Robust Digital Watermarking Based Falling-off-Boundary in Corners Board-MSB-6 Gray Scale Images

Mehemed Bashir Aliwa†, Tarek El-Ahmady El-Tobely†, Mahmood M. Fahmy†, Mohamed EL Said Nasr† and Mohamed Hashem Abd El-Aziz††
† Faculty of Engineering-TANTA University, Egypt.
†† Faculty of Computers & Information Sciences-Ain Shams University, Egypt.

Summary
Digital watermarking has been considered as a solution to the problem of copy protection in multimedia objects and many algorithms has been proposed. One of the problems in digital watermarking is that the three requirements of imperceptibility, capacity, and robustness that are must be satisfied but they almost conflict with each other. In this paper we propose a new digital watermarking technique in the spatial domain capable of embedding a totally indistinguishable in original image by the human eye. In addition by applying falling-off-boundary in corners board of cover image with the random pixel manipulation set of the most significant bit-6 (MSB 6) leads to undetectability, imperceptibility and increase robustness. Experimental results of the proposed scheme imperceptibility, undetectability and robustness against large blurring attacks measured by peak signal to noise ratio, normalized cross correlation and similarity function values showed a significant improvement with respect to a previous works.

Key words: Data hiding, digital watermarking, imperceptible, PSNR, laplace operator, LSB & MSB.

1. Introduction
In the last decade, an important research effort has been devoted to the development of techniques addressing the issue of digital data protection. Among them, Digital Watermarking has become the most efficient and widely used. Digital Watermarking refers to techniques that are used to protect digital data by imperceptibly embedding information (the watermark) into the original data in such a way that always remains present[12][16].

1.1 Overview of Digital Watermarking
Information hiding (or data hiding) is a general term encircling a wide range of problems beyond the embedding messages in content. The term hiding can refer to either for information imperceptibility (watermarking) or information secrecy (steganography). Watermarking and steganography are two important sub disciplines of information hiding that are closely related to each other and may be coincide but with different underlying properties, requirements and designs, thus result in different technical solutions[8][18]. Steganography is a term derived from the Greek words steganos, which means “covered,” and graphia, which means “writing.” It is the art of concealed communication. The existence of a message is secret[8][14][18]. Examples include invisible ink which would glow over a flame used by both the British and Americans to communicate secretly during the American Revolution and hidden text using invisible ink to print small dots above or below letters and by changing the heights of letter-strokes in texts used by German spies in World Wars[8].

The watermarking a term used back from paper watermarking, on the other hand has the additional concept of resilience against attempts to remove the hidden data. This is because the information hidden by watermarking systems is always associated to the digital object to be protected its owner, while steganographic systems just hide any information. Robustness criteria are also different since steganography mainly concerns with detection of hidden message while watermarking concerns potential removal by a pirate. Besides, steganography typically relates to covert point-to-point communication while watermarking is usually one-to-many[8][17]. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows[8] Text watermarking, Image watermarking, Audio watermarking and video watermarking as shown in Fig.1. A set of requirements should be met by any watermarking technique. The main requirements are perceptual transparency, payload of the watermark and robustness. Perceptual transparency refers to the property of the watermark of being imperceptible in the sense that humans can not distinguish the watermarked images from the original ones by simple inspection[15]. Capacity knowing how much information
1.2 Classification of Digital Watermarking

First: According to the domain for watermark embedding, spatial domain watermarking technologies as shown in Fig.1 change the intensity of original image or Gray levels of its pixels. This kind of watermarking is with low computing complexity, because no frequency transform is needed. However, there must be tradeoffs between invisibility and robustness, and it is hard to resist common image processing and noise[8][10], where several techniques have been proposed in spatial domain as the references[1]-[3][10]-[13] and in recent years they are becoming generally abandoned[15]. The advantage of the spatial domain methods is that their application is done very easily, and requires minimal computational power. Their possible disadvantage is that they do not allow exploitation of this subsequent processing in order to increase the robustness of the embedded watermark[9]. Frequency domain watermarking technologies as shown in Fig.1 embed the watermark into the transformed image. It is complicated but has the merits that the former approach lacks[10], where several techniques have been proposed in frequency domain as the references[5]-[8]. Feature domain methods first generation transform domain methods are applied blindly, regardless to the specific content of images. This makes them more prone to detection & attacks. The 2nd generation methods detect the feature points of each image, then based on these points the watermark is embedded adaptively on their local area. Embedding the watermark around the feature points makes these algorithms robust to various kinds of image manipulations like JPEG compression, geometric distortions and noise addition[9].

Second: According to the application and how watermark is detected and extracted, from Fig.1 shows the source-based and destination-based schemes. Where the Source based schemes focus on ownership identification/authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. An important constraint to consider for many source-based applications is the ability to detect the watermark without the original image. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer or end user. The destination-based watermark could be used to trace the end-user in the case of illegal use such as reselling. It is reasonable to assume that the content provider has the original image available for watermark detection in destination-based applications[11]. Blind extracting watermarking (also referred to as public or oblivious watermarking) means watermark detection and extraction do not depend on the availability of original image. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult. Non-blind extracting watermark (also called private watermarking) can only be detected by those who have a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships. Semi-blind watermarking (or called semiprivate watermarking) does not use the original data for detection, but answers the same question. Potential applications of private and semiprivate watermarking are for evidence in court to prove ownership, copy control in applications such as digital versatile disc (DVD) where the disc reader needs to know whether it is allowed to play the content or not, and fingerprinting where the goal is to identify the original recipient of pirated copies[10][17].

Third: according to the ability of watermark to resist attack, fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection[8][10].

1.3 Parameters of digital watermarking systems

There are a lot of parameters and variables in digital watermarking systems. Tradeoffs must be made between some of them. The most important ones are listed here[15]:
First: Quantum of information embedded, this important parameter is determined by the specific application and directly influences the robustness of the system. The more information inserted, the less robust the watermarking will be. Second: Watermark intensity, also known as the power of the embedded watermark. To increase the robustness, one may increase this parameter, but at the cost of the degradation of original image. Third: Size of watermark, Similar to its intensity, the larger the size of watermark is, the robust the system will be. It should be noted that watermark that is too small tend to have little value in real application. Forth: Control information though it has nothing to do with the invisibility or robustness of the watermarking system, the control information, for example, the key used to rearrange the watermark before embedding it, plays an important role in system security. Good overviews on the state of the art of classical watermarking techniques can be found in the recent textbooks[16]-[19]. The paper is organized as follows. Section 2 describes the principle of previous works. In section 3 describes the performance evaluation of watermarking system. Section 4 describes the proposed method insertion and extraction of watermarking. Experimental of performance results are given in section 5. Finally, Section 6 conclusion and future work.

### 2. Previous Methods

The principle of previous methods of related works in spatial domain the ciphers can be embedded into a general, natural image, hackers would be misdirected. This method is called data hiding. Image hiding techniques mainly deal with a secret image embedded with in a cover image to get a Stego-image. This Stego-image conceals hidden data without advertising that it is hiding anything. One common method is called Least Significant Bit (LSB)[17][12][17]. LSB replaces a cover-image directly, after hiding a secret image within it. In general, bit-mapped images are commonly used. Every image is comprised of pixels, and each pixel indicates one color. If an image is shown in gray-scale, with a range of values from 0 to 255, lower values signify darkness, and higher values, lightness. Therefore, a gray-level image can be adjusted by adjusting the values. At least 8 bits are required to represent these values, and the binary system stores them from the most signification bit to the least signification bit of Least Significant Bit Substitution Technique in Digital Watermarking[1]. The first replaces the LSB of the image with an m-sequence while the second adds the m-sequence to the LSB of the image and uses auto-correlation to detect it later on[13]. Anther method the authors using the LSB [3] of the cover for embedding the message, LSB has been used to increase the robustness, where the authors using the (LPAP) local pixel adjustment process LSB_{1,2} to modified according to the bit of the message, to minimize the difference between the cover and the stego-cover. For more protection to the message bits a stego-Key has been used to permute the message bits before embedding it[3]. Anther method the authors using LSB technique based on manipulating[2] to be embedded into the k-rightmost LSBs of the cover-image where k=1, 2, ... ,5, and applying an optimal pixel adjustment process (OPAP) to the stego-image to enhance the image quality of the stego-image[2]. Anther method the authors proposed, "Robust and Blind Spatial Watermarking in Digital Image"[10], using watermark insertion process exploits average brightness of the homogeneity regions of the cover image by spatial mask of suitable sizes is used to hide data with less visual impairments, by cover image is partitioned into non-overlapping square blocks of size(8x8) pixels. A block is denoted by the location of its starting pixel (x, y). If the cover image is of size (N x N), total (N/8 x N/8) number of such block is obtained for watermark insertion and calculated all such blocks are arranged in ascending order based on their variance statistical average values of the block, where the blocks having low variance (zone) values called as homogenous blocks, Where one pixel from watermark replaces a particular bit of Least Significant Bit planes in bit plane representation of block for each homogenous block and inserting the value of bit position selected for different homogenous block located in the '1' position of the secret image. This positional information as gray value of the secret image helps to extract watermark pixel from the homogenous block[10]. Anther method the authors using the Least Significant Bit Substitution Technique in Digital Watermarking[1], study presents the results of implementing a Least Significant Bit (LSB) digital watermarking system to investigation the digital watermarking is used by those who wish to prevent others from stealing their material. LSB substitution is not a very useful in the art of steganography, due to its lack of robustness. LSB embedded watermarks can be easily recovered and even altered by an attacker. It would appear that LSB will remain in the domain of steganography due to its useful nature and its overall capacity of information[1].
3. Performance Evaluation of Watermarking System

3.1 Imperceptibility:

Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark[5]. Developers and implementers of watermarking image need a standard metric to measure the quality of watermarking images compared with the original image or called (cover image). A common measure used of the quality of a watermarked image, the Mean square error (MSE) and Peak signal to noise ratio (PSNR) is typically used. It is familiar to workers in the field, it is also simple to calculate, but it has only a limited, approximate relationship with the perceived errors noticed by the human visual system. This is why higher PSNR values imply closer resemblance between the watermarked image and the original images. Denoting the pixels of the original image by F(i,j) that contains (M by N) pixels represent the size of image and the pixels of the image watermarking image by \( f(i,j) \), where \( f \) is reconstructed watermarking image by decoding the encoded version of \( F(i,j) \) original image. Error metrics are computed on the luminance value only so the pixel values \( f(i,j) \) range between black (0) and white (255). We define error metrics as[17][20]:

**First:** define the mean square error (MSE) between the two images as Eq(1) [17]:

\[
MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (F_{i,j} - f_{i,j})^2
\]  

(1)

The summation is over all pixels. The root mean squared error (RMSE) is the square root of MSE.

**Second:** define the Peak signal to noise ratio (PSNR) [17]. For images with 255 gray levels, as Eq(2):

\[
PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) dB
\]  

(2)

OR, PSNR are described computed by using Eq(3) as:

\[
PSNR = 20 \log_{10} \left( \frac{255}{RMSE} \right) dB
\]  

(3)

For a grayscale image with eight bits per pixel, the numerator is 255. For color images, only the luminance component is used. The typical PSNR values range between 20 and 40[19]-[21]. Some definitions of PSNR use Eq(2) rather than Eq(3). Either formulation will work because we are interested in the relative comparison, not the absolute values. For our proposal we will use the definition given above in Eq(3).

3.2 Detection:

a) **Discrete Laplacian Operator:** The watermarking image that obtained embedded watermark image hides in grayscale of cover original image called (digital watermarking image) by simply storing one bit of information in the LSB or MSB of every cover-pixel of original image. By using the discrete laplacian operator[11] or called discrete laplace operator filter[17] can detect (watermark or messages) in grayscale images, an image \( f(i,j) \) is represented by a \((i,j)\) matrix defined as[17]:

\[
\nabla^2 f(i,j) = f(i+1,j)+f(i-1,j)+f(i,j+1)+f(i,j-1)-4f(i,j)
\]

(4)

Where \( \nabla^2 f(i,j) \) is not defined for boundary pixels. That is, for an MxN image, \( \nabla^2 f(i,j) \) is not defined for \( i=0 \) or for \( j=0 \), nor for \( i=M-1 \) or \( j=N-1 \). (Keep in mind that a MxN image is interpreted as a MxN matrix. However the indexing goes left to right, from 0 to M-1, in the horizontal direction, and top to bottom, from 0 to N-1, in the vertical direction[11]. Evaluating above equation at every point \( (i,j) \) gives the "Laplace filtered" image. Since we can expect neighboring pixels to have a similar color, the histogram of \( \nabla^2 f(i,j) \) is tightly clustered around zero. Since the embedding process adds noise to the picture, which is statistically quite different from true random noise, the new histogram differs extremely. Laplace filtering prove the existence provide strong evidence that the picture was subject to modifications.

b) **Construction Technique:** The construction technique measured for displaying errors is to construct an error image which shows the pixel-by-pixel errors to find which pixel that embedded the watermark. The simplest computation of this image is to create an image by taking the difference between the reconstructed and original pixels. These images are hard to see because zero difference is black and most errors are small numbers which are shades of black. The typical construction of the error image multiples the difference by a constant to increase the visible difference and translates the entire image to a gray level \( T_e \). The computation is defined as :

\[
E_r (i,j) = 2 \left[ F(i,j) - f(i,j) \right] + T_e
\]

(5)

You can adjust the constant \( T_e=2 \) or the translation 255 to change the image, where 255 is white to signify no error and difference from white as an error which means that darker pixels are bigger errors \( E_r (i,j) \). Has been chosen adjust the constant for each bits as \( T_e=LSB_1=2 \), \( LSB_2=4 \), \( LSB_3=8 \), \( LSB_4=16 \), \( MSB_1=32 \), \( MSB_2=64 \), \( MSB_3=128 \) and \( MSB_4=256 \) for these translation to change the image.

3.3 Robustness:

Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, internationally or
unintentionally, by different types of digital signal processing attacks\cite{15}. We will report on robustness results which we obtained of major attacks: Gaussian noise, Salt & Pepper noise, altered image, drawing image, image cropping, changing in lower order bit manipulation of gray values and lossy data compression like JPEG. They are good representatives of the more general attacks. That is the Gaussian and Salt & Pepper noise are a watermark degrading attacks, altered and drawing image are a watermark removal attacks and cropping is a watermark disposition geometrical attack. We measured the similarity between the original watermark $W(i,j)$ and the watermarked extracted $W'(i,j)$ from the attacked image, whereas the similarity values $NCC$ and $SM$ of about 0.75 or above is considered acceptable.

a) Normalized Cross Correlation:
The quantitative estimation for the quality of extracted watermark image $W'(i,j)$ with reference to the original watermark $W(i,j)$ can be expressed as normalized cross correlation gives maximum value of (NCC) as unity defined as\cite{17}:
\[
NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (W(i,j) \cdot W'(i,j))}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{M} W(i,j)^2 \cdot \sum_{i=1}^{N} \sum_{j=1}^{M} W'(i,j)^2}}
\]

b) Similarity Function:
Function similarity estimation between extracted watermark $W'(i,j)$ and original watermark $W(i,j)$ is computed by the following formula\cite{15}:
\[
SM = 1 - \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (W(i,j) - W'(i,j))^2}{\sum_{i=1}^{N} \sum_{j=1}^{M} W(i,j)^2}
\]
If the result is larger than some determined threshold, we consider the extracted watermark $W'(i,j)$ as equal original watermark $W(i,j)$.

4. The Proposed Method
In this paper we shall propose a new image digital watermarking by applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSBs of cover image is developed to improve the quality of embedding results, undetectability and robustness. Whereas the bitmap watermark insertion process needs the secret Key1 to determine the number of frames per row in watermark and secret Key2 to changing the pixels of watermark depending on the number of frames per row determined by secret Key1.

Setp1:
In the proposed scheme, one watermark pixel is inserted in each of falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSBs. Before insertion as shown in Fig.2, will using secret key for spatial dispersion of the watermark to changing pixels as the following below:

First: Reads the indexed of watermark $W$ into X. From the indexed identify the size of matrix $X[\cdot,\cdot]$ in separate variables $W$ and $L$ number of pixels of watermark as shown in Fig.2.
Second: Secret Key1 using to determine the number of frames per row, where the Key1 chosen the dimension number divided by the frame number without remainder as Eq(1) and Eq(2).

\[
m = \text{width (w)} / \text{number of frames (Key1)} \quad (1)
\]
\[
n = \text{length (l)} / \text{number of frames (Key1)} \quad (2)
\]

Third: Define the indexed identify the size of new matrix $Y[\cdot]$ for the arranging and changing pixels of watermark and then using Key2 to generate the random permutation of the integers depending on the number of Secret Key1 as:

\[
\text{Key2} = (1: \text{number of frames per row (Key1)}) \quad (3)
\]

Four: Generate two loops \{i, j\} to selecting a frames by secret Key1 from indexed identify the size of matrix $X[W, L]$ and by defined the indexed identify the size of new matrix $Y[\cdot]$ to changing pixels of watermark depending on the secret Key2 as the algorithm below, shown in Fig.2:

Algorithm:
For i=1 to Secret Key1 do
For j=1 to Secret Key1 do
Selecting the frames from indexed identify the size of matrix $X[W, L]$ by Secret Key1 in to matrix $[WK]$. Where $W$ is the size of drawbacks $[T, U]$.

\[
WK = (X[(i-1)*m+1:i*m,(j-1)*n+1:j*n]) \quad (4)
\]
From Eq(4) by arranging the frames of pixels by using Secret Key2 to changing the selecting frames in the new image $Y[\cdot]$ as Eq(5):

\[
Y[(Key2(i-1)*m+1:Key2(i)*m,Key2(j-1)*n+1:Key2(j)*n)]=WK
\]

Five: For more robustness in digital watermarking applying drawbacks of the payload of watermark in the falling-off-boundary in corners board are placed in more than one place in the cover image to prevent the blurring attacks to alter it and can not defeat the purpose, as the algorithm below:

For ii=1 to T do
For jj=1 to U do

\[
\text{Drawback}(ii,jj)=\text{payload}(\text{mod}(ii,T)+1,\text{mod}(jj,U)+1);
\]

Where is the size of drawbacks $[T, U]$.

Setp2:
In this paper, the cover image is of size $[M, N]$ 512*512 gray level image has been used. So we can hide a payload of
watermark up to 2044 bits (256 bytes). We embedded the payload of watermark in falling-off-boundary in corners board of cover image with random pixel manipulation between boundary corners board set of the MSB6.

Lets have the drawbacks payload bits set of the $WL_{(i,j)}$, the maximum bits can be embedded $1 \leq T \times U \leq 2044$ bits, whereas the size of $WL=[T,U]$ and $T=U$. Let's have the cover image $F=\{pixel_0, pixel_1, \ldots, pixel_{264144}\}$. So, has been determine the pixels of falling-off-boundary in corners board of cover image employed as a sequence number $k_1, k_2, k_3, k_4$ where $k_1=1,2,\ldots,N$, $k_2=1,2,\ldots,N$, $k_3=2,3,\ldots,M-1$, and $k_4=2,3,\ldots,M-1$, then employed sequence number $G$ to manipulation of pixel between boundary corners board in cover image where $1 \leq G \leq 4$, as the following embedding algorithm shown in Fig.2:

**Embedding Algorithm:**
For $ii = 1$ to size of drawback
For $jj = 1$ to size of drawback
if $G==1$
if $k_1 <= N$
Get the corner pixel in falling-off-boundary board when $F(1, k_1)$ and set bit of the MSB6

Then $f(1, k_1) = Embedded the payload of watermark bit $WL_{(i,j)}$ to MSB6 of the pixel $F(1, k_1)$

$k_1=k_1+1$;

$}$

if $G==2$
if $k_2 <= N$
Get the corner pixel in falling-off-boundary board when $F(M, k_2)$ and set bit of the MSB6

Then $f(M, k_2) = Embedded the payload of watermark bit $WL_{(i,j)}$ to MSB6 of the pixel $F(M, k_2)$

$k_2=k_2+1$;

$}$

if $G==3$
if $k_3=\neq M$
Get the corner pixel in falling-off-boundary board when $F(k_3, 2)$ and set bit of the MSB6

Then $f(k_3, 2) = Embedded the payload of watermark bit $WL_{(i,j)}$ to MSB6 of the pixel $F(k_3, 2)$

$k_3=k_3+1$;

$}$

if $G==4$
$G=0$;
if $k_4=\neq M$
Get the corner pixel in falling-off-boundary board when $F(k_4, N)$ and set bit of the MSB6

Then $f(k_4, N) = Embedded the payload of watermark bit $WL_{(i,j)}$ to MSB6 of the pixel $F(k_4, N)$

$k_4=k_4+1$;

$}$

$G=G+1;$

$}$

From above algorithm of the falling-off-boundary in corners board in cover image with random pixel manipulation between boundary corners board set of the MSB6 in each pixel to protect the payload of watermark. Which are employed by sequence number? This sequence of indexes used to permute the payload of watermark bits as shown in Fig.2. The embedding process is very easy to achieve the low complexity time, which is only replace the permuted bits of the payload of watermark by the MSB6 set of the
falling-off-boundary in corners board of cover image with random pixel manipulation between boundary corners board obtain the new digital watermarking \( f(M, N) = \{\text{newpixel}_0, \text{newpixel}_1, \ldots, \text{newpixel}_{2^{44144}}\} \).

**Step3:**
Reconstruct the watermark using to extracted watermark bits from drawbacks in falling-off-boundary in corners board of digital watermarking \( f(M, N) \) by using inverse the same procedure of embedded algorithm and sequence number G to know the manipulation pixel between boundary corners board in digital watermarking \( f(M, N) \) and then select one of drawbacks set of MSB 6, after extracted watermark required the secret Key 1,2 to arranging the change of frames per row, then watermark in original form is thus obtained. This completes watermark extraction process.

A quantitative estimation for the quality of extracted watermark image \( W(i,j) \) under inspection with or without external attacks by compared with the original watermark \( W(i,j) \) as reference can be expressed as normalized cross correlation and similarity function.

### 5. Performance Results

In order to compare the performance results of the proposed watermarking scheme in falling-off-boundary in corners board of cover image, with the An investigation into the use LSB substitution in digital watermarking[1], Robust and Blind Spatial Watermarking in Digital Image by insertion process exploits average brightness of the homogenous blocks of the cover image[10], Hiding data in images by simple LSB substitution with applying OPAP[2], Hiding data using LSB-3 with modified LSBi, by applying LPAP[3] and embedding watermark by simple MSB substitution. A set of standard grayscale image, ‘Lena’ (512 × 512) gray level image has been used as a cover image as shown in Fig. 3(a) and payload logo watermark 45x45 shown in Fig. 4(a). For grayscale image each pixel has a value between 0 and 255. The image is broken down into coordinates and pixels.

In Least Significant Bit (LSB) substitution, the least significant bit is changed because this has little effect to the appearance of the carrier payload of watermark as shown in Fig.3(b, c, d, e, f, g, h and i) for example(10000000)2, the grayscale pixel bit size is 128. This shows that the grayscale image would change significantly if there were any other bit changed than the LSB. It changes more and more the closer you get to the MSB. When the LSB is changed, the pixel bit value changes from \( (10000000)_2 \) to \( (10000001)_2 \), which is undetectable with the human eye. With the MSB changed, the pixel bit value changes from 128 to newpixel\( = (00000000)_2 \), 0, which makes a significant change to the grayscale view. The theory is that if you take two grayscale images, and change the LSB of image pixel\( = (10000000)_2 \) to the LSB of image pixel\( = (10000001)_2 \) for each coordinate or pixel, image pixel\( = (10000000)_2 \) will be hidden in image pixel\( = (10000000)_2 \).

![Fig.3 Grayscale images and their 8 corresponding bit planes (from left to right, original images, LSB1,..., and LSB8 & MSB5,..., and MSB8, respectively).](image)

On the other hand, embedding payload of watermark directly in bit planes will cause visible damages to the edges in the bit planes MSB\( _5,6,7,8 \) as shown in Fig.3(f, g, h, i). To overcome this difficulty, from Fig.3 (f, g, h, i) see a visible watermark makes slight modifications to an image. The transformation is such that the image can still be seen, but the watermark is effectively laid over the top of it, in this paper we proposed a new image digital watermarking applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSBi, of cover image leads to imperceptibility, undetectability and increase the robustness.

#### 5.1 Imperceptibility:

To measure and compare between the previous methods[1]-[3][10]. We evaluated imperceptibility to sense the degree of distortion resulting from pixel value changes in digital watermarking image \( f(M, N) \) by measuring PSNR as shown the variation in Table 1.

<table>
<thead>
<tr>
<th>Methods</th>
<th>PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding watermark by simple LSBi [1]</td>
<td>51.14</td>
</tr>
<tr>
<td>Embedding watermark by simple LSBi [1]</td>
<td>45.13</td>
</tr>
<tr>
<td>Embedding watermark by simple LSBi [1]</td>
<td>39.11</td>
</tr>
</tbody>
</table>

Table 1: The results of PSNR comparison between previous methods
Embedding watermark by simple LSB\textsubscript{4} \cite{1} 33.09
Embedding watermark by simple MSB\textsubscript{5} 27.03
Embedding watermark by simple MSB\textsubscript{6} 21.03
Embedding watermark by simple MSB\textsubscript{7} 14.98
Embedding watermark by simple MSB\textsubscript{8} 9.04
Embedding watermark by simple MSB\textsubscript{8} 9.04
Embedding watermark by simple LSB using OPAP\textsubscript{2}(k=1) substitution\cite{2} 51.40
Embedding watermark by simple LSB using OPAP\textsubscript{2}(k=3) substitution\cite{2} 40.69
Robust and blind spatial watermarking using homogenous blocks embedding in (LSB substitution)|\cite{10} 41.61
Embedding watermark by simple LSB\textsubscript{3} with modified LSB\textsubscript{1,2} by LPAP\cite{3} 42.29
Proposed method by set of the MSB\textsubscript{8} 42.29
Proposed method by set of the LSB\textsubscript{3} 60.21

Fig.3 (a) show "Lena" image used as cover image and Fig.4 (a) show the watermark image using logo/hidden and Fig.4 (b) show the digital watermarking image of proposed method. From the comparison in Table 1 show the proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSB\textsubscript{8} the PSNR=42.29 dB and 60.21dB by set of the LSB\textsubscript{3}, it is high quality with compared by previous methods. Where the typical PSNR values range between 20 and 40, where higher is better for quality image\cite{16}|\cite{19}-|\cite{21}. The PSNR of the digital watermarking image to the original image is obtained 42.290 dB of proposed method, where the quality degradations could hardly be perceived by human eye, so this is the prove imperceptibility of our proposed.

Fig.4 (a) Logo watermark. (b) Digital watermarking.

| 5.2 Detection |

\textbf{a) - Discrete Laplacian Operator:}
\textbf{First:} Let us look at the embedding payload watermark by using simple LSB substitution as shown in Fig.3 (b, c, d, e) and simple MSB substitution as shown in Fig.3 (f, g, h and i) methods, by using Discrete Laplacian Operator filter of each bit plane as shown in Fig.5 will see the simple LSB substitution methods the midrange of the histogram of the discrete Laplacian of original image as shown in Fig.5 (a), it is the same shape of discrete Laplacian range of a digital watermarking in LSB\textsubscript{2,3,4} methods, but small variation of magnitude and with gray level color variation, the discrete Laplacian range of a digital watermarking in LSB\textsubscript{1} method as shown in Fig.5 (a and c), compared with discrete Laplacian range of original image shows humps every values. This is because the LSB\textsubscript{1} have been affected. The LSB\textsubscript{1} method of digital watermarking image is not as correlated as the discrete Laplacian range of original image. Therefore when we replace the LSB\textsubscript{1,2,3,4} of the cover image of the embedded payload of watermark image, under the simple LSB method , we see that the LSB of the resulting digital watermarking image have the wrong statistical signature as shown in Fig.5 (a), where the embedding process of payload watermark adds noise to the picture, which is statistically quite different from true random noise, the new histogram differs extremely. Laplacian filtering the existence of a secret watermark embedded.

Let us look at the simple MSB substitution methods the midrange of the histogram of the discrete Laplacian filter of cover image as shown in Fig.6 (a), it is not the same shape of discrete Laplacian filter of a digital watermarking in MSB\textsubscript{5,6,7,8} methods with compared by discrete Laplacian filter of original image, there are big variation of magnitude and with gray level color variation, the discrete Laplacian filter range of a digital watermarking in MSB\textsubscript{7} methods as shown in Fig.6 (c, d, e and f) have been affected, where the embedding process of payload watermark adds big noise to
the picture. Which are statistically quite different between the embedding processes of watermark in each MSB?

Second: From the above methods of the simple LSB & MSB substitution methods are detected by the discrete Laplacian filter as shown in Fig.(5 and 6), we proposed watermarking scheme in falling-off-boundary in corners board of cover image to investigation the LSB substitution methods is not a very good candidate for digital watermarking where the attacker can be flip one LSB and the watermark cannot be recovered, so from the simple LSB & MSB substitution methods embedded watermarks can be easily detected by the discrete Laplacian filter. So that by applying proposed method falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB1,2,3,4, it is undetectability by the discrete Laplacian filter, to prove this we implemented the algorithms by using the simple LSB & MSB methods to show our proposed methods are imperceptibility, where are high quality PSNR = 72.24dB at LSB1 and 29.80dB at MSB8 as shown in the Table 2 with compared by the simple LSB & MSB substitution methods and undetectability by the discrete Laplacian filter for each bit planes.

<table>
<thead>
<tr>
<th>Bit planes</th>
<th>Proposed method set of the bit planes PSNR (dB)</th>
<th>Simple LSB &amp; MSB substitution PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB1</td>
<td>72.24</td>
<td>51.14</td>
</tr>
<tr>
<td>LSB2</td>
<td>66.35</td>
<td>45.13</td>
</tr>
<tr>
<td>LSB3</td>
<td>60.21</td>
<td>39.11</td>
</tr>
<tr>
<td>LSB4</td>
<td>54.45</td>
<td>33.09</td>
</tr>
<tr>
<td>MSB5</td>
<td>48.46</td>
<td>27.03</td>
</tr>
<tr>
<td>MSB6</td>
<td>42.29</td>
<td>21.03</td>
</tr>
<tr>
<td>MSB7</td>
<td>36.21</td>
<td>14.98</td>
</tr>
<tr>
<td>MSB8</td>
<td>29.80</td>
<td>9.04</td>
</tr>
</tbody>
</table>

Fig.7 Detection of histograms discrete laplacian operator filter compared between the cover image and digital watermarking image using proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB1,2,3,4, where the (X axis) the magnitude of the formula $\nabla^2 f(i, j)$ increases with the (Y axis) gray level color variation. (a) Histogram Laplacian filter comparison between cover image and different embedded watermark in MSB5,6,7 methods. (b) Histogram Laplacian filter of cover image. (c) Histogram Laplacian filter embedded watermark in MSB5. (d) Histogram Laplacian filter embedded watermark in MSB6. (e) Histogram Laplacian filter embedded watermark in MSB7. (f) Histogram Laplacian filter embedded watermark in MSB8.

Fig.8 (a, b, c, d and e) see the undetectability by using the discrete Laplacian filter for each bit planes (LSB1,2,3,4 & MSB5,6,7) where the same range magnitude of the formula $\nabla^2 f(i, j)$ and the same gray level color variation. But in MSB8 as shown in Fig.8 (a and f) have been affected, where the embedding process of payload watermark adds noise to the picture. Which are statistically quite different between the embedding processes of payload watermark in MSB8.
Fig.8 Detection of histograms discrete laplacian operator filter compared between the original image and digital watermarking image using proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSB1,2,3,4, where the (X axis) the magnitude of the formula $\nabla^2 f(i, j)$ increases with the (Y axis) gray level color variation. (a) Histograms Laplacian filter comparison between cover image and different embedding watermark in MSB5,6,7,8 methods. (b) Histogram Laplacian filter of cover image. (c) Histogram Laplacian filter embedding watermark in MSB5. (d) Histogram Laplacian filter embedding watermark in MSB6. (e) Histogram Laplacian filter embedding watermark in MSB7. (f) Histogram Laplacian filter embedding watermark in MSB8.

### b) Construction Technique:

**First:** Let us look at the simple LSB & MSB substitution methods using the construction technique measured for displaying errors "Er" is to construct an error image which shows the pixel-by-pixel errors to find which pixel that embedding watermark. so from Fig.9 (a, b, c, d, e, f, g and h) show the errors "Er" have been affected, where the embedding process of payload watermark adds noise to the picture. Which are quite different between the embedding processes of payload watermark in each bit planes (LSB and MSB).

**Second:** From the simple LSB & MSB substitution methods are detected by evaluated the construction technique as shown in Fig.9 (a, b, c, d, e, f, g and h). We evaluated construction technique of the proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB1,2,3,4 and MSB5,6 have been undetectability as shown in Fig.9 (i).

### 5.3 Robustness:

We evaluated robustness of the proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB1,2,3,4 and MSB5,6 under major digital signal processing operations (attacks): Gaussian noise, Salt & Pepper noise, image Drawing, image cropping and altered image. They are good representatives of the more general attacks. We measure the similarity between the original watermark and the watermark extracted after applying attacks by NCC and SM, whereas the similarity values NCC and SM of about 0.75 or above is considered acceptable. The Table 3 showed the proposed method set of MSB8 with deferent burring attacks.

<table>
<thead>
<tr>
<th>Extracted watermark from proposed method set of the MSB under:-</th>
<th>NCC</th>
<th>SM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ideal condition</td>
<td>0.999</td>
<td>0.991</td>
</tr>
<tr>
<td>Gaussian noise attack.</td>
<td>0.978</td>
<td>0.977</td>
</tr>
<tr>
<td>Salt &amp; Pepper noise attack.</td>
<td>0.993</td>
<td>0.991</td>
</tr>
<tr>
<td>Drawing image attack.</td>
<td>0.999</td>
<td>0.991</td>
</tr>
<tr>
<td>Image cropping attack.</td>
<td>0.999</td>
<td>0.991</td>
</tr>
<tr>
<td>Altered image</td>
<td>0.999</td>
<td>0.991</td>
</tr>
<tr>
<td>Changing in lower order bit manipulation of gray values (all LSB)</td>
<td>0.999</td>
<td>0.991</td>
</tr>
<tr>
<td>JPEG compression</td>
<td>0.777</td>
<td>0.778</td>
</tr>
</tbody>
</table>

a) Experiment results under Gaussian noise attack:
The Gaussian noise is a watermark degrading attack, where are add noise can be used as an attack to remove the watermark. In this experiment we add Gaussian noise to the digital watermarking image as shown in Fig.10 (a), and then try to extract the watermark as shown in Fig.10 (b, c, d, e, f
and g) and compute the normalized cross correlation NCC & similarity SM.

![Fig. 10: a) Digital watermarking image added Gaussian noise. b) Extracted watermark form proposed method set of the LSB 1 c) Extracted watermark form proposed method set of the LSB 2 d) Extracted watermark form proposed method set of the LSB 3 e) Extracted watermark form proposed method set of the MSB 4 f) Extracted watermark form proposed method set of the MSB 5 g) Extracted watermark form proposed method set of the MSB 6 Results are shown in Fig. 10 (b, c, d, e, f and g) and Table 4 shown the PSNR obtained after add noise, as seen by applying proposed method of set the MSB 6, we extracted watermark and compute the NCC=0.978664 and similarity=0.977758. The results show the proposed method deals with Gaussian noise excellently and good robustness. The extracted watermark can maintain a good similarity with the original one even after the watermarked image is adding Gaussian noise as shown in Fig.10 (g).

![Table 4: Measuring extracted watermark under Gaussian noise attack]

<table>
<thead>
<tr>
<th>Proposed method set of the bit planes</th>
<th>PSNR(dB) After add Gaussian noise</th>
<th>NCC</th>
<th>SM</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB 1</td>
<td>49.12</td>
<td>0.515770</td>
<td>0.527140</td>
</tr>
<tr>
<td>LSB 2</td>
<td>48.27</td>
<td>0.702226</td>
<td>0.715284</td>
</tr>
<tr>
<td>LSB 3</td>
<td>45.92</td>
<td>0.857143</td>
<td>0.856349</td>
</tr>
<tr>
<td>LSB 4</td>
<td>41.53</td>
<td>0.933210</td>
<td>0.930623</td>
</tr>
<tr>
<td>MSB 5</td>
<td>36.01</td>
<td>0.967532</td>
<td>0.967982</td>
</tr>
<tr>
<td>MSB 6</td>
<td>29.76</td>
<td>0.978664</td>
<td>0.977758</td>
</tr>
</tbody>
</table>

b) Experiment results under Salt & Pepper noise attack: The Salt & Pepper is a watermark degrading attack; in this experiment we add Salt & Pepper noise to the digital watermarking image as shown in Fig. 11 (a), and then extracted the watermark as shown in Fig. 11(b, c, d, e, f and g) and compute NCC & similarity SM.

![Fig. 11 a) Digital watermarking image add Salt & Pepper noise. b) Extracted watermark for proposed method set of the LSB 1 c) Extracted watermark for proposed method set of the LSB 2 d) Extracted watermark for proposed method set of the LSB 3 e) Extracted watermark for proposed method set of the MSB 4 f) Extracted watermark for proposed method set of the MSB 5 g) Extracted watermark for proposed method set of the MSB 6 The results are shown in Fig. 11(b, c, d, e, f and g) and Table 5 shown the PSNR obtained after adds noise. The proposed method set of the MSB 6, we extracted watermark, where the NCC = 0.993506 and similarity = 0.991210. The results show the proposed method deals with Salt & Pepper noise excellently and more robustness with compared by added Gaussian noise as

![Table 5: Measuring extracted watermark under Salt & Pepper noise]

<table>
<thead>
<tr>
<th>Proposed method set of the bit planes</th>
<th>PSNR(dB) After add Salt &amp; Pepper noise</th>
<th>NCC</th>
<th>SM</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB 1</td>
<td>22.53</td>
<td>0.987941</td>
<td>0.988858</td>
</tr>
<tr>
<td>LSB 2</td>
<td>22.46</td>
<td>0.988868</td>
<td>0.991170</td>
</tr>
<tr>
<td>LSB 3</td>
<td>22.55</td>
<td>0.989796</td>
<td>0.988879</td>
</tr>
<tr>
<td>LSB 4</td>
<td>22.56</td>
<td>0.991651</td>
<td>0.990733</td>
</tr>
<tr>
<td>MSB 5</td>
<td>22.59</td>
<td>0.986085</td>
<td>0.989303</td>
</tr>
<tr>
<td>MSB 6</td>
<td>22.57</td>
<td>0.993506</td>
<td>0.991210</td>
</tr>
</tbody>
</table>

c) Experiment results under image drawing attack: The image drawing is a removal attack; in this experiment we add Salt & Pepper noise to the digital watermarking image as shown in Fig.11 (a), and then extracted the watermark as shown in Fig. 11(b, c, d, e, f and g) and compute NCC & similarity SM.

![Fig. 12 a) Drawing in digital watermarking image. b) Extracted watermark for proposed method set of the LSB 1,2,3,4 & MSB 5,6 d) Experiment results under image cropping attack:]

d) Experiment results under image cropping attack:
The image cropping is a disposition geometrical attack; in this experiment we crop the digital watermarking image as shown in Fig.13 (a), and extracted the watermark as shown in Fig.13 (b), then compute NCC & similarity SM. The results are shown in Fig.13 (b) by applying proposed method falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB$_{1,2,3,4}$ and MSB$_{5,6}$, where the NCC=0.993 and similarity 0.991. The results show the proposed method high robustness.

![Fig. 13: a) Cropping the digital watermarking image. b) Extracted watermark for proposed method set of the LSB$_{1,2,3,4}$ & MSB$_{5,6}$](image)

e) Experiment results under altered image attack:
The altered image attack a removal attack, where the extraction/detection process for still image is presented. In this experiment we altered image of the digital watermarking image as shown in Fig.14 (a and b), and extracted the watermark as shown in Fig.14 (c), then compute NCC & similarity SM. The results are shown in Fig.14 (c) by applying proposed method falling-off-boundary in corners board of cover image with random pixel manipulation set of the LSB$_{1,2,3,4}$ and MSB$_{5,6}$, where the NCC=0.993 and similarity 0.991. The results show the proposed method high robustness of watermark.

![Fig. 14: a) Digital watermarking image. b) Altered image of digital watermarking. c) Extracted watermark for proposed method set of the LSB$_{1,2,3,4}$ & MSB$_{5,6}$](image)

f) Experiment results under changing in lower order bit manipulation of gray values:
If the attacker knows that the image has watermark embedded, then the attacker would only have to replace all LSB bits with a '1' fully defeating the effects and the watermark cannot be recovered from LSB$_{1,2,3,4}$. So that the proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSB$_{6}$ to prevent the attacker to detect or replacing bit, where the PSNR obtained after changing in lower order bit LSB$_{1,2,3,4}$= 31.48dB and then extracted watermark, measured by NCC=0.993 and similarity 0.991 get high robustness.

g) Experiment results under JPEG compression:
Image files on the internet are usually compressed by JPEG standard in order to reduce the file size and save limited bandwidth. As a result, digital watermarking algorithms should be robust under JPEG compression called unintentionally attack. In this experiment, the digital watermarking image "Lana" is compressed by JPEG standard, where the PSNR obtained after compression=35.87dB. The proposed method applying falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSB$_{6}$, the watermark can be well detected and extracted, where are moderate robustness by measuring the NCC=0.777365 and similarity SM=0.77808.

6. Conclusion and Future Work

Digital watermarking is used by those who wish to prevent others from stealing their material. The proposed technique describes a new digital watermarking technique robust and oblivious digital watermarking image in spatial domain, our method of embedding watermark in falling-off-boundary in corners board of cover image with random pixel manipulation set of the MSB$_{6}$, it is high quality with compared by previous works as shown in Table 1 where increasing the PSNR=42.29 dB leads to provide imperceptibility "high secret digital watermarking image", undetectability under applying " Discrete Laplacian Operator filter & Construction Technique ", whereas increasing high robustness with applying degrading attack and removal attack, disposition geometrical attack, altered image attack and changing in lower order bit manipulation of gray values by attacker, and moderate robustness under lossy data compression JPEG called unintentionally attack, where the embedding process is very easy achieved the low complexity time. So that the attacker cannot notices the difference between the digital watermarking image and the original cover. Also, we are investigating and prove the LSB substitution is not a very good candidate for robustness digital watermarking, but it is very useful in the fragile watermarking, due to its lack of robustness. The fragile watermarks are used to detect any corruption of an image, whereas the LSB embedded watermarks can easily be removed using techniques that do not affect the image visually to the point of being noticeable. Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness.
Further research works may be carried out in spatial domain watermarking to generate:
1. Applying proposed method on the color image to achieve increasing the capacity and higher robustness.
2. Fragile digital watermarking image by applying proposed method to set of LSB imperceptibility and undetectability to achieve data authentication.
3. Higher robustness by applying proposed method to set of MSB with modifying LSB & MSB according to the bit of the watermark to enhance the quality of digital watermarking image may be using LPAP or OPAP to achieve robustness against other types of external attacks and high robustness under JPEG compression.

References