ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.30; No.2.| 2022

A Non-Blind Image Watermarking Method for Copyright Protection

Sheimaa A. Hadi[1] Suhad A Ali[2] Majid Jabbar Jawad[3]

[1]Department of Computer Science, College of Science for Women, Babylon University ,Iraq.
shaymaa.hadi@student.uobabylon.edu.iq
[2]Department of Computer Science, College of Science for Women, Babylon University ,Iraq
suhad.ali2003@yahoo.com
[3]Department of Computer Science, College of Science for Women, Babylon University ,Iraq
Majid_al_sirafi@yahoo.com
***Corresponding author email** Email: haider9111973@gmail.com.

Received:	20/4 /2021	Accepted:	13/5/2021	Published:	30/6/2022

ABSTRACT

In this paper, a non-blind watermarking method for protecting the copyright of digital color images is introduced. This method based on the combination of digital transforms (DWT, DCT) in the frequency domain. The embedding process in this method depends on the partition of the host image into 16×16 non-overlapped blocks and the use of edge entropy metric to choose the appropriate blocks for the insertion process for the purpose of increasing the imperceptibility of the proposed system. As for the extraction process, it is carried out in a way that requires the presence of the original image but rather follows the same embedding protocol to extract the embedded encrypted watermark. To raise the security level, a hybrid encryption method using the chaotic map and DNA coding has been applied for encrypting the watermark before embedding it. Experimental results demonstrate that the differences between the watermarked image and the original image are indistinguishable. The proposed method is effectively resisted common image processing attacks.

Keyword: DCT , DWT , DNA encoding , Chaotic Map.

الخلاصة

في هذا البحث ، تم تقديم طريقة العلامة المائية غير العمياء لحماية حقوق النشر الخاصة بالصور الرقمية الملونة. تعتمد هذه الطريقة على مجموعة من التحويلات الرقمية (DWT ، DCT)في مجال التردد. تعتمد عملية التضمين في هذه الطريقة على تقسيم الصورة المضيفة إلى كتل غير متراكبة 16 × 16 واستخدام مقياس إنتروبيا الحافة لاختيار الكتل المناسبة لعملية التضمين لزيادة عدم الإدراك في النظام المقترح. أما بالنسبة لعملية الاستخراج ، فهي تتم بطريقة تتطلب وجود الصورة الأصلية ولكنها تتبع نفس بروتوكول التضمين لاستخراج العلامة المائية المشفرة المضمنة . و لرفع مستوى الأمان ، تم تطبيق طريقة تشفير هجينة باستخدام الخريطة الفوضوية وترميز الحمض النووي لتشفير العلامة المائية قبل تضمينها. تظهر النتائج التجريبية أن الاختلافات بين الصورة ذات العلامة المائية والصورة الأصلية لا يمكن تمييزها. الطريقة المقترحة قاومت بشكل فعال هجمات معالجة الصور الشائعة.

الكلمات المفتاحية:تحويل جيب التمام منفصلة ، تحويل مويجي منفصل ، تشفير الدي ان اي ، الخريطة الفوضوية

مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

1. Introduction

The rapid development of digital technologies has led to a great development in the processes of exchanging, accessing, copying, and storing digital images at a low cost and high speed. However, these features allowed digital image distortion and copying operations that may be lead to distortion, duplication, or illegal distribution of digital images, which led to an increased risk of violating the property rights of these images and harming their owners [1]. Watermark is an important and powerful way to protect ownership of digital images. Some of the watermarks are visible, while others are invisible [2]. In addition, a watermark is classified according to its resistance to attacks into a fragile watermark and a robust watermark. Fragile watermark utilizes for authentication digital image; while a robust watermark utilized to prove ownership of the digital image [3]. The watermark classifies according to the method of retrieving the watermark from the host image into the blind and non-blind watermarks. The blind watermark method retrieves the embedded watermark without the need for the original cover image; while the non-blind watermark method needs the original host image to retrieve the embedded watermark [4].

During the transfer of the digital image, may be exposed to different types of attacks, both intentional and unintentional attacks. Intentional attacks are those that lead to a change in the pixel values of the host image, a change in the intensity, a change in the size or shape of the host digital image. As for unintended attacks, it means the changes that a digital image may be exposed to during transmission or storage, such as compression of digital images [5].

Several watermarking schemes for digital color image have been proposed**.** In 2016 [6], Podili and Jagadeesh introduced a watermark color image algorithm for copyright protection using artificial intelligence techniques to obtain a good balance between imperceptibility and robustness. In this algorithm both fuzzy logic and backward propagation neural networks are used in the frequency domain by the combination of both DCT with DWT. The system is tested against cropping, image contrast attack, and salt and pepper noise. In 2016 [7], Rita and Girish presented a digital watermarking image technique using 2-level DWT to obtain four components (LL, LH, Hl, HH) in each band.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

The embedding of the watermark is done in the (LL) component of the cover image using a variable visibility factor. Tests of this algorithm showed that the watermarked image and the extracted watermark are depending on the visibility factors and the two-levels of DWT gives better results than the one - level of DWT. In 2017[8], Mohammad suggested a method for non-blind watermarking in color images. The objective of the algorithm is copyright protection. This method relies on converting the color image to a color space called (YCoCgR) and using the Y component as a cover for embedding a secret logo. The Y component is chosen for watermark insertion, and transferring it to the frequency domain by DCT, and dividing it into 8*8 blocks. The embedding method is adaptive by selecting the blocks with the most complex properties to be resisted against some attacks; especially the JEPC attack. To obtain more security, the Arnold method is applied to the secret logo. In 2017 [9], Jianzhong Li et al presented a non–blind watermark color digital image depend on the quaternion Hadamard transform (QHT), and Schur decomposition. The algorithm is computing the (QHT) of a color image that is represented by quaternion algebra. The watermark is inserted into the cover image by adjusting the Q matrix by employing Schur decomposition. This algorithm satisfied the robustness and security requirements and resist cropping and rotation attacks. In 2018 [10], Nesrine et al suggested a blind image watermarking mechanism using DCT and a least significant bit (LSB). The Arnold transform is applied to the secret image for achieving better safety. In the suggested algorithm, the host image is converted to YCbCr space. The (Y) and (Cb) components of the original image are replaced by the bits of the secret image. The purpose of the suggested method is copyright protection and is tested against some attacks such as the JPEG attack. In 2018 [11], Te-Jen et al presented a method for copyright protection depend on using DCT and Two-Dimensional Linear Discriminant Analysis (2DLDA). In the beginning, the color image is converted into the YIQ color space. Then, the DCT is used to transform the quadrature chrominance component into the frequency domain. Next, a couple of binary watermarks (one for reference, and the other for logo) are appended to certain bits of the AC coefficients. To retrieve the logo watermark, the matrix-based 2DLDA is used based on the DCT method.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مـجلـة جـامعة بـابـل للعلـوم الصـرفـة والتطـبيقيـة مـجلـة جـامعة بـابـل للعلـوم الصـرفـة والتطـبيقيـة مـجلـة جـامعة بـابـل للعلـوم الصـرفـة والتطـبيقيـة

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

In this paper, a non-blind watermarking method is proposed to prove the ownership of digital color images. The watermark is included in the frequency domain by combining the features of both DCT and the DWT transforms, and by using a coding method based on a combination of chaotic and coding by DNA rules to encode a watermark before inserting it in the host image.

2. Preliminaries

2.1 Chaotic Map

There are many encryption algorithms available for digital data, which provide a high security ratio for the embedded data. In recent years, the chaotic algorithms appeared have been proven to be very suitable for encryption because of its advantages. It is a non-linear system and the resulting sequence cannot be predicted, as it is a sensitive system for the random and initial state. Encryption algorithms based on chaotic systems increase cryptographic system strength against potential attacks because it has a number of characteristics. There are some well-known maps such as Logistic Map, Tent Map, Quadratic Map, and others [23 theses]. Mathematically, any chaotic map can be defined as in Equation (1)[12].

$$x_{n+1} = f(x_n) \quad , n = 1,2, \ldots n \quad \ldots \ (1)$$

Where xn is called the state of iteration n, the function f is mapping the state $x_{n\text{-}1}$ to the next state x_n.

In this paper researcher used and concentrates on Quadratic Map. Quadratic map equation can be defined as in Equation (2).

$$x_{n+1} = r - (x_n)^2 \ \ldots \ (2)$$

Where n represents the iterations number and r is the parameter of chaotic. The quadratic map is used in this proposed work for the permutation of image pixels.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

2.2 DNA Encoding and XOR Operation for DNA Sequences

Deoxyribonucleic acid DNA is the main carrier of genetic information in organisms. Each cell in the Organism's body has a set of DNAs. Each individual of organisms has a unique DNA. DNA is a dual helical structure with two strands working in parallel; each is made of what are called nucleotides. Nucleotides are composed of phosphate, sugar, and one of the nitrogenous bases. DNA contains three nitrogen bases (adenine A, cytosine C, thymine T, and guanine G). Thymine and cytosine are linked to be pyrimidine, Adenine, and guanine is linked to be purines [13]. Figure (1) shows the general structure of DNA.

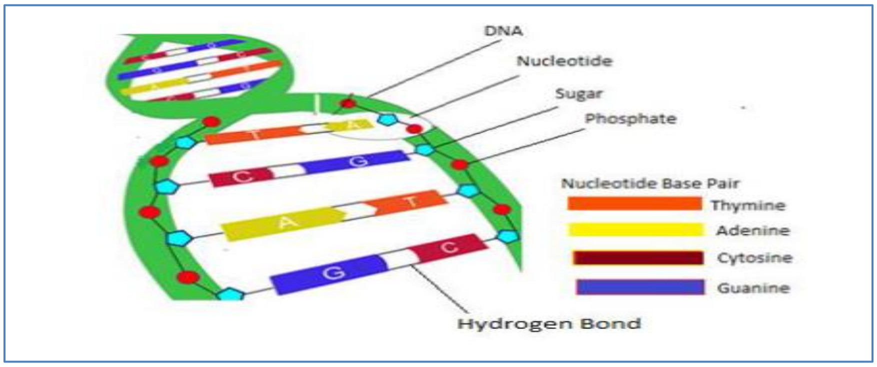


Figure (1) :The general structure of DNA [13]

DNA cryptography is considered the newest cryptographic method using the inbred operation of DNA formation to encrypt information. It uses the biological technology is used as an execution tool and DNA is used as a Data holder [14]. Each nitrogen base can be expressed by binary symbols (0 and 1) as illustrated in Table (1)[15].

Table 1. DNA Encoding Rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The XOR operation is applied to the rules for DNA mentioned in the table (1) in the same way as it applies it to the binary numbers .The XOR are reflexive operation, meaning when it is applied between two rules and obtain the resulting rule, it is possible to apply a XOR between the result and one of the coefficients of the first XOR operation to obtain the second parameter. For that reason, it's used in encryption methods. To clarify, if we apply the XOR operation between the sequence [ATTC] and the sequence [GTAC] then the result will be [GATA] as shown in table (2). When we reverse the operation and apply the XOR between the sequence [GATA] and the sequence [GTAC] then the result will be [ATTC] [16].

Table (2) : XOR operation

XOR	**A**	**C**	**G**	**T**
A	A	C	G	T
C	C	A	C	G
G	G	T	A	C
T	T	G	T	A

The XOR operation is implemented to the rules for DNA mentioned in table (1) in the identical way as it applies it to the binary numbers. The XOR is a reflexive operation, when it is applied between two rules and obtain the resulting rule, then it can be applied an XOR between the result and one of the coefficients of the first XOR operation to get the second parameter. For that reason, it's used in encryption processes [16].

2.3 Discrete Wavelet Transform (DWT)

It used in several media applications such as digital image watermarking and audio and video compression. Wavelet transform provides a multi-resolution signal decomposition approach. In this transform, the image is divided into three spatial directions: vertical, horizontal, and diagonal. At each level of division, DWT divides the image into four bands (LL, HL, LH, and HH). The LL band coefficients are considered the most significant with low frequencies and the (HL, LH, and HH) coefficients are the least significant coefficients with high frequencies. It is possible to decompose the LL band by applying another level

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

of DWT to it to obtain four new sub-bands. This process can be repeated several times depending on which application is used [17].

2.4 Discrete Cosine Transforms (DCT)

It converts a sequence of data in the spatial domain to a sum of cosine waveforms in the frequency domain. When applying it to an image, the resulting set of coefficients will have three bands of frequencies. The top-left coefficient represents the Low-frequency band, and the other coefficients will be mid and higher frequency bands, figure (2) shows the three frequency bands for the block of (8×8)size. The human eyes are sensitive to low frequency so it is not used to embed watermark. Embedding in high frequencies will be affected by the compression attacks. Therefore, modulation is preferred in the medium frequencies[18].

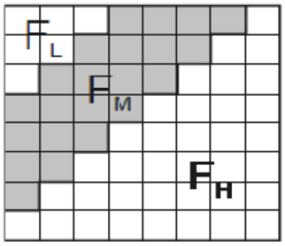


Figure (2) : DCT Frequency Bands

The DCT can be computed depending on equation (3) [19].

$$DCT(u,v) = \alpha_u * \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) * cos\frac{(2x+1)u\pi}{2M} * cos\frac{(2y+1)v\pi}{2N} \quad \ldots (3)$$

Where

$$\alpha_u = \alpha_v = \sqrt{\frac{1}{M}} \qquad u = v = 0 \;\ldots (4)$$

$$\alpha_u = \alpha_v = \sqrt{\frac{2}{N}} \qquad u \neq v \neq 0 \quad \ldots (5)$$

The inverse of DCT can be computed according to equation (6)

$$\boldsymbol{IDCT(u,v) = \alpha_u * \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} DCT(u,v) * cos\frac{(2x+1)u\pi}{2M} * cos\frac{(2y+1)v\pi}{2N}} \quad \ldots (6)$$

مجلة جامعة بابل للعلوم الصرفة والتطبيقية
ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

2.5 Standard Deviation (STD):

It is a statistical Metric that shows how much variation exists from the average. A low value of standard deviation (STD) indicates that the data points heads are to be close to the mean, whilst a high value of the standard deviation (STD) refers tells that the data points are prevalent over a wide range of values. Standard deviation can be calculated based on equation (7)[20],[21].

$$\text{STD}=\sqrt{\frac{\sum(\mathrm{x}-\bar{\mathrm{x}})^2}{\mathrm{n}}} \quad \dots \quad (7)$$

As STD utilized to measure the variability, it can be utilized to indicate for the edge, meaning that the larger STD on the edge of the image.

2.6 Edge Entropy

Edge entropy is a metric that gives some information about the texture of an image as edges of the image. This metric used in some watermark techniques to determine the appropriate location to embedding a watermark in an image. The points edge not suitable for embedding and can cause destroying the host image, so using this metric used to determine which block of the image is good for the embedding process, in other words, this metric preserve provides a good level of imperceptibility[22]. Edge entropy is calculated according to the equation (8) .

$$E = \sum_{i-1}^{n} P_i^{\exp(1-P_i)} \qquad \dots (8)$$

Where P_i represents the probability of the pixel value i.

3. The Proposed Non-Blind Color Image Watermarking System

The suggested system objective is to prove the ownership of color images against unauthorized users. The proposed system includes three procedures, encryption of the watermark, embedding the watermark, and watermark extraction process as show in figure(3).

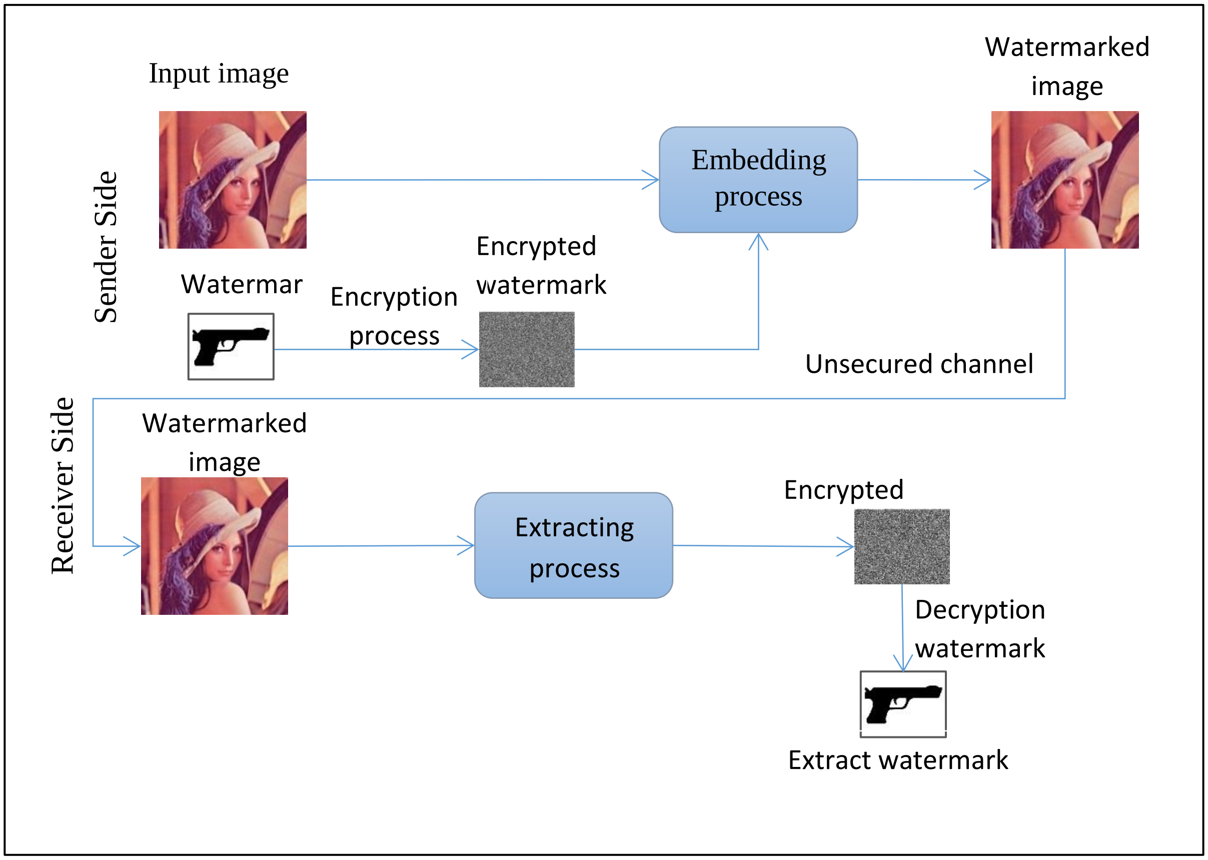


Figure (3) General diagram for Proposed System

3.1 Watermark Encryption Procedure

To improve the security level of the suggested system, an encryption method depend on DNA philosophy and chaotic map are utilized to encrypt the secret logo (watermark) before inserting it into the host image.

In the encryption process, some steps must be applied. Firstly, the watermark image is split into a set of non-overlapped blocks of n × n pixels, and the blocks are scrambling to generate a scrambled image by using the following equations:

$$Nb1=(Key\times lenw) \bmod Nb +1 \qquad (9)$$

Where *Key* is a prime number used for blocks scrambling, *Nb is the total number of* blocks, lenw is a counter in the range (1 … Nb), Nb1 is the number of blocks.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية

In the second step, the input 2D binary image is converted into a 1D vector (vec_Img) then a chaotic sequence (Seq) with a length equal to (vec_Img) is generated according to the standard Quadratic chaotic system equation (2). The generated chaotic sequence (Seq) is used for Image Pixels Diffusion and Mask Generation.

In the Image pixels diffusion process, using the generated chaotic sequence (Seq) by sorted it in ascending order. The bit location of an image is changed according to the corresponding indices (loc) of the sorted sequence. Finally, the result (Diffused -Vector) is converted into a 2D image (Diffused -Image). Equations (10) and (11) show how the diffusing operation is done:

$$[Sorted\_Seq, loc] = sort(Seq) \quad (10)$$

$$Scrambled\_(Vector(i)) = image(loc(i)) \;,\quad for \quad i \ldots length\ (image) \quad (11)$$

Where loc is the arrangement of the elements of (Seq) into Sorted_Seq).

While in the mask generation Process, The generated chaotic sequence (Seq) is utilized to create the binary mask which is used later in the encryption process according to the following equation:

$$Mask\_Seq(i) = \| \lfloor Seq\ (i) \times 255 \rfloor \| \quad \ldots(12)$$

$$for\ i = 1 \ldots length\ (image)$$

Where Seq represents the generated chaotic sequence, i represents a current index of the generated chaotic sequence (Seq), and ||. || represents an absolute value. Then the (Mask_(seq)) elements are converted to a binary range (0,1) according to equation(13).

$$Mask(i) = \begin{cases} 1 & \text{if} \quad Mask_{seq(i)} \geq T \\ 0 & \quad\quad\quad \text{oterwise} \end{cases}, \quad \ldots\ (13)$$

Where, T is the threshold which is set from user-selected by test.

The final step include DNA encoding for both Diffused Image and Generated Mask. Each one of Diffused Image and Generated Mask is divided into two matrices:(Even, Odd). The Odd matrix contains the pixels in the odd rows positions and the even matrix contains the

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

pixels in the positions of the even rows. The odd and the even image matrices are converted into a 1D vector. The odd (mask, image) and the even (mask, image) vectors are encoded by rule (1) and by rule (3) of DNA rules respectively. After that, Converted the two 1D arrays into binary then reconstruct them to obtain a 2D array that represented the Encrypted array. Algorithm(1)the states of encryption watermark.

Algorithm (1): Watermark Encryption Activity

```
Input:    Ore_W    // Original watermark, Chaotic key, Scrambling key

Output : EN_W    // encrypted watermark

   Step 1: Scrambling Ore_W  by scrambling block .
        1.1    : Divide the original watermark in to non-overlap blocks.
        1.2    : Scrambling block according to equations (3.1)using
                 scrambling key.
   Step 2 : Scrambling image resulting from step 1 using Quadratic
                 chaotic map.
        2.1  : Convert 2D array of image in to 1D array (vec_Img).
        2.2  : Generate  a chaotic sequence (Seq) with length equal to
               (vec_Img) according to the standard Quadratic chaotic
               System equation (2.2)using chaotic key.
        2.3  : Sort (Seq ) in ascending  to Diffuse the (vec_Img)
                According to equations (3.2) ,(3,3).
        2.4  : Using a chaotic sequence (Seq)  to generating mask
              (Mask_seq)  according to equation (3.4) .
          2.5    : Convert (Mask_seq ) to binary value according to equation
                 ( 3.5 ) ,which using in step3 for encryption .
  Step 3 : Encrypt  the image resulting from step 2 by using DNA
```

encoding .

3.1 : Divide mask in to odd O_mask, and even array E_mask

3.2 : Divide scrambled image in to odd O_img and even array , E_img

3.3 : Encode O_img and O_mask by rule 1 of DNA to result ODNAimg and ODNAmask .

3.4 :Encode E_img , and E_mask rule 3 of DNA to result EDNAimg and EDNAmask.

3.3 : Applied XOR operation between ODNAimg and ODNAmask depend on rule of DNA ,then between EDNAimg and EDNAmask depend on rule of DNA as showed in table (2.2) .

3.4 : Reconsruct and merge two 1D arrays result from step 3.3 to obtain 2D EN_W (Encrypted watermark).

3.2 Non - Blind Watermark Embedding Procedure

In order to perform the embedding process, a colored image is first separated into three image bands, which are (R_img, G_img, and B_img). The embedding process is done by hiding one bit from the secret logo in image bands (R_img, G_img) and two bits in the (B_img) image band. These images are divided into non-overlapping 16 ×16 blocks and are arranged according to the edge entropy value of blocks (in ascending order) from the lowest to the highest, the edge entropy is calculated by using equation (8). The purpose of the edge entropy calculation is to select the appropriate blocks for the embedding process,

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

which means the blocks are arranged in a way that ensures the increased imperceptibility. The low value of edge entropy means that the block is smooth and will be more robust in the embedding process, while the highest value of edge entropy means that the block is coarse and will be more robust against attacks.

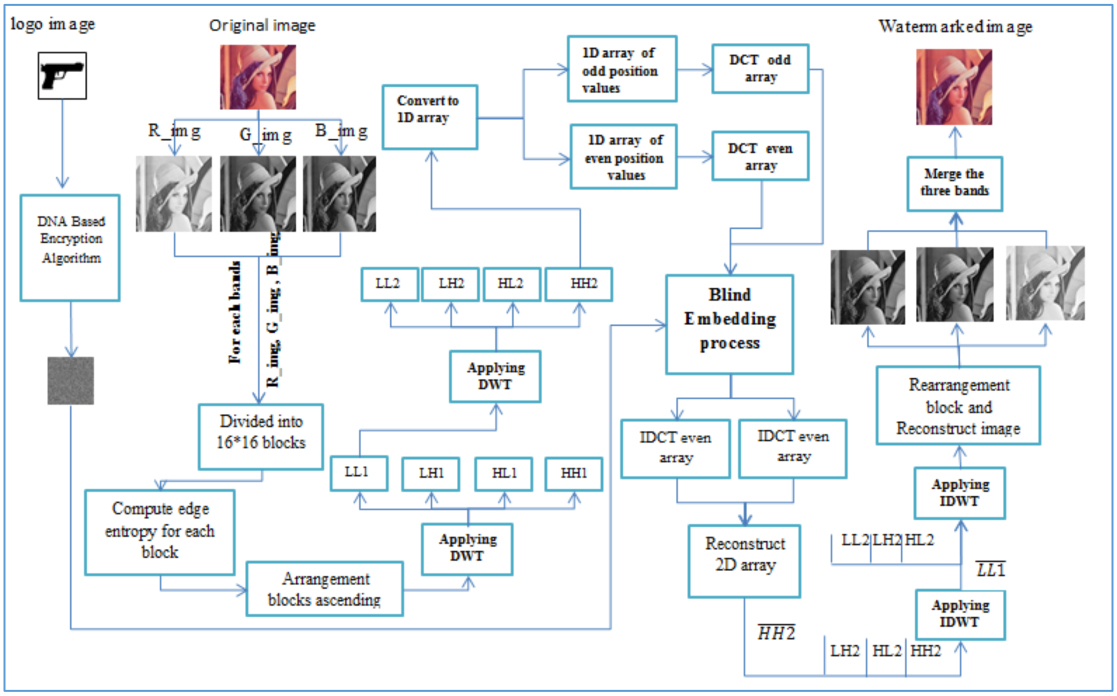


Figure (4) : Non-blind embedding process for color image

The embedding is done depending on equations are illustrated in (14), and (15):

$$O\_dct(idx) = (1/2 \times (O\_dct(idx) + E\_dct(idx))) + (fac \times sce) \ldots (14)$$

$$E\_dct(idx) = (1/2 \times (O\_dct(idx) + E\_dct(idx))) + (fac \times sce) \ldots (15)$$

For R_img and G_img, idx=3

For B_img, idx= 3,4

It should be noted that choosing both the third and fourth bits for the purpose of the inclusion process, because they are among the intermediate transactions, which offer a good trade-off between insensibility and resistance.

مـجلة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية مـجلة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية مـجلة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Where O_dct, E_dct represent the odd and the even array after applying DCT on them, Sec equal 1 or -1 depending on the value of watermark as shown in (16):

$$Sec = \begin{cases} -1 & if \quad W(j) = 0 \\ 1 & otherwise \end{cases} \qquad \ldots (16)$$

fac represents a scaling factor, this value is changing depending on the smoothness degree of the host image block to ensure impressibility. To measure the block smoothness degree, the standard division (std) of the block is computed to select the appropriate value of the scaling factor (fac) according to equation (17). The selected blocks are divided into three sets of bocks (smooth, partial smooth, and coarse) by comparing the standard division of the block with a threshold (T) according to the following:

```
if std<18   the block is smooth
else if std≥ (18  )&& Std<( 24 )
the block is partially smooth
else
the block is coarse
```

According to the above comparison, the high value is assigned to fac when the block is coarse while the low value is assigned when the block is smooth. After each embedding process, IDCT is applied on the watermarked block to obtain the sub-band (HH2). Finally, the IDWT is applied then rearranging the scrambled blocks. The watermarked image is resulted by combining the three watermarked images (R_img, G_img, B_img).

3.4 Non - Blind Watermark Extracting Procedure

In this technique, the extracting process required the existence of the original color image. Figure (4) shows the steps of the extracting process.

In the non-blind method, the same steps are applied to the blocks of the watermarked image and the original image. The extraction process begins by separating the watermarked image into three images (R_img, G_img, and B_img) then dividing them into non-overlapping blocks with dimension 16 × 16. The embedding process is done in a

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

non-blind manner therefore the selection of blocks suitable for embedding is based on computing the edge entropy of each block. Then, the blocks are arranged in an ascending order depending on the edge entropy values of these blocks. The embedding process is done by selecting the blocks with the lowest edge entropy to hide the bits of the secret watermark. The two levels of DWT are applied on each block to obtain four sub-bands (LL2, LH2, HL2, HH2). It will produce four bands (LL1, LH1, HL1, HH1) for each block, then apply the second level of DWT on the LL1 to result in the other four bands (LL2, LH2, HL2, HH2). The HH2 that resulting from blocks of (R_img, G_img, B_img) are stored in three separated arrays to use in the extract process. Each of these arrays will be divided into two 1D arrays. The first array is used for storing the odd locations' value (O_array), and the second array is used for storing the even locations' value (E_array). To complete the extraction process, the DCT is applied on each of these arrays (O_dct, E_dct). Finally, the extraction equation (17) is applied to obtain the pixels' values of the embedded watermark(encrypted watermark).

$$\mathrm{Wbit(i)} = \begin{cases} 1 \quad \text{if} \quad \mathrm{O_{dct(idx)}} > \mathrm{E\_dct(idx)} \\ 0 \qquad\qquad\qquad\qquad \text{oterwise} \end{cases} , \ldots \quad (17)$$

For R_img band, G_img band idx=3

For B_img band idx=3,4

The extraction process is done by extracting one bit from the block of (R_img), one bit from the block of (G_img), and two bits from the block of (B_img).

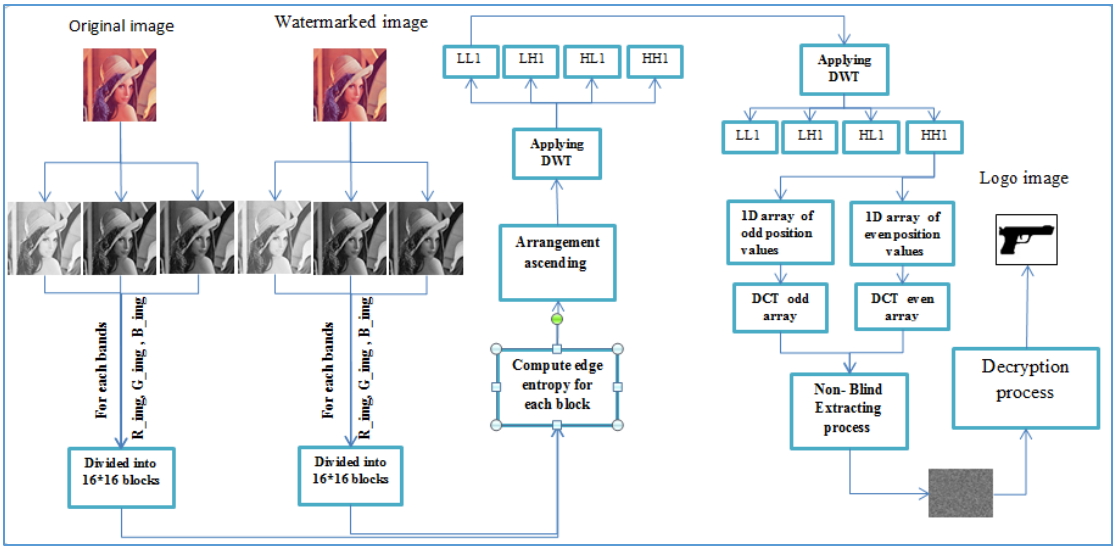


Figure (5) : Non-blind extraction process

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

3.5 Watermark Decryption Procedure

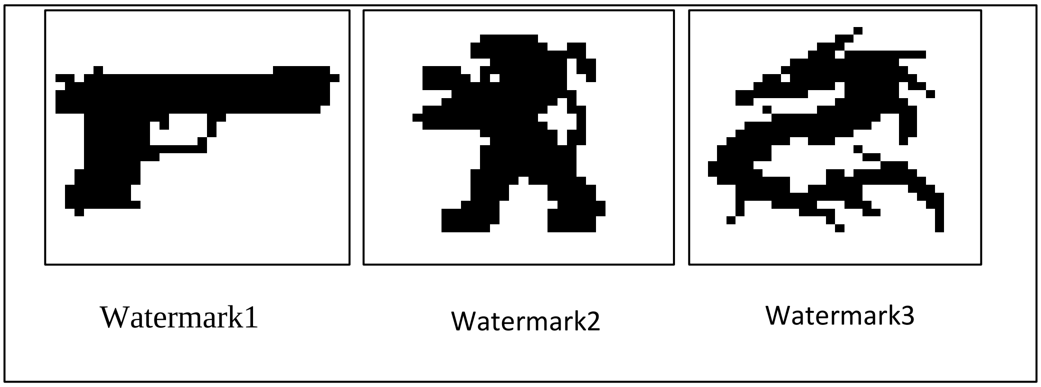
To restore the original watermark image, a decryption process must be performed on the extracted watermark image.

Firstly, equation (2) is used to generate a random vector with the size of the encrypted image based on the quadratic chaotic system. The mask is generated according to equation (12) by using the generated chaotic random vector then converted to a binary value according to equation (13). The encrypted image is divided into two matrices:(Even, Odd). The Odd matrix contains the pixels in the odd rows positions and the even matrix contains the pixels in the positions of the even rows. Also, the generated mask is splitting into two matrices, one has the elements of the odd position rows and the other has the elements of the even position rows. The odd and the even image matrices are converted into a 1D vector. The odd (mask, image) vectors are encoded by rule (1) of DNA rules and save the result in a 1D array (ODNAmask, ODNAimg). Also, the even (mask, image) vectors are encoded by rule (3) of DNA rules.

Applying decrypted XOR operation between odd(mask, image). And even (mask, image) to obtain decoded watermark by DNA rules. The decrypted image by XOR DNA rules must be diffused using the generated chaotic random vector according to equations (10),(11). Finally, the diffused image is divided into a set of non-overlapped blocks of n × n pixels. After that, the blocks are repositioned using a key (position key) to generate a descrambled image based on the equations (9).

4. Experimental Results

To assess the effectiveness of the proposed cryptography algorithm, some performance measurements are used after encrypted three samples of images which are shown in figure (6) and the result was as illustrated in the table (3).



Watermark1 Watermark2 Watermark3

Figure (6)Samples of Watermarks

مجلـة جامعـة بابـل للعلـوم الصـرفـة والتطبيقيـة مجلـة جامعـة بابـل للعلـوم الصـرفـة والتطبيقيـة مجلـة جامعـة بابـل للعلـوم الصـرفـة والتطبيقيـة

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table (3) Result of the proposed encoding system evaluation metrics

Watermark	**AE value**	**Entropy value**	**CC value**	**NPCR value**	**UACI value**
Watermark1	0.5322	0.9800	0.0242	53.2227	53.2227
Watermark2	0.5234	0.9880	0.0125	52.3438	52.3438
Watermark3	0.5205	0.9865	0.0227	52.0508	52.0508

Several tests are done in order to select the best blocks for embedding based on their entropies. The tests include a comparison among (less, Medium, and high) edge entropies of blocks for embedding. The Non-blind algorithm is used to insert the watermark and the PSNR imperceptibility metric is applied to evaluate this algorithm. The PSNR value is calculated according to the equation (18).

$$PSNR = 10\log_{10}\frac{(2^L)^2}{MSE} \quad (18)$$

Where L represents the number of bits required to represent image pixels. The PSNR values and the watermarked images are illustrated in figure (7) using blocks with less lower edge entropies for embedding.

Original image	**Watermarked image**	**PSNR**
Lena Image		
		48.7623
Pepper Image		
		48.7505

مجلـة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية مجلـة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية مجلـة جـامعة بـابل للعلـوم الصـرفة والتطـبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

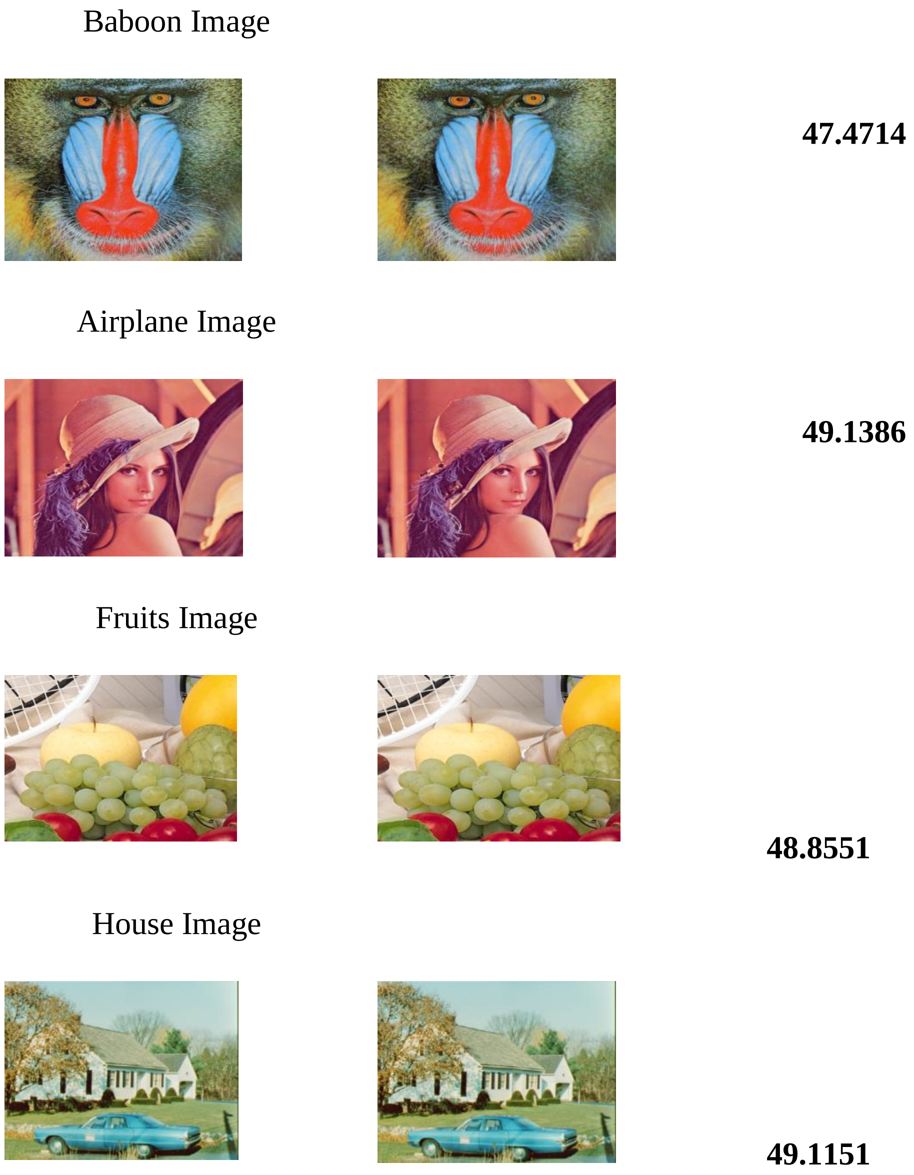


Figure (7): PSNR values of proposed method for test images

In the suggested method, the image blocks are selected according to their edge entropies therefore it must determine which blocks with (low, middle, or high) edge entropies are selected for embedding. Several tests are done to determine the best blocks. "NC and BER" metrics are used to measure the robustness of the non-blind watermark proposed system after subjecting the watermarked image to different types of attacks. NC and BER are computed according to the following equations:

$$NC = \frac{\sum_{i=1}^{x}\sum_{i=1}^{y} w(i,j)w'(i,j)}{\sum_{i=1}^{x}\sum_{j=1}^{y} w(i,j)^2} \ldots (19)$$

$$BER = \frac{1}{X*Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}|\ w(i,j) - w'(i,j)| * 100\% \quad \dots (20)$$

Where w and $\overline{w}$ are represent the original and extracted watermark respectively.

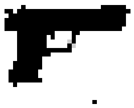
The robustness measures when selected blocks with low edge entropies are illustrated in the table (4).

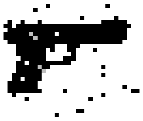
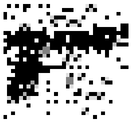
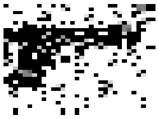
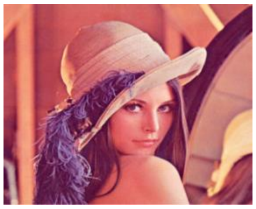
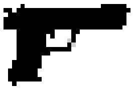
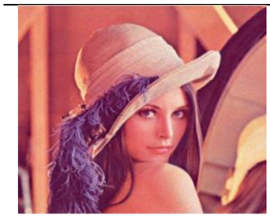
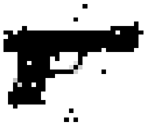
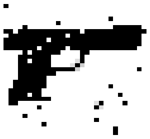
Table (4) the value of NC and BER for the non-blind method, Less Edge Entropy

Type of attack		Lena		Pepper		Baboon	
		NC	BER	NC	BER	NC	BER
No attack		1	0	1	0	1	0
	Degree of noise						
Salt & Pepper with different density	0.001	1	0	1	0	1	0
	0.01	0.9758	0.0361	0.9609	0.0586	0.9753	0.371
	0.02	0.9186	0.1191	0.9093	0.1328	0.9276	0.1064
	0.03	0.8994	0.1465	0.8564	0.2051	0.9006	0.1445
Speckle Noise With different density	0.001	1	0	1	0	1	0
	0.005	0.9903	0.0146	0.9929	0.0107	0.9857	0.0215
	0.009	0.9778	0.0332	0.9857	0.0215	0.9594	0.0605
Gaussian Noise With different density	0.00001	0.8959	1514	0.8655	0.1934	0.8867	0.1641
	0.001	0.8837	0.1680	0.8620	0.1982	0.8982	0.1475
	0.005	0.8967	0.1504	0.8748	0.1797	0.8943	0.1533
	0.009	0.8819	0.1709	0.8755	0.1787	0.9004	0.1455
Poisson Noise		0.9903	0.0146	0.9955	0.0068	0.9903	0.0146
Compression with different Quality factors	0.80	1	0	1	0	1	0
	0.75	1	0	0.9974	0.0039	1	0
	0.50	1	0	0.9935	0.0098	1	0

Median 3×3	0.9994	0.0009	0.9935	0.0176	0.9785	0.0322
Mean 3×3	1	0	0.9883	0.0176	0.9837	0.0244
Brightness+50	0.9726	0.0420	0.9987	0.0020	0.9394	0.0898
Brightness+25	0.9942	0.0088	1	0	0.9981	0.0029
Histogram	1	0	0.9994	0.0009	0.9994	0.0009
Sharpen	1	0	1	0	1	0
Cropping Upper Left	0.9483	0.0771	0.9812	0.0283	0.9987	0.0020
Cropping Center	0.9754	0.0371	0.9474	0.0781	0.8261	0.2480
Rotation 10	1	0	1	0	1	0
Rotation 20	0.9552	0.0664	0.9491	0.0752	0.8951	0.1523
Rotation 180	0.9733	0.0400	0.9565	0.0645	0.9055	1377
Gaussian filter	1	0	1	0	1	0
Resize 256	1	0	1	0	1	0
Gamma correction	1	0	1	0	1	0

Figures (8) show watermarked image after applying the above attacks Non Blind (Less Edge Entropy) Method

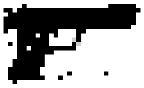
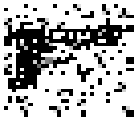
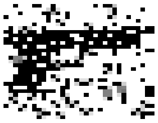
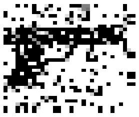
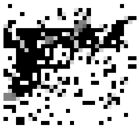
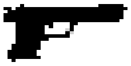
Type of Attacks	**Watermarked image**	**Extracted watermark**
0.001		

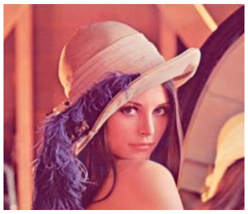
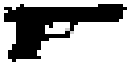
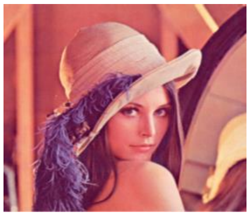
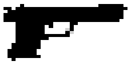
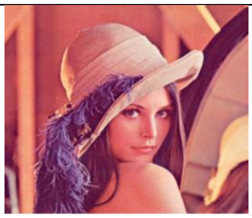
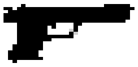
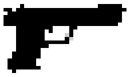
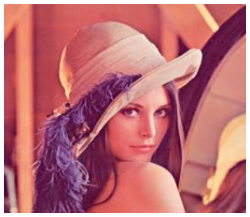
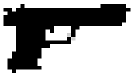
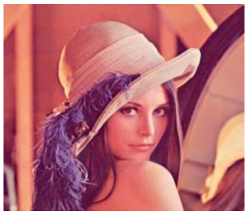
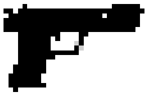
Salt & Pepper with different density	0.01		
	0.02		
	0.03		
	0.001		
Speckle Noise with different	0.005		
	0.009		

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

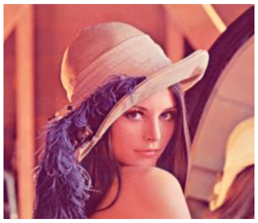
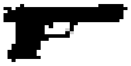
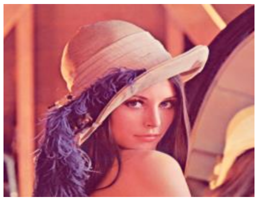
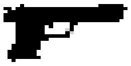
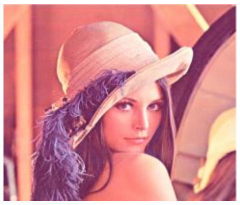
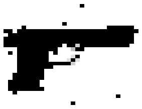
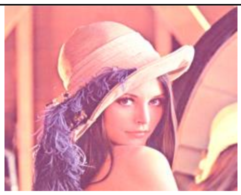
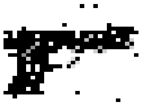
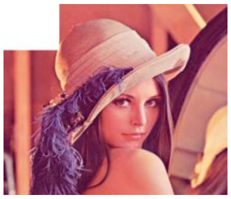
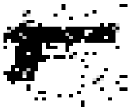
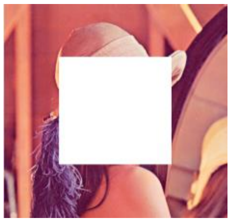
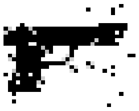
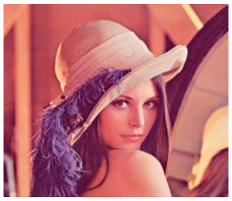
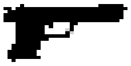
مـجلة جـامعة بـابل للعلوم الصـرفة والتطبيقية مـجلة جـامعة بـابل للعلوم الصـرفة والتطبيقية مـجلة جـامعة بـابل للعلوم الصـرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Poisson Noise			
Gaussian Noise with different density	**0.00001**		
	0.001		
	0.005		
	0.009		
Histogram Equalization			

	Sarpen		
Compression with different Quality	50		
	75		
	80		
Attack Filter	Mean 3×3		
	Median 3×3		

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

	Gaussian		
	Resize		
Brightness with different degree	25		
	50		
Cropping Attack	Upper left		
	Center		
Rotation with different angle	10		

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

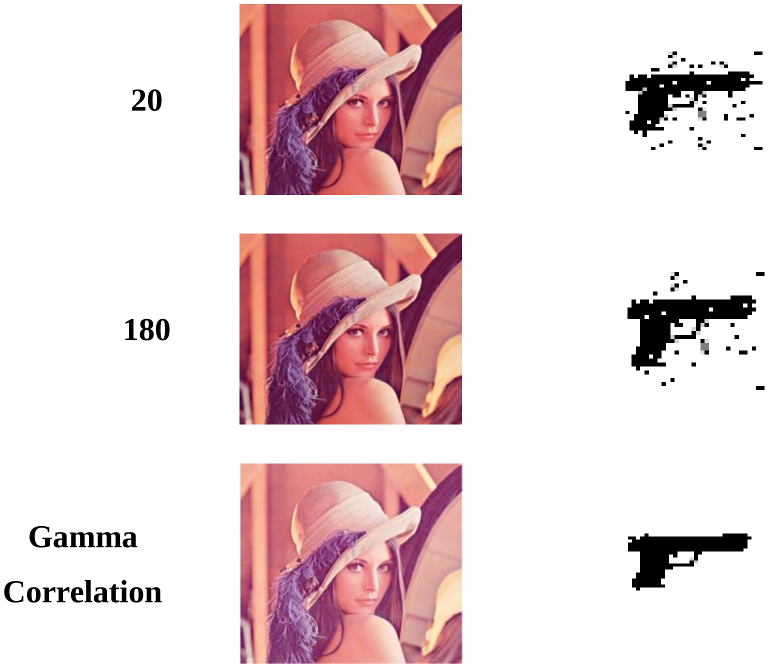


Figure (8) Extraction of watermark against different attacks using blocks of lower edge entropy values

To clarify the effect of selecting image blocks for embedding based on their highest entropy values the following tests are done as in the table (5).

Table (5) PSNR, CN and BER values of embedding watermark in blocks with high values of entropy

		Lena		Pepper		Baboon	
Type of attack		**PSNR= 45.3931**		**PSNR= 46.5074**		**PSNR = 42.1986**	
		NC	**BER**	**NC**	**BER**	**NC**	**BER**
No attack		1	0	1	0	1	0
	Degree of noise						
Salt & Pepper with different density	**0.001**	1	0	1	0	1	0
	0.01	0.9870	0.0195	0.9844	0.0234	0.9922	0.0117
	0.02	0.9607	0.0586	0.9458	0.0801	0.9779	0.0322
	0.03	0.9156	0.1230	0.9138	0.1260	0.9519	0.0713

مجلـة جامعـة بابـل للعلـوم الصـرفة والتطبيقيـة مجلـة جامعـة بابـل للعلـوم الصـرفة والتطبيقيـة مجلـة جامعـة بابـل للعلـوم الصـرفة والتطبيقيـة

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Speckle Noise With different density	**0.001**	1	0	1	0	1	0
	0.005	0.9974	0.0039	0.9974	0.0039	1	0
	0.009	0.9922	0.0117	0.9890	0.0166	0.9994	0.0009
Gaussian Noise With different density	**0.00001**	0.9028	0.1416	0.8814	0.1719	0.9573	0.0635
	0.001	0.9131	0.1270	0.8971	0.1494	0.9552	0.0664
	0.005	0.9056	0.1377	0.9055	0.1377	0.9535	0.0693
	0.009	0.9092	0.1328	0.9049	0.1387	0.9572	0.0635
Poisson Noise		0.9968	0.0049	0.9948	0.0078	1	0
Compression with different Quality factors	**0.80**	1	0	1	0	1	0
	0.75	1	0	1	0	1	0
	0.50	0.9987	0.0020	0.9994	0.0009	0.9987	0.0020
Median 3×3		0.9568	0.06475	0.9575	0.0635	0.8370	0.2305
Mean 3×3		0.9439	0.0830	0.9567	0.0645	0.8742	0.1807
Brightness+50		1	0	0.9994	0.0009	0.9994	0.0009
Brightness+25		1	0	1	0	1	0
Histogram		0.9987	0.0020	0.9851	0.0225	1	0
Sharpen		1	0	1	0	1	0
Cropping Upper Left		0.9948	0.0078	0.9640	0.0537	0.9503	0.0742
Cropping center 25%		0.8225	0.2529	0.8815	0.1729	0.9648	0.0527
Rotation 10		1	0	1	0	1	0
Rotation 20		0.9160	0.1221	0.8941	0.1533	0.7456	0.3477
Rotation 180		0.9334	0.977	0.9045	0.1387	0.7957	0.2852
Gaussian filter		1	0	1	0	1	0
Resize 256		1	0	1	0	1	0
Gamma correction		1	0	1	0	1	0

When comparing the results of the above table with the results of embed in the blocks which have less value of edge entropy, it becomes clear that the PSNR values are less than the PSNR value of embedding in less edge entropy block method that indicated in the figure (7), and this means that it is less imperceptibility and less distortion in the sites embedding in the image, in addition to some types of attacks being weak such as (median, mean, cropping and rotation) when to compare the result of NC and BER in the table (4) with the result of NC and BER in the table (5), therefore are considered a method of embedding the watermark in less entropy value blocks is preferable.

Finally, when arranging the image blocks in ascending order depending on the edge entropy value, the blocks with intermediate values between those with higher edge entropy and lower edge entropy were chosen, the results of the implementation were as shown in table (6).

Table (6) PSNR, CN and BER values of embedding watermark in blocks with Medium values of entropy

Type of attack		Lena		Pepper		Baboon	
		PSNR= 48.1038		PSNR= 48.4316		PSNR= 45.1122	
		NC	BER	NC	BER	NC	BER
No attack		1	0	1	0	1	0
	Degree of noise						
Salt & Pepper with different density	0.001	0.9994	0.0009	0.9994	0.0009	0.9994	0.0009
	0.01	0.9805	0.0293	0.9792	0.0313	0.9850	0.0225
	0.02	0.9310	0.1016	0.9411	0.0869	0.9667	0.0498
	0.03	0.9180	0.1201	0.8930	0.1553	0.9284	0.1055
Speckle Noise With different density	0.001	1	0	1	0	1	0
	0.005	0.9922	0.0117	0.9948	0.0078	1	0
	0.009	0.9818	0.0273	0.9935	0.0098	0.9974	0.0039
Gaussian Noise With different density	0.00001	0.8867	0.1631	0.8873	0.1641	0.9326	0.0.996
	0.001	0.8948	0.1523	0.9084	0.1338	0.9240	0.1113
	0.005	0.8841	0.1660	0.8912	0.1572	0.9292	0.1045
	0.009	0.8743	0.1816	0.8855	0.1650	0.9260	0.1084
Poisson Noise		0.9916	0.0127	0.9942	0.0088	0.9981	0.0029
Compression with different Quality factors	0.80	1	0	1	0	1	0
	0.75	1	0	1	0	1	0
	0.50	0.9994	0.0009	1	0	0.9987	0.0020
Median 3×3		0.9929	0.0107	0.9935	0.0098	0.9385	0.0908
Mean 3×3		0.9935	0.0098	0.9974	0.0039	0.9425	0.0850

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Brightness+50	0.9877	0.0186	1	0	0.9981	0.0029
Brightness+25	0.9994	0.0009	1	0	1	0
Histogram	0.9968	0.00994	0.9994	0.0009	0.9994	0.0009
Sharpen	1	0	1	0	1	0
Cropping Upper Left	0.9870	0.0145	0.9780	0.0332	0.9837	0.0244
Cropping Center	0.9025	0.1426	0.8736	0.1836	0.9064	0.1387
Rotation 10	1	0	1	0	1	0
Rotation 20	0.9261	0.1084	0.9282	0.1055	0.8041	0.2734
Rotation 180	0.9452	0.0811	0.9458	0.0801	0.8321	0.2373
Gaussian filter	1	0	1	0	1	0
Resize 256	1	0	1	0	1	0
Gamma correction	1	0	1	0	1	0

When comparing the PSNR value in the above table (6) with the PSNR results of the method in figure (7) of using blocks with lesser edge entropy in the embedding process, it becomes clear that the value of the PSNR is better, and this indicates that the less edge entropy method offers less imperceptibility from embedding in medium edge entropy value blocks. In addition, the value of NC and BER in table (4) illustrate that embedding in less edge entropy block has result preferable than result value of NC and BER in the table (6), so the robustness of Non-blind watermark embedding is less entropy value blocks is the better choice because its offer good trade of between imperceptibility and robustness.

The following Figures (9), (10), (11), (12), (13), (14), (15) , (16) illustrate comparison among Less, High and Medium edge entropy blocks for standard images against different attacks.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

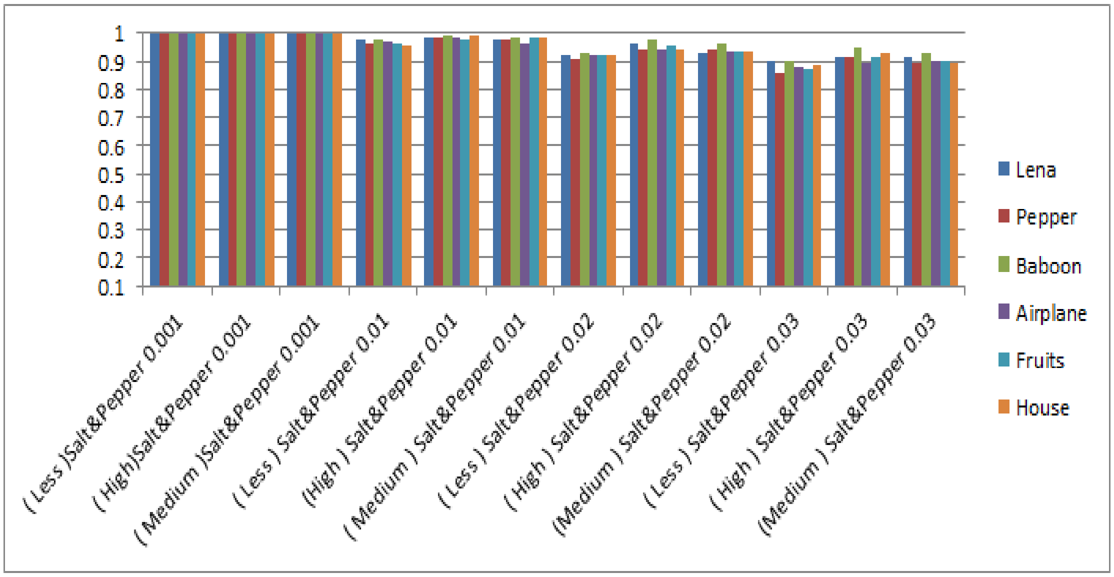


Figure (9) NC Values of reconstructed watermarked against Salt & Pepper Noise Attack

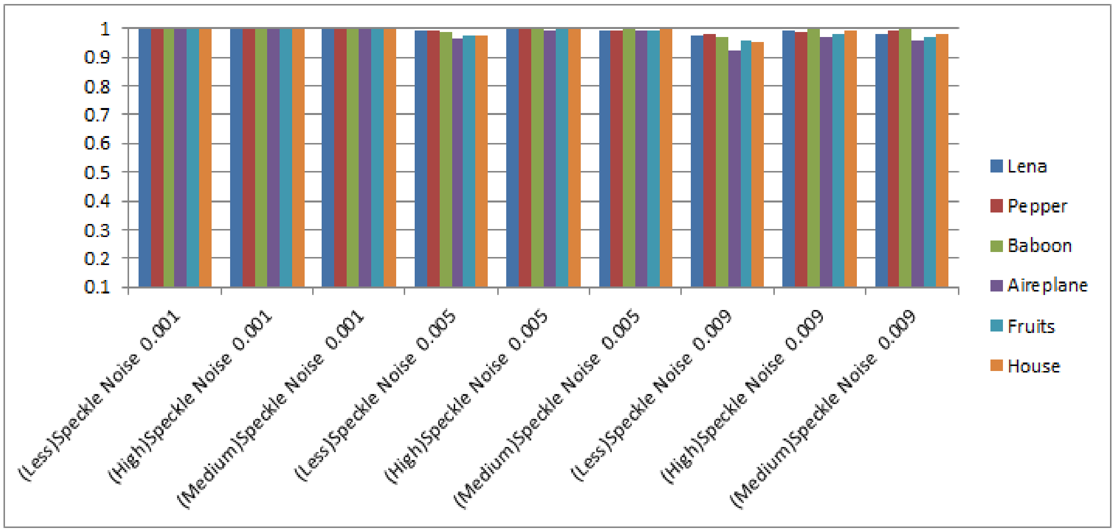


Figure (10) NC Values of reconstructed watermarked against Speckle Noise Attack

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

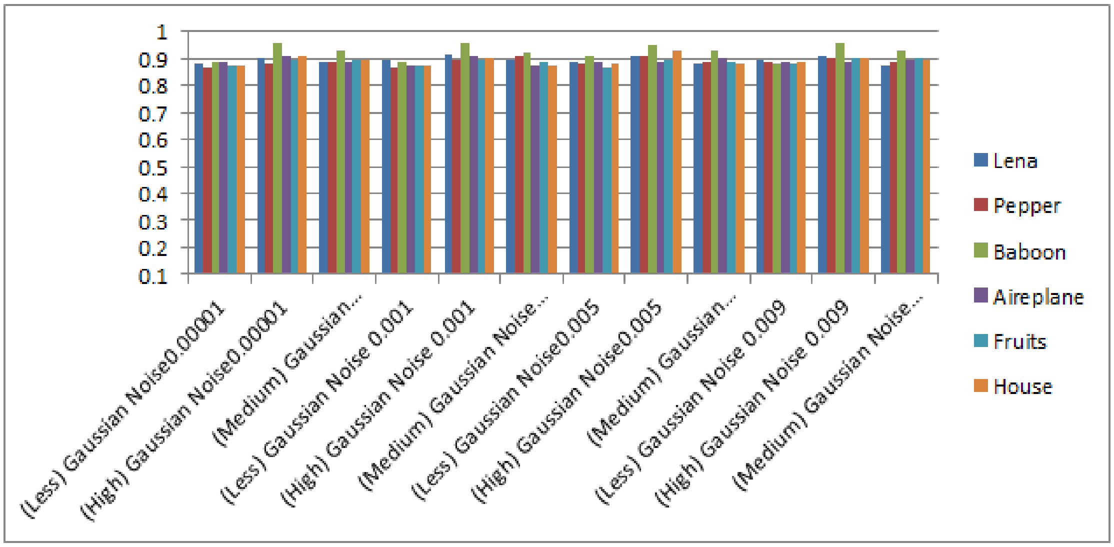


Figure (11) NC Values of reconstructed watermarked against Gaussian Noise Attack

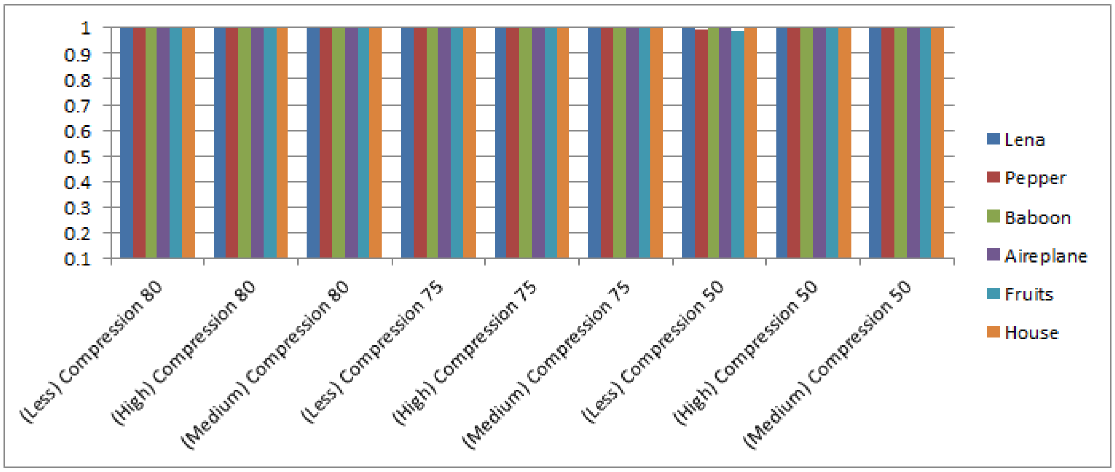


Figure (12) NC Values of reconstructed watermarked against Compression Attack

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

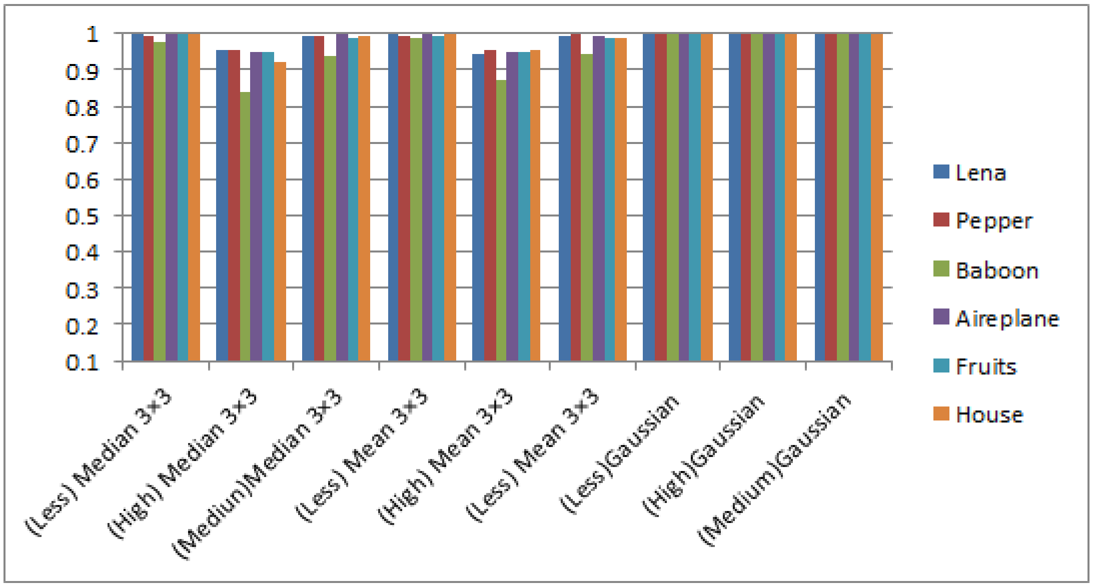


Figure (13) NC Values of reconstructed watermarked against Filtering Attack

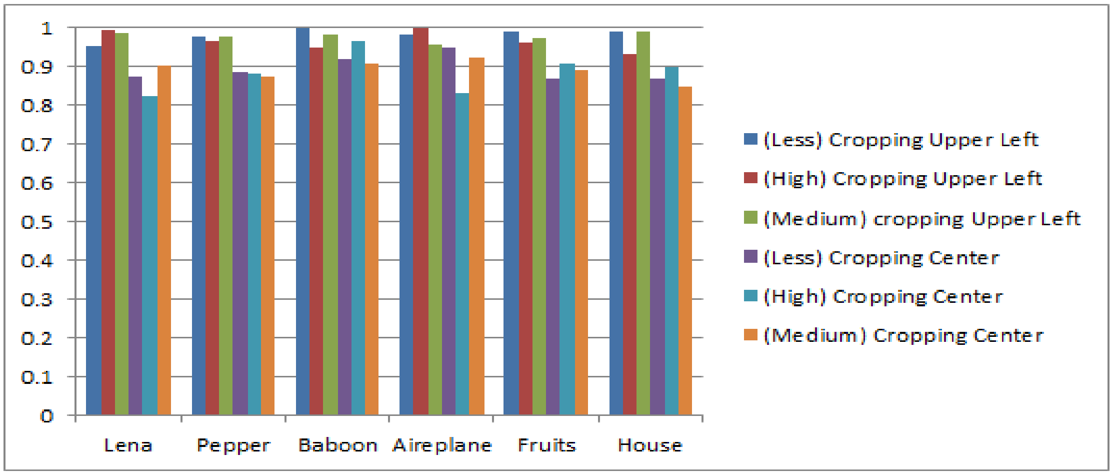


Figure (14) Comparison among Non-Blind Methods Cropping Attack

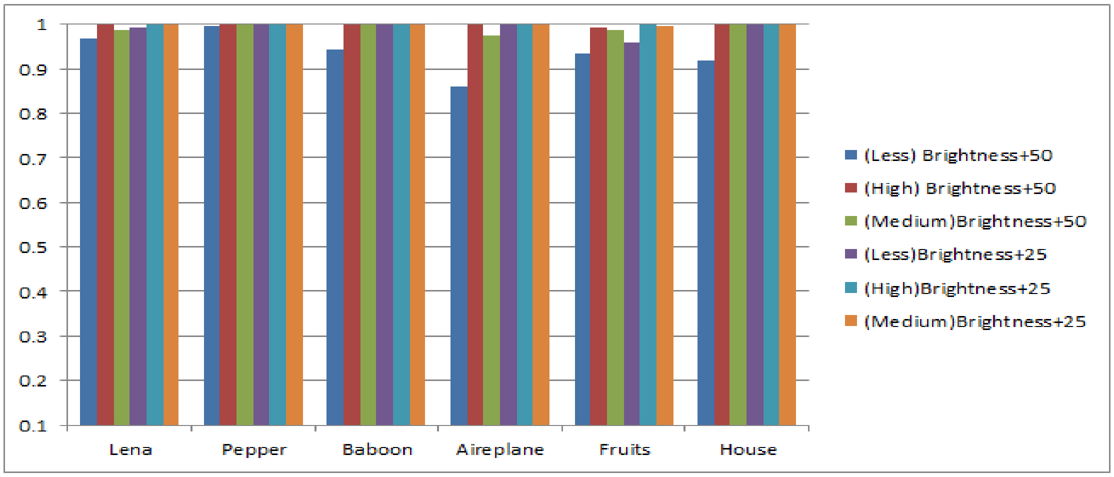


Figure (15) NC Values of reconstructed watermarked against Brightness Attack

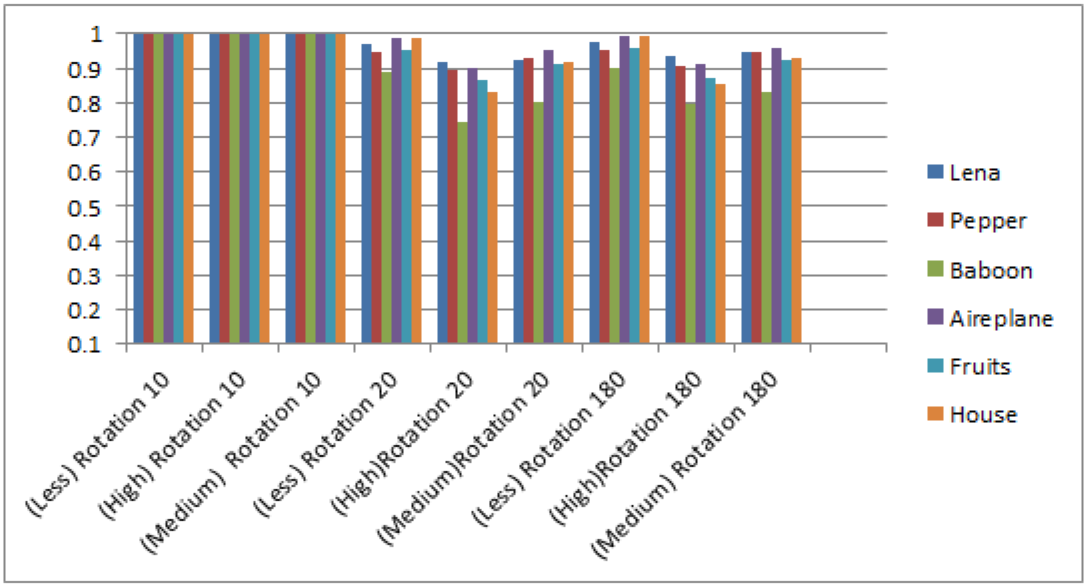


Figure (16) NC Values of reconstructed watermarked against Rotation Attack

5. Conclusion

In this paper, we suggested a Non-blind robust watermarking system for copyright protection of the digital color image. The embedding process is implemented into the frequency domain by applying both DWT and DCT transforms respectively on the cover image. The embedding process uses a scaling factor to increase robustness against different attacks. The large value of the scaling factor can cause a blocky effect in smooth blocks

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

while obtaining good robustness against attacks. Therefore, this paper it adopting a technique based on the standard deviation value to choose the variable value of the scaling factor to make a trade-off between robustness and imperceptibility. As well as, in the suggested method, the entropy metric is used to determine the appropriate locations for embedding to increase the imperceptibility. It can be concluded from obtaining results that the best blocks depending on entropy metric for embedding are the ones with low entropy because they introduce the best trade-off between imperceptibility and robustness. The proposed system tested against different types of attacks and provides very good strength. Also, the system fulfilled the security and imperceptibility requirements for any watermarked system.

Conflict of interests.

There are non-conflicts of interest.

References

[1] Singh, Neha and Joshi, Sandeep and Birla, Shilpi, "Color Image Watermarking with Watermark Authentication against False Positive Detection Using SVD", *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India* , 2019.

[2] Guoqing Hu, and Xinlong Chen ," An Adaptive Color Image Visible Watermark Algorithm Supporting for Interested Area and its Application System Based on Internet" , *MATEC Web of Conferences* , Vol. 25, 6 October , 2015

[3] X. Liu, C. Lin and S. Yuan, "Blind Dual Watermarking for Color Images' Authentication and Copyright Protection,", *IEEE Transactions on Circuits and Systems for Video technology*, vol. 28, no. 5, pp. 1047-1055, May 2018.

[4] O. Jane, E. Elba, and H. G. İlk, " Hybrid Non-Blind Watermarking Based on DWT and SVD", *Journal of Applied Research and Technology*, Vol.12, Issue 4, Pages 750-761,2014.

[5] Yong-Seok Lee , Young –Ho Seo ,and Dong – Wook Kim , "Blind Watermarking Based on Adaptive Data Spreading in n – Level DWT Subbands" , *Security and communication Networks* , vol.2019 , 2019.

[6] Podili Brahma Srinu, B.Jagadeesh ,” Copyright Protection of Digital Images using FIS-BPNN Technique in Hybrid Transform Domain”, *International Journal of Innovative Research in Science, Engineering and Technology*, Vol.5, No. 10, October 2016.

[7] Rita Choudhary, and Girish Parmar , "A robust image watermarking technique using 2-level discrete wavelet transform (DWT), 2016 2nd International Conference on Communication control and Intelligent Systems (CCIS), Mathura, India, pp. 120-124,2016.

[8] Mohammad Moosazadeha, and Gholamhossein Ekbatanifard,” An Improved Robust Image Watermarking Method Using DCT and YCoCg-R Color Space ” , ” *International Journal for Light and Electron Optics* “ Vol.140 , 2017,

[9] Jianzhong Li , Chuying Yu , B. B. Gupta ,and Xuechang Ren . ”Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition”,*Multimed Tools Appl* ,pp. 4545–4561, (2018).

[10] Nesrine Tarhouni, Chokri Ben Amar ,and Maha Charfeddine , “A New Robust and Blind Image Watermarking Scheme In Frequency Domain Based On Optimal Blocks Selection “, *Short Papers Proceedings*, 2018.

[11] Te-Jen Chang, Hui Pan, Ping-Sheng Huang, and Chen-Hao Hu,” A robust DCT-2DLDA watermark for color images”, *Multimed Tools Appl* , pp.9169–9191 ,2018.

[12] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-samie. " Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map", *American Journal of Signal Processing*, vol. 6, no. 1, pp. 1–13,2016.

[13] Gambhir Singh, and Rakesh Kumar Yadav "DNA Based Cryptography Techniques with Applications and Limitations" , *International Journal of Engineering and Advanced Technology (IJEAT)* ,Vol. 8 , No. 6, August 2019.

[14] Junxin Chen , Zhi-liang Zhu , Li-bo Zhang , Yushu Zhang , and Ben - qiang Yang ,"Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption" , *Signal Processing* ,Vol.142,pp. 340-353 , January ,2018.

[15] Mandrita Mondal , and Kumar S. Ray ,"Review on DNA Cryptography", *ArXiv* ,(2019) .

[16] Guesmi , M. A. B. Farah , A. Kachouri and M. Samet ,"A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2",*Nonlinear Dyn 83*, pp.1123–1136, 14 Septwmber (2015)

[17] Malika Narang, and Sharda Vashisth.," Digital Watermarking using Discrete Wavelet Transform.In", *International Journal of Computer Applications*, Vol. 74, No. 20, July 2013.

[18] Abhigyakari, Neetesh Raghuwanshi and Anurag Rishishwar, " A Review of Digital Water Marking Techniques and Uses' , " *In :International Journal of Electrical, Electronics and Computer Engineering*". Vol.4 , No. 2 , pp. 66-74, 2015.

[19] Mitesh Patel , and Swati Patel ," To study Digital watermarking technique based on DCT and DWT", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* **,** Vol.3 No. 5, May,2014.

[20] Aymen Mudheher Badr, Mohammed Layth Talal, and Ghassan Sabeeh Mahmood "A novel Digital watermarking technique based on STD (standard division) "," *International Journal of Scientific & Engineering Research*" . Vol.6, No.4, April ,2015.

[21] Gurpreet Kaur, and Kamaljit Kaur "Implementing LSB on Image Watermarking Using Text and Image",*International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 8, August , 2013.

[22] Chuying Yu , Xiaowei Li, Xinan Chen and Jianzhong Li," An Adaptive and Secure Holographic Image Watermarking Scheme" , "*entropy*", 2019.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com