DWT-DCT-Based Watermarking Technique

Najla'a Abd Hamza AL-Mayahee,
Baghdad University
Amera Abdul-Wohid Funjan Al-Tayee And Hanna Muhassen Ali
Babylon University

Abstract

This research proposes a watermarking scheme for digital images. It uses a discrete wavelet transform (DWT) prior to the Discrete Cosine transform (DCT) to provide better imperceptibility in harmony with the human visual system, and higher robustness against signal processing attacks.

In this research, DWT is implemented for the cover image, and then applying the DCT to the DWT sub bands, binary watermark (payload) is modulated by exclusive-or (XOR) operation with a key to increase the security of the system and then embedding in the middle frequency DCT coefficients. The key is secret and stored inside the cover image to increase the robust of the system.

الخلاصة:

يقترح البحث تقنية علامة مائية للصور الرقمية، وقد استخدم التحويل الموجي المتقطع ومن ثم تحويل الجيب تمام المتقطع في هذه الطريقة لتوفر غموض اكثر (عدم رؤيا) بالنسبة لنظام الرؤيا البشري وتوفير اعلى حماية ممكنة ضد هجمات معالجة الاشارة. في هذا البحث قد تم اجراء التحويل الموجي المتقطع على الصورة الغطاء، ومن ثم اجراء تحويل الجيب تمام المتقطع على قطاعات التحويل المويجي وان العلامة المائية الرقمية(المعلومات المراد اخفائها) قد تم اجراء عملية التغيير (التحويل) عليها قبل اجراء عملية الاخفاء وذلك لزيادة امنية النظام، ومن ثم تم اخفائها في الترددات الوسطى لمعاملات الجيب تمام. وان المفتاح المستخدم في هذه الخوارزمية هو من نوع المفتاح السري وقد تم خزنه داخل الصورة الغطاء لزيادة حصانة هذا النظام.

1. Introduction

The advent of the Internet has resulted in many new opportunities for creating and delivering content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is protection of the rights of content owners. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest in developing new copy deterrence and protective mechanisms. One approach that has been attracting increasing interest is based on *digital watermarking* techniques [1]. Digital watermarking is a scheme of embedding data in an image called host image for the purpose of copyright protection, integrity check, and/or access control . Some of the requirements of digital watermarking are transparency, robustness, and capacity. Specifically, transparency means that the watermark embedded in the host image is imperceptible to human eyes, robustness means the resistance of the watermark to malicious attacks, and capacity denotes the amount of data that can be hidden in the host image. Digital watermarking has been applied to many applications [2]

2. Digital Watermarking Systems

Digital watermarking system consists of two main components: *watermark embedder* and *watermark detector*, as illustrated in Figure 2 and figure 3. The embedder combines the *cover work* C_o , an original copy of digital media (image, audio, video), and the *payload P*, a collection of bits representing metadata to be added to the cover work, and creates the *watermarked cover* C_w . The

watermarked cover C_W is perceptually identical to the original C_O but with the payload embedded in. The difference between C_W and C_O is referred to as *embedding distortion.* The payload *P* is not directly added to the original cover C_O. Instead, it is first encoded as a *watermark W,* possibly using a secret key *K*.

The watermark is then modulated and/or scaled, yielding a *modulated watermark* W_M *,* to ensure that embedding distortion will be small enough to be imperceptible.

Before it gets to a detector, the watermarked cover C_W may be subjected to different types of processing yielding *corrupted watermarked cover* $C_W^{\wedge}$. This corruption could be caused either by various distortions created by normal signal transformations, such as compression, decompression, D/A and A/D conversions, or by distortions introduced by various malicious attacks. The difference between $C_W^{\wedge}$ and C_W is referred to as *noise N*.

Watermark detector either extracts the payload *P*ˆ from the corrupted watermarked cover $C_W^{\wedge}$, or it produces some kind confidence measure indicating how likely it is for a given payload *P* to be present in $C_W^{\wedge}$. The extraction of the payload is done with help of a watermark key*K* .

Watermark detectors can be classified into two categories, *informed* and *blind*, depending on whether the original cover work C_O needs to be available to the watermark detection process or not. *Informed detector*, also known as a non-blind detector, uses the original cover work C_O in a detection process. *Blind detector*, also known as an oblivious detector, does not need the knowledge of the original cover C_O to detect a payload.[3]

Watermarking schemes can be robust or fragile. A robust watermarking scheme is designed to resist to malicious or intentional distortions, such as general image processing and geometric distortions; while a fragile watermarking scheme is designed for the purpose of authentication and verification. We can also classify watermarking schemes according to operation domain: the spatial domain and frequency domain.

The watermarking scheme based on the frequency domains can be further classified into the Discrete Cosine Transform (DCT) (Cox *et al.*, 1997; Hsu and Wu, 1999), discrete wavelet transform (DWT) (Hsu and Wu, 1998; Tsai *et al*., 2000; Barni *et al*., 2001) and Discrete Fourier Transform (DFT). There are many DCT-based schemes proposed. But more and more researches focus on the DWT approaches because DWT is used in the upcoming JPEG2000 standard[3]. The watermarking scheme proposed in this research is based on the DWT approaches and DCT approaches.

3. Concepts of Substitution systems

Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits, the receiver can extract the information if he has knowledge of the position where secret information has been embedded. Since only minor modification is made in the embedding process, the sender assumes that they will not be noticed by an attacker. Substitution system may be grouped into eight categories as follows:

1. Least Significant Bit Substitution (LSB).
2. Pseudorandom Permutation.
3. Image Downgrading and cover channels.
4. Cover Regions and Parity Bits.
5. Palette-based Image.
6. Quantization and Dithering.

7. Information Hiding in Binary Images.
8. Unused or Reversed Space in Computer Systems.

In the Least Significant Bit Substitution (LSB), the embedding process consists of choosing a subset $\{j_1,..., j_{\ell(m)}\}$ of cover elements and performing the substitution operation $c_{ji} \leftrightarrow m_j$ on them, which exchange the LSB of C_{ji} by m_i (can be either 1 or 0). [4]

We will now go over an example that involves inserting an A into 3 pixels of a 24 bit image. Here is the original raster data:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value of A is 10000011 and encoding A into the last bits of this 3 pixel sequence will change the above sequence to:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001).

Notice that only the underlined bits had to be changed in order to create the A. On the average only have of the bits would have to be changed in an LSB(Least Significant Bit) encoding scheme. With such a small variation in the colors it would be very difficult for the human eye to discern the difference.[5]

In the extraction process, the LSB of the selected cover image is extracted and lined up to reconstruct the secret message. This basic scheme is presented in the following algorithm

Algorithm Embedding Process: Least Significant Bit Substitution

For i=1,…, $\ell(c)$ do

$s_i \leftarrow c_i$

End for

For i=1,…, do

Compute index j_i, where to store i-th message bit

$s_i \leftarrow c_i = m_i$

End for

Algorithm Extraction Process Least Significant Bit Substitution

For i=1,…, $\ell(m)$ do

Compute index j_i, where the i-th bit is stored

$m_i \leftarrow LSB(c_{ij})$

End for

Amore sophisticated approach is the use of a pseudorandom number generator to spread the secret message over the cover in a rather random manner. a popular approach is the random interval method. If both communication partners share a stego-key k usable as a seed for a random number generator. They can create a random sequence $\{k_1,\cdots\cdots,k_{\ell(m)}\}$.Thus, the distance

between two embedded bits is determiner pseudorandomly. Since the receiver has access to the seed k and knowledge of the pseudorandom number generator. This basic scheme is presented in the following algorithm[4]

Algorithm Embedding Process Random Interval Method

For i=1,…, $\ell(c)$ do

$s_i \leftarrow c_i$

End for

Generate random sequence k_1 using seed k

$n \leftarrow k_1$

For i=1,…, $\ell(M)$ do

$s_n \leftarrow c_n = m_i$

$n \leftarrow n + k_1$

End for

Algorithm Extraction Process Random Interval Method

Generate random sequence k_1 using seed k

$n \leftarrow k_1$

For i=1,…, $\ell(M)$ do

$m_i \leftarrow LSB(c_n)$

$n \leftarrow n + k_1$

End for

4. Concepts of Discret Image Transform

The concept of a transform is familiar to mathematicians. It is a standard mathematical tool used to solve problems in many areas. The idea is to change a mathematical quantity (a number, a vector, a function, or any thing else) to another form, where it may look unfamiliar but may exhibit useful features. The transformed quantity is used to solve a problem or perform a calculation, and the result is then transformed back to the original form [6].

The general form of the transformation equation for N×N images is given by:

$$T(u,v) = \sum_{r=0}^{N-1}\sum_{c=0}^{N-1} I(r,c)B(r,c;u,v) \quad .....(1)$$

Where I(r,c) is the original image, T(u,v) are the transform coefficients, B(r,c;u,v) correspond to the basis image, r and c are the spatial domain variable, and u and v are the frequency domain variable. The transform coefficients T(u,v) are the projections of I(r,c) onto each B(u,v).These coefficients tell how similar the image is to the basis image. By applying the inverse transform, one can obtain the image form the transform coefficients as follows:-[7]

$$I(r,c)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}T(u,v)B^{-1}(r,c;u,v) \quad \ldots.(2)$$

Hence the $B^{-1}(r,c;u,v)$ represent the inverse basic images.

There are several transformation types: Fourier Transform, Discrete Cosine Transform, Walsh –Hadmard Transform, and Wavelet Transform.

5. Concepts of Discrete Cosine Transform(DCT):

Most popular among block transform is DCT, Which partitions an input image into non-overlapped blocks, then transforms them into blocks of coefficients.

The discrete cosine transform (DCT) has been used in JPEC and MPEG compression successfully at decorrelating and concentrating the energy of pixel data into spatial domain. In this format, the information lends itself to loosy quantization and compression in a manner that is almost invisible to Human Visual System[7].

Assming N * N image, its two dimensional DCT produces the (N * N) array of numbers, its given by[8]:

$$T(u,v)=\alpha(u)\alpha(v)v\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}I(r,c)\cos\frac{(2r+1)u\pi}{2n}\cos\frac{(2c+1)v\pi}{2n} \ldots. (3)$$

where $$\alpha(u),\alpha(v)=\begin{cases}\frac{1}{\sqrt{n}} & if \quad u,v=0\\ \frac{2}{\sqrt{n}} & if \quad u,v=1,2,..n-1\end{cases} \quad \ldots.(4)$$

The inverse DCT is :-

$$I(r,c)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)\cos\frac{(2r+1)u\pi}{2n}\cos\frac{(2c+1)v\pi}{2n} \quad \ldots.(5)$$

Where u,v varies from 0 to n-1.

The result of the DCT is the square (N * N) array T(u,v) of real numbers, The coefficients T(0,0) is called the "DC coefficient" and the remaining are called the AC coefficients.

6. The Wavelet Transform:-

The wavelet transform (wt) has been adopted as the standard tool in JPEG 2000 still image compression as it produces a higher compression ratio than the DCT does. Studies of image compression also show that the wavelet transform provides better frequency and time (spatial) resolution than other transform techniques do[9].

The basic idea of the DWT for a one dimensional signal is as follows. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely confined in the high frequency part. The low frequency part is split again into two parts of high and low frequency. This process is continued until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking application, generally no more than five decomposition steps are computed. Furthermore, from the DWT coefficients, the original signal can be reconstructed. The reconstruction process is called the inverse DWT (IDWT). Mathematically, the DWT and IDWT can be stated as follows. Let

$$\mathrm{H}(\omega)=\sum_{\mathrm{k}}h_k.e^{-jk\omega}, \quad \ldots. \qquad (6)$$

and

$$G(\omega) = \sum_{k} g_k \cdot e^{-jk\omega} \quad \ldots. \qquad (7)$$

be a low-pass and a high-pass filter, respectively, which satisfy certain conditions for the reconstruction stated later. A discrete signal, F(n) can be decomposed recursively as

$$f_{j-1}^{low}(k) = \sum_{n} h_{n-2k} f_j(n) \quad \ldots. \qquad (8)$$

And $$f_{j-1}^{high}(k) = \sum_{n} g_{n-2k} f_j(n) \quad \ldots \qquad (9)$$

for $j = J+1, J, ..., J_0$ where $f_{J+1}(k) = F(f), k \in Z.J+1$ is the highest resolution level index and J_0 is the low resolution level index. The coefficients $f_{J_0}^{low}(k), f_{J_0}^{high}(k), f_{J_{0+1}}^{high}(k), ..., f_J^{high}(k)$ are called the DWT of the signal F(n), where $f_{J_0}^{low}(k)$ is the lowest resolution part of F(n) (the approximation) and the $f_j^{high}(k)$ are the details of F(n) at various bands of frequencies. Furthermore, the signal F(n) can be reconstructed from its DWT coefficients recursively,

$$f_j^{low}(n) = \sum_{k} h`_{n-2k} \cdot f_{j-1}^{low}(k) + \sum_{k} g`_{n-2k} \cdot f_{j-1}^{high}(k). \quad \ldots. \qquad (10)$$

The DWT and IDWT for a two dimensional image *F(m,n)* can be similarly defined by implementing the one dimensional DWT and IDWT for each dimension *m* and *n* separately resulting in the pyramidal representation of the image[10],where HH,HL,LH are the higher resolution subbsnds and the less sensitive components, LL is the lowest resolution subbands, which contains the most energy in the image[3]. The use of wavelets in image coding has increased significantly over the years, mainly due to the superior energy compaction property of wavelets compared with the traditional transforms like the DCT. The new compression standard, JPEG 2000, is based on the Discrete wavelet transform, for example [10].

There are several reasons to use the DWT domain [3]:-

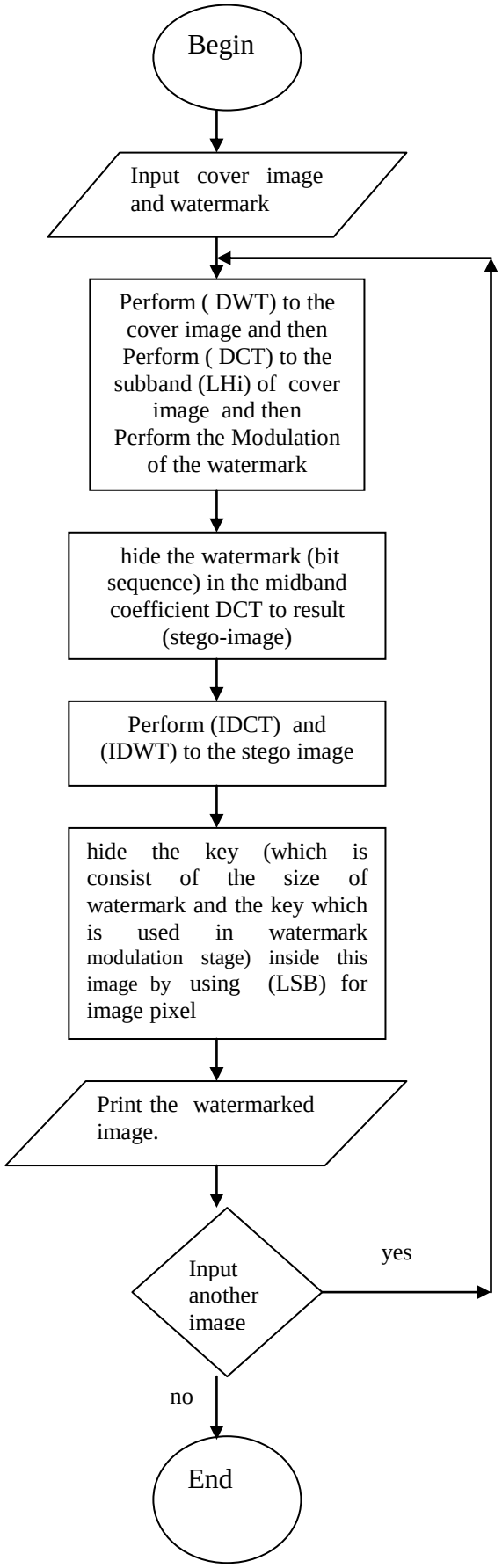
1. The DWT domain is the kernel technique of JPEG-2000.
2. The DWT is highly integrable with JPEG-2000.
3. The goal to be robust against JPEG-2000 compression is achieved.
4. The DWT based approach usually produce watermarked images with the best tradeoff between transparency and robustness while the DFT and DCT domain approach have blocking artifacts

7. DWT-DCT- Based Watermarking Algorithm:-

The main purpose for inserting the watermark in the transform domain is the resulting dispersion of the watermark in the spatial domain, hence it become very difficult to remove the watermark from the image. The algorithm consists of two parts: the embedding process and the extraction process as shown details in the following sections .It is high invisibility and robustness as the experimental results demonstrate.

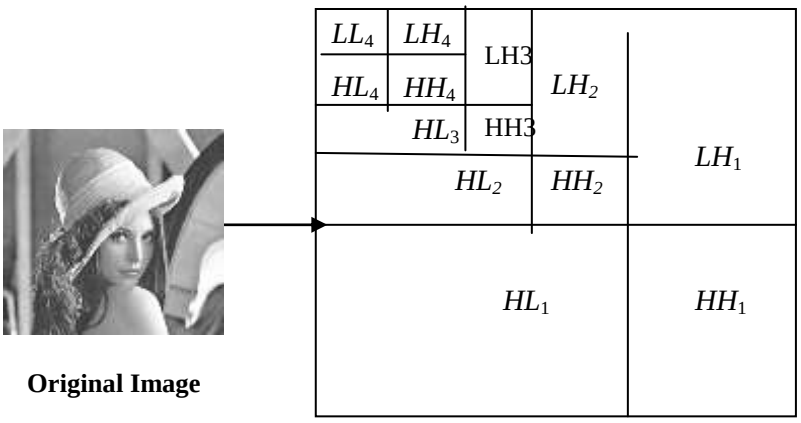
7.1. The embedded process:-

The embedded process consists of several stage:-Transformation Stage, Watermark Modulation, Extract midband coefficients, Hidden Stage and Inverse Transformation Stage, as shown in the following flow chart.


Begin
Input cover image and watermark
Perform (DWT) to the cover image and then Perform (DCT) to the subband (LHi) of cover image and then Perform the Modulation of the watermark
hide the watermark (bit sequence) in the midband coefficient DCT to result (stego-image)
Perform (IDCT) and (IDWT) to the stego image
hide the key (which is consist of the size of watermark and the key which is used in watermark modulation stage) inside this image by using (LSB) for image pixel
Print the watermarked image.
Input another image
yes
no
End

7.1.1. Transformation Stage:-

The original image (cover image) is decomposed with a four-level DWT the result of decomposition is (12) frequency subbands of high frequency (*HHi, HLi, LHi, i=1..4*) and one low frequency subband (*LL4*) as shown in figure(1).by using the following steps:



Figure(1): four-level DWT

Step 1: -Convolve the lowpass filters with rows and save the results. Step 2: -Convolve the lowpass filters with the columns (of the result from step 1) to obtain the lowpass-lowpass(LL)subimage . Step 3: -Convolve the result from step 1,the lowpass filtered rows, with the highpass filter on the columns. To produce the Lowpass-Highpass (LH) Subimage.
Step 4: -Convolve the original image with the Highpass filters on the rows and save the result.

Step 5: -Convolve the results from step 4 with the lowpass filter on the columns; Subsamples to yield the Highpass-Lowpass (HL) subimage.

Step 6: - To obtain the Highpass-Highpass (HH) subimage, convolve the columns of the Result from step 4 with Highpass filter[11]

After applying the DWT, then applying the DCT to particular (DWT) sub bands (LHi) in order to increase robustness against attacks like compression, cropping, rotating, etc, the sub bands of cover image are partitions into blocks of (8*8) pixels, these blocks will be transformed using DCT to get on blocks of (8*8) coefficients of real numbers.

For example a 512× 512 pixel image, the first level, the subband (LH1) consist of 256×256 pixel, therefore, a total of 1024 blocks of transform coefficients is generated, in the second level, the subband (LH2) consist of 128×128 pixel, therefore, a total of 256 blocks of transform coefficient is generated, in the third level, the subband(LH3) consist of 64 ×64 pixel, a total of 64 block is generated, in the last level , the subband (LH4) consist of 32 ×32 pixel, a total of 16 block is generated, therefore a total of 1360 block of transform coefficient is generated by the DCT stage.

After each(8*8) block of DCT coefficients is calculated, it is quantized to transform the real number to integer numbers. Each number in the DCT coefficient block is divided by the corresponding number (quantizer number), and the result is rounded to the nearest integer.

The quantizer value based on one parameter R is supplied by the user. The equation (11) is used to measure the corresponding number (quantizer number).

$$Q_{ij} = 1 + (i + j)/R \quad \ldots(11)$$

Where i, j range from 1 to n. [12]

7.1.2 Watermark Modulation Stage:-

The watermark, $L=[1_1,1_2,\ldots,1_N]$ with $l_i \in \{0,1\}$, is a bit sequence with length N. The bit sequence may be a meaningful image such as the logo or a binary sequence which can indicate a legal owner uniquely of the images. [10]

The watermark is modulated to increase the security of the system by a bit-wise logical XOR operation with Keyword, (the value of key is determined by the user must be in range [0..9]) to give the modulated watermark as shown in Figure (2) by using the equation (12)[13].

$$p \oplus k = c \qquad \ldots..(12)$$

Where:-

P: is a plaintext.

K: is a keyword.

C: is a ciphertext.

The values of the keyword is regarded as key for the algorithm and stored inside the cover image to increase the quality the system.

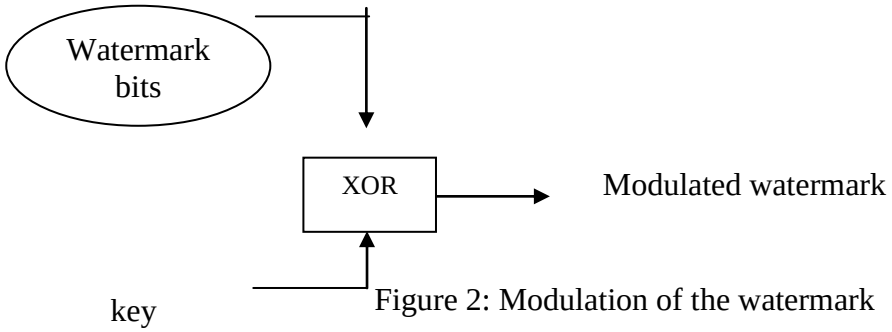


Figure 2: Modulation of the watermark

7.1.3 Extract midband coefficients:-

In this stage, the algorithm will select the required midband coefficients from the transform domain coefficient (LHi) as shown in figure(3)

0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7
1,0	1,1	1,2	1,3	1,4	1,5	1,6	1,7
2,0	2,1	2,2	2,3	2,4	2,5	2,6	2,7
3,0	3,1	3,2	3,3	3,4	3,5	3,6	3,7
4,0	4,1	4,2	4,3	4,4	4,5	4,6	4,7
5,0	5,1	5,2	5,3	5,4	5,5	5,6	5,7
6,0	6,1	6,2	6,3	6,4	6,5	6,6	6,7
7,0	7,1	7,2	7,3	7,4	7,5	7,6	7,7

→

2,3	3,3	4,3	5,3
2,4	3,4	4,4	5,4

Figure(3): midband coefficient selection

7.1.4:Hidden Stage:

In this stage, the algorithm will hide the watermark (bit sequence) in the midband coefficient DCT. The algorithm depends on Pseudorandom Permutations method (described in section 3) for midband coefficient in hidden process, where the watermark bit is distributed randomly over the

middle frequency bit. The distribution between pixel and pixel by the distribution distance is calculated by [14]:-

mm= (wid*hig)div (size of the watermark*8)…..(13)

Where:-

wid=width of subband(LHi).

hig=high of subband(LHi).

For example, a 512× 512 pixel image, the size of each block is (8*8) pixel, the watermark is 4byte, then:

mm=(64)div(4*8)=2

therefore, the watermark pixel is hiding in the first midband coefficient (by exchange the LSB of this coefficient by first watermark pixel), then leave distance(2) and go (jump) to fourth midband coefficient to hide second pixel , therefore , only 3 coefficient is exchange in one block)

7.1.5 Inverse Transformation Stage:-

After perform Hidden Stage, the algorithm will perform inverse transformation stage, The algorithm will perform inverses quantization (dequantization). BY each number in DCT quantization coefficient is multiplied by the corresponding number(the same number which used in quantization step)

Then, the algorithm will perform (IDCT) to get the original number of pixel in subbands.

After apply (IDCT) , The algorithm will perform (IDWT) to get the watermarked image.

The inverse wavelet transform performed by enlarging the wavelet transform data to its original size. Insert zeros between each two values horizontally and vertically, then convolve the corresponding (lowpass and highpass) inverse filters to each of the four sub images, and sum the results to obtain the original image.

The procedure of Inverse wavelet transform doing by many steps:-

Step 1: Upsample the rows for each Sub-bands (LL, LH, HL, HH) by inserting zero between every two samples.

Step 2: Convolve the rows result from step1 with low and high pass filter, where the sub-bands (LL, LH) with low pass filter and (HL, HH) with the high pass filter.

Step 3: Upsample the columns for the result from step2 by inserting zero between every two samples.

Step 4: Convolve the result from step 3 with low pass and high pass filters, where the sub-bands (LL, HL) with the low pass filter and (LH, HH) with high pass filters.

Step 5: Add the results from step 3 with the result from step 4 and save the result.[8]

After get the watermarked image, the algorithm will hide the key (which is consist of the size of watermark and the key which is used in watermark modulation stage) inside this image by using Least Significant Bit Substitution (LSB) for image pixels (described in section 3).

7.2.The Extraction Process

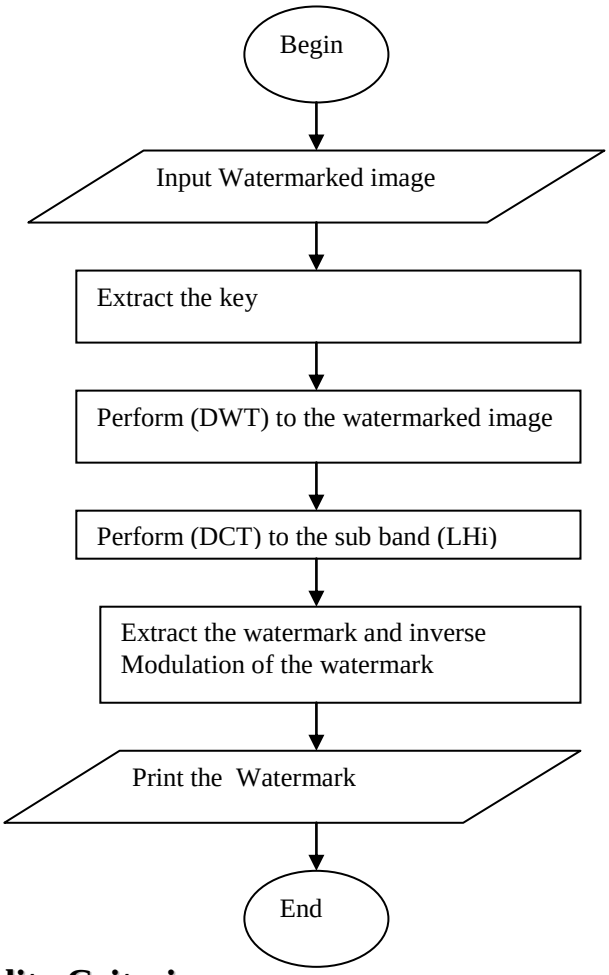
The extraction process contains of three stage:- Key Extraction, transformation Stage and watermark Extraction.

In the Key Extraction stage, the algorithm will extract the key from the watermarked image by extracted the LSB of the selected image elements and lined up to reconstruct the secret key, from the first byte, the extractor will known the size of watermark, from the second byte, the extractor will known the modulation key.

In the transformation stage, the watermarked image is decomposed to four levels DWT, then applying the DCT to particular (DWT) sub bands (LHi).

In the watermark Extraction, the algorithm will extract the watermark from the same coefficients which is used in the embedded process (midband coefficient) by applying Pseudorandom Permutations extraction from midband coefficient(inverse Pseudorandom Permutations hiding), therefore, must calculate the hidden distance (mm) between pixels by

performing the equation (13) to reconstruct the wastermark by extracted the LSB of the selected midband coefficient (which in subband LHi) and leave distance(mm) to get the other LSB, The extracted bits are then XOR ed with the same key which is used for embedding to produce the extracted watermark, as shown in the following flow chart.



8. Image Fidelity Criterion:-

There are two types of fidelity criteria; namely, the objective and the subjective criteria. The first one provides us with equations that can be used to measure the amount of the error in the reconstructed image, whereas the second requires the definition of qualitative scale to assess image quality, and this scale can be used by human test subjects to determine image fidelity.

In order to provide unbiased results, evaluation with subjective measure requires careful selection of the test subjects and carefully-designed evaluation experiments. The objective criteria are useful as relative measures in comparison with different versions of the same image. Commonly used objective measure are the peak signal-to-noise ratio(PSNR) which is the main test that gives a good metric for security and equality of the stego image. The PSNR is usually measured in dB and can be defined as[11]:-

$$PSNR = 10\log_{10}\frac{(l-1)^2}{\frac{1}{M\times N}\sum_{r=0}^{N-1}\sum_{c=0}^{M-1}[I_2(r,c)-I_1(r,c)]^2} \quad \text{..... (14)}$$

Where:-

M: is the height of the two images(because the two images must be the same size).

N: is the width of the two images.

r and c: are row and column numbers.

l: is the number of the gray levels.

$I_1(r,c)$:is the original image.

$I_2(r,c)$:is the modified image.

9. The Results:-

In this section we demonstrate the performance of our algorithm using our proposed method on grayscale test images of sizes 512×512 pixels, and the watermark is binary sequence (name for image)

Example1:-

Original image

Lena

watermark

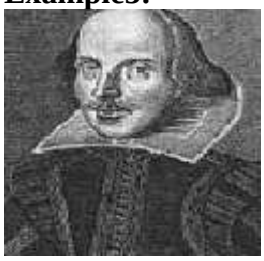
Example2:-

Original image

cat

watermark

Example3:-



Original image

shik

watermark

In the following table shows the results of the test (PSNR) between the watermarked image and the original image for the previous examples:-

No of example	PSNR
1	38.67
2	39.16
3	35.65

10.Conclusions:-

After having performed the watermarking algorithm, the following conclusion can be reached:-

1. The watermark system uses the DWT/DCT combined technique provides better imperceptibility and higher robustness against the changes and treatments done for the cover image.
2. The key in watermark system is generated during the embedded process and stored inside the host image to increase the security of the system. Without knowledge of the key, the receiver cannot extract the watermark.
3. The good quality of watermarking images is achieved as shown when applying the PSNR test.

References:-

[1]R. Chandramoul, Department of ECE, Stevens Institute of Technology, Hoboken, Nj,07030, Nasir Memon, department of Computer Science, Polytechnic University, Brooklyn, ny,11201 and Majid Rabbani, imaging research and advanced development, Eastman Kodak Company, Rochester, Ny,14650, **Digital Watermarking**,2002.

[2] Lu-Tingko,Jwu-E-Chen,Yaw-Shih Shieh,His-Chin Hsin, and Tze-Yun Sung, "**Nested Quantization Index Modulation for Reversible watermarking and Its Application to healthcare Information Management Systems"**Hindawi publishing corporation, Computational and Mathematical methoda in Medicine,2011.

[3] T. Chen,G.Hory and S. Wang,"**A Robust Wavelet-Based Watermarking Scheme Using Quantization and Human Visual System Model",** Institute of Computer Science, National Chung-Hsing University,2003. .

[4] S.Katzenbeisser and F.A.Petitcolas**, Information Hiding Techniques for Steganography and Digital Watermarkin** , Artech House INC. , Boston /London , 2000.

[5] F.Queirolo, **Steganography in image**, final communications report, 1998.

[6] D. Salomon**, Data Compression**, Second Edition,Springer,2000.

[7] A. M. Jafer, **Image Steganography Using Wavelet Transform Technique**, M. Sc. Thesis, University of Baghdad,2002.

[8] S. A. Khayam, **The Discrete Cosine Transform (DCT): Theory and Application**, department of Electrical and Computer Eengineering, Michigan State University, March 10th,2003.

[9] L.Chang**, Issues In Information Hiding Techniques**, Research Supported By The Office Of Naval Research,2002.

[10] D. B. Ali," **Digital Image Watermarking Techniques For Copyright Protection",** D.Thesis, College of Computer Sciences & Mathematics, University of Mosul, 2004

[11] S.E.Umbangh, **Computer Vision and Image Processing,** Prentics Hall, London, 1998.

[12] T. A. AL-Asadia, **Ahybrid Algorithm for Image Compression**, Ph. Thesis, University of Technology, 2004

[13] J.Wiley and Sons, **Applied Cryptography**,second edition, protocols, algorithm and source code in C, Newyork. Chicheser. Brisbone. Toronto Singapore.

[14] N.A.AL-mayyahee, **New Robust Information Hiding Technique**, M.Sc.Thesis, University of Technology,2005.