits | Attacked Poisson on watermarked image | MSE    | PSNR  | Attacked Speckle on watermarked image | MSE    | PSNR  |
|------------|--------------------------------------|--------|-------|--------------------------------------|--------|-------|
### 4. CONCLUSIONS
This paper attempted to provide the most important digital watermarking information that will help new researchers acquire the full expertise in this field. Where digital watermarking is one of the best ways to avoid unauthorized copying, alteration and dissemination of multimedia information, especially with increasing the development of the communication technology and distribution digital information. In this paper, watermarking algorithm is used for hiding digital image in another digital image with

|   |   |   |   |   |
|---|---|---|---|---|
| 1 | 32.9412 | 32.9534 | 71.8677 | 29.5655 |
| 2 | 32.9613 | 32.9508 | 71.9902 | 29.5581 |
| 3 | 33.1629 | 32.9243 | 73.2341 | 29.4837 |
| 4 | 33.7424 | 32.849 | 74.6095 | 29.4029 |
| 5 | 35.172 | 32.6688 | 76.2804 | 29.3067 |
| 6 | 36.5302 | 32.5043 | 81.5682 | 29.0156 |
| 7 | 38.8246 | 32.2397 | 83.6915 | 28.904 |
| 8 | 56.3666 | 30.6206 | 101.175 | 28.0801 |
different LSB bits, where a watermark image was embedded on the cover image to keep the information of the watermark. We embedded (no. of bits) MSB of watermark in the (no. of bits) LSB of cover, where the ratio of appearing the information of the watermark in the watermarked image depends on the number bits embedded. Such that increasing the number bit increase the information display. Using (MSE) and (PSNR) to evaluate the goodness of watermarked. The results show that the goodness of watermarked depends on the number of bits of watermark that embedding on original image, where increasing the number of bits less the goodness science when increase the number of embedding bits increase information display. Experimental results show that the suggested algorithm satisfied the robustness and imperceptibility requirements. The results of proposed algorithm give better results less "MSE" and high "PSNR" against Salt and Pepper attack when it applied on the watermarked image and an original image and, on the other side MSE depends on the embedding bits for the watermarked image, where "MSE" not inversely proportional with embedding bits. As Future works, we are planning to combine encryption algorithms with steganography algorithms for increasing the layer security, the proposed algorithm can be applied on another media such as text, video, color image, or sound.

References

[1] W. Ch. Alisawi, et.al., " Improvement of Classical Cipher Algorithm based on a New Model of Timed-Released Encryption", International Journal of Applied Engineering Research, Volume 14, Number 16 pp. 3531-3536, 2019.

[2] A. Upadhyay and N. Tiwari,"LSB and DES based Quad Tree Digital Watermarking", International Journals of Advanced Research in Computer Science and Software Engineering, Volume 8, Number 2, 2018.

[3] R. Singh, S. Singh, and N. Sharma, "A Review of Digital Watermarking Technique". International Journal of Computer Applications, 2015.

[4] D. Chopra, P. Gupta, B.C. Gaur Sanjay, and A. Gupta, "LSB Based Digital Image Watermarking For Gray Scale Image", Journal of Computer Engineering (IOSRJCE), Volume 6, number, pp. 36-41, 2012.

[5] A. Bamatraf, R. Ibrahim and M. N. M. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", Journal of Computing, Volume 3, Number 4, 2011.

[6] K. Joshi, R. Yadav and A. K. Yadav,"An Additive Watermarking Technique in Gray Scale Images Using Discrete Wavelet Transformation and Its Analysis on Watermark Strength", World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Volume 10, Number 7, 2016.

[7] N. Makbol, et.al, " Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics ", IET Image Processing, Volume 10, Number 1. pp. 34-52, 2016.

[8] K. A. Y. Ibrahim, "Utilization of Watermarking Techniques for Securing Digital Images", A Thesis Submitted for the Degree of Master of Engineering Science, Department of Computer Science and Engineering, Menoufia University Faculty of Electronic Engineering Department of Computer Science and Engineering, 2017.

[9] N. A. Loan, et.al., “Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption”, IEEE, Volume 6, pp. 19876 – 19897, 2018.

[10] A. Shehab, ET.AL.,” Secure and Robust Fragile Watermarking Scheme for Medical Images”, IEEE, 2018.

[11] M. Mamutli, S. kazan,"A Novel Digital Image Watermarking Scheme for Medical Image”, International Journal of Computer Science and Mobile Computing, IJCSMC, Volume 8, Number 4, pp.198 – 203, 2019.

[12] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, "Digital watermarking techniques and Trends”, Springer topics in signal processing ISBN 978-981-10-2095-7(ebook), 2017.

[13] Z. Ch. Oleiwi, K. thanoon, K. I. Alsaif, " High Frequency Coefficient Effect on Image Based on
Contourlet Transformation", 2019 international conference on computing and information science and technology and their applications (ICCISTA), IEEE, 2019.

[14] Z. Ch. Oleiwi, "Imp measuring the quality of watermarked image. Simulation results show that the quality of watermarked image act of Poisson parameter of Impulsive Multiplicative Noise on Impairment of Single-tone Sinusoid Signals ", Journal of Engineering and Applied Sciences, Volume 13, Number 18, pp.7630-7636, 2018.