

Copyright Protection And Fingerprinting For Still Digital Image By Using digital Watermarking



Ahmed Sultan Al-Hegami¹, Taha Al-Rawhani¹, Muath Shakir Al-Ubaydi²

¹Department of Information Systems
Arab Academy for Banking and Financial Sciences
Sana'a, YEMEN

²Department of Information Systems
University of Science and Technology
Sana'a, YEMEN

{mubaydi@yahoo.co.uk, ahmed_s_gamil@yahoo.com, alrawhani@yahoo.com}

ABSTRACT: *The Internet has today become the main channel to perform the e-business activities, and consequently, most of the products and services have been transformed from physical products/services to digital products/services, and the manner of delivery of such products (e.g. Journals, certificates, images, advertising, video... etc) have been converted to the digital way.*

The ease of copying and transforming digital products generates an intellectual property problem; that means, the copying and transformation of digital products will be achieved without the permission of the owner or publisher. The useful proposed way to solve intellectual property problem is digital watermarking technique. This technique has been used to keep copyright of digital products, such as audio, video, image, and general digital documents. The ownership authentication and the illegal copies identification of digital media are the main issues of the copyright protection [7], that we will discuss in this paper.

In this paper, we propose a copyright protection and fingerprinting scheme that met the main objectives: 1) Minimize the number of the original image blocks when we use the DCT transform in order to increase the speed of embedding process, (treatment of the capacity issue), 2) Raise the level of security by using unique Key to encrypt the watermark, 3) Increase the robustness to compression by JPEG and cropping, and, 4) Identify each image through buyer information (fingerprinting). We tested the proposed scheme and experiment with some common images and found the results quite promising.

Key words: Digital watermarking, Discrete Cosine Transform (DCT), encryption/decryption, image copyright protection, fingerprinting, Digital Intellectual Property.

Received: 9 March 2010, Revised 5 April 2010, Accepted 11 April 2010

©2010 DLINE. All rights reserved

1. Introduction

The technique of digital watermarking is mechanism to embed information (mark) in the digital media products (i.e. image within image) without effecting the media's value. [3] Such that mark (usually called watermark) can be extracted or detected later. By using watermarking the owner of digital media will able to check if a digital media product has been modified without authorization [9].

Some of other definition, watermarking is the process to achieve secretly embedding encoded information into digital data source (image, sound, and video) to achieve the characteristics of: imperceptible watermark, only authorized parties can read watermark easily, and unauthorized parties can not remove watermark without destroying the original data. The watermark is embedded in such way that the quality of the host media is practically maintained and it cannot be captured by a human eye (for images) or ear (for audio content). Only the knowledge of a secret key allows extracting the watermark from the original image [20].

Figure 1, Illustrates the digital watermarking system which consists of a watermark embedder and a watermark detector. In general, the watermark embedder inserts a watermark into the cover signal (original image) and the watermark detector detects the presence of watermark signal (watermark image). To achieve the process of embedding and detecting of watermarks the watermark key is used. This key is private and known to authorized parties only. The digital watermarking techniques should be resistance to both noise and attacks when the digital content is transmitted through the networks [20].

• **Applications of Digital Watermarking**

The main applications of digital watermarking are:

Copyright Protection: The owner of the digital property (image, audio, and video) embeds his/her copyright information into the digital data. This can ensure security for copyright violation, and prove ownership in court [17] when the copyright material redistributed over the Internet.

Copy protection: To prevent the illegally replicated of digital content, the digital content can be watermarked. [20] This feature allows to develop electronic data copying devices so that they recognize watermarked content, and do not allow the user to make unauthorized copies of it [19].

Fingerprinting: This allows the owner of the digital property to know the source of illegal copies of their products. The owner embeds a unique information (mark) for each buyer, and upon finding an illegal copy, the owner can trace the buyer who has leaked the property to a third party. [17].

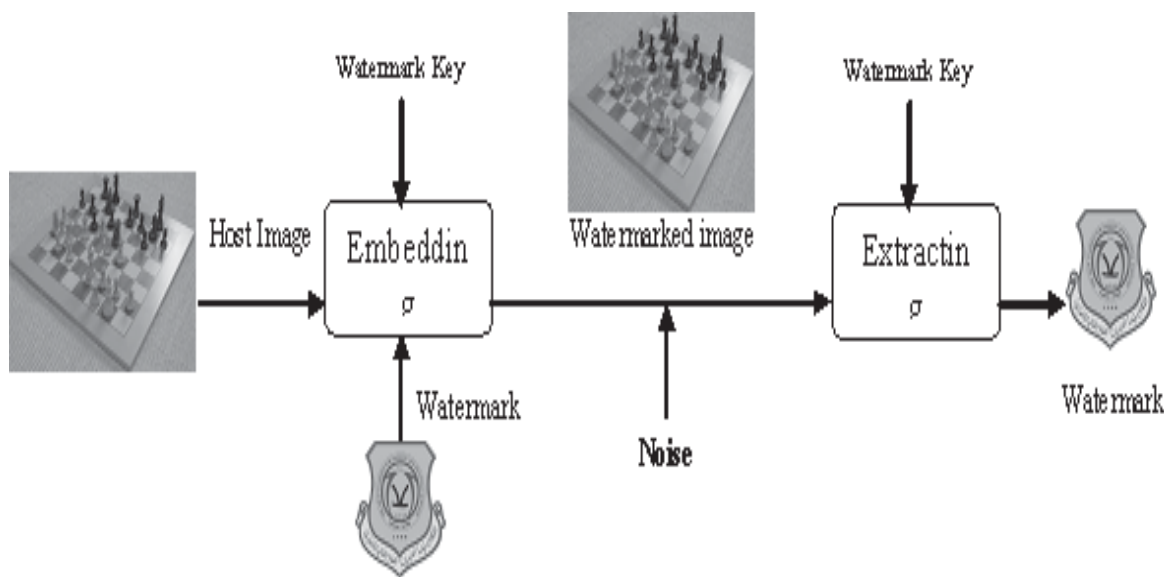


Figure 1. Digital watermarking system

• **Classification of Digital Watermarking Techniques**

The characteristics which are used to classify and measure the Digital watermarks are Depending on the type of application. These characteristics include the difficulties to notice the survival of common distortions and resistance to tampering attacks, the capacity of bit information, and the complexity of the watermarking methods [12]. The main digital watermarking techniques are:

Robust watermarking: The watermark should be resistant to distortion introduced during either normal use, or a deliberate attempt to remove the watermark present. Normal uses involve the Process commonly applied to image during normal use, such as, cropping, resizing, compress ... etc [13].

Fragile watermarking: It is a technique to determine if the watermarked image has been modified or not. [18].

Visible watermarking: It is equivalent to stamping a watermark on formal paper, and for this reason it is usually called digitally stamped, e.g. Logo in the corner of TV picture [4].

Invisible watermarking: It is not visual and it cannot be detected by just viewing the digital content.

Symmetric watermarking: in this mechanism, same keys are used for embedding and extracting watermarks [20].

Blind watermarking: It means that watermark detection without need to original image. The drawback is that when the watermarked image is seriously destroyed, watermark detection will become very difficult [13].

Non-blind watermarking: this technique depends on the host image to extract the watermark by simple comparison and correlation processes [12].

• Features of Digital Watermarking

There are a number of desirable features that a watermark should exhibit. The main features are:

Imperceptibility or Difficulty to Notice: The watermark should not be visual to the viewer nor should the watermark degrade the quality of original image. [11] “The embedded watermarks are imperceptible both perceptually as well as statistically and do not alter the aesthetics of the watermarked image” [20].

Robustness: watermarks should resistant standard data (image) processing, which alters and modifies the watermarked image. [20] Such As standard image processing, resizing, file compression, rotation, [12] digital to analog and analog to digital conversion (such as, printing and scanning), sharpening and blurring, cropping addition of caption [20].

Inseparability: this feature means; it is not possible to retrieve the original image by separating the content from the watermark, after the original digital image is embedded with watermark [20].

Security: By using the watermark secret keys, this will ensure that only authorized users are able to detect/modify the watermark [20].

Data Capacity: it is represented the amount of information that can be stored within the original image [14].

2. Related Works

There are many methods used to protect the digital media rights on Internet. The main methods are cryptographic and digital watermarking methods. The main problem in encryption method is that it cannot help the seller monitor to know how a legitimate customer handles the content after decryption as shown in Fig. 2, while digital watermarking can protect content even after it is decrypted [10].

To generate a powerful protected right in digital image, combination of encryption & digital watermark is made. In this section we discuss the main algorithm which is used in digital watermarking, and compare between them to demonstrate the advantages and disadvantage with the proposed algorithm.

Digital watermarking processing means how to embed the watermark into the original image, and how to extract the watermark from the watermarked image [20]. The image watermarking algorithms can be classified into two categories: Spatial-domain techniques and frequency-domain techniques. The spatial-domain techniques directly modify the color values of selected pixels while the frequency-domain techniques modify the values of some transformed coefficients [5].

- Spatial domain image watermarking using LSB Replacement algorithm [15]

Spatial watermarks are constructed in the image spatial domain, and embedded directly into image's pixel data. This algorithm embeds the Most Significant Bit (MSB) of each pixel of the watermark in the Least Significant Bits (LSB) of the original image. This algorithm extracts the (MSB) of the watermark which is embedded in the original image. If the extracted bits correspond to the inserted bits, then the watermark is detected.

A correlation measure of extracted bit vector and inserted bit vector can be calculated to measure the matching between them.. In general this algorithm saves the watermark from any geometric image processing, such as rotating and cropping. From the above points this algorithm achieves the robustness.

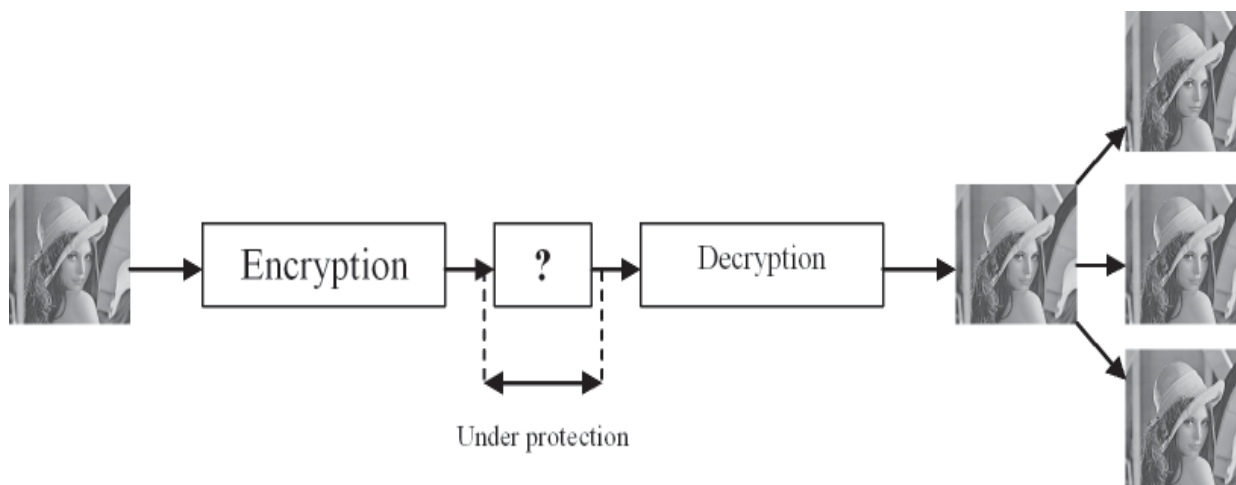


Figure 2. Problem of encryption method in protecting copyrights

- Frequency domain image watermarking using DCT Transform algorithm [15]

To hide a watermark into the transform domain, a mathematical Discrete Cosine Transformation (DCT) is first applied to the original image, and then the transform coefficients are modified by the watermark. The inverse transform is finally applied to obtain watermarked image [6].

DCT splits up the image into frequency bands, so the watermark can be embedded in the most important frequencies [2]. DCT Domain Digital Watermarking is more robust compared to simple Spatial Domain Watermarking; it is robust against simple image processing operations, such as, low pass filtering, brightness and compression ... etc. At the same time it is weak against geometric attacks such as rotation, scaling, cropping ... etc. The common type of DCT Domain Digital watermarking is called DCT and depends on the following equation:

$$y(u, v) = \sqrt{\frac{2}{M}} \sqrt{\frac{2}{N}} \alpha_u \alpha_v \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} x(m, n) \cos\left(\frac{(2m+1)u\pi}{2M}\right) \cos\left(\frac{(2n+1)v\pi}{2N}\right) \quad (1)$$

The equation 1 is resulting three frequency sub-bands as shown in Fig. 3: low frequency sub-band, mid frequency sub-band, and high frequency sub-band. Horizontal frequencies increase from left to right, and vertical frequencies increase from top to bottom. The constant-valued basis function at the upper left is often called the DC basis function, and the corresponding DCT coefficient $y(0,0)$ is often called the DC coefficient [19].

After processing the DCT coefficients, the image is reconstructed by applying inverse DCT operation using equation (2).

$$x(u, v) = \sqrt{\frac{2}{M}} \sqrt{\frac{2}{N}} \alpha_u \alpha_v \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} y(m, n) \cos\left(\frac{(2m+1)u\pi}{2M}\right) \cos\left(\frac{(2n+1)v\pi}{2N}\right) \quad (2)$$

where $\alpha_u, \alpha_v = 1/\sqrt{2}$ for $m, n = 0$, and $\alpha_u, \alpha_v = 1$ otherwise [1].

The watermark bits are embedded in each $n \times n$ DCT block of the image. It is not wise to embed the watermark in the high frequency components of the DCT block, because these coefficients are subjected to heavy quantization during JPEG compression.

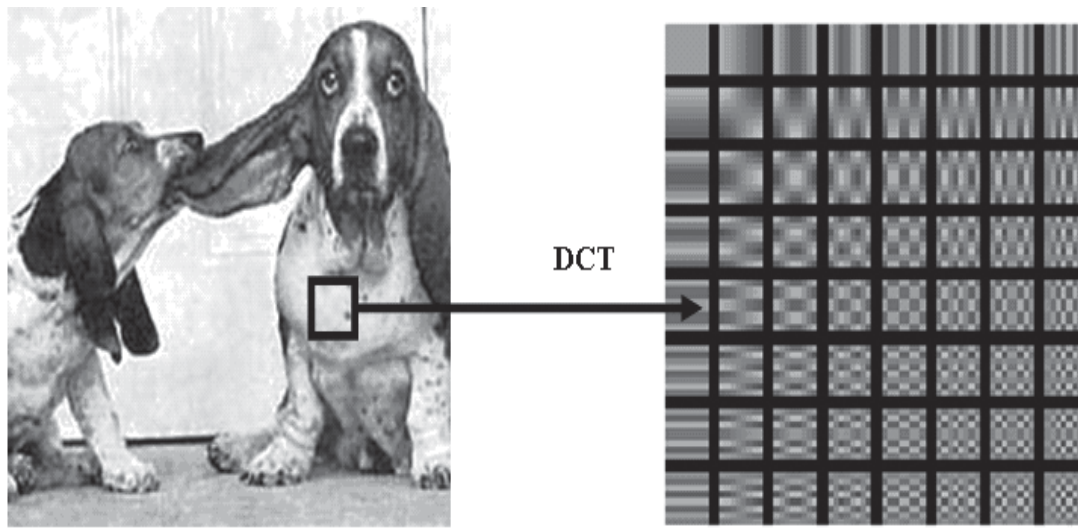


Figure 3. The 64 DCT coefficients of an 8×8 block

The watermark bits are embedded in each $n \times n$ DCT block of the image. It is not wise to embed the watermark in the high frequency components of the DCT block, because these coefficients are subjected to heavy quantization during JPEG compression.

In this proposed method, the embedded binary watermark image must be invisible to human eyes and robust to most image processing operations. To meet these requirements, each binary watermark pixel value (0 or 1) is embedded in one block (exactly in DC coefficients) of the host image. To obtain the extracted watermark from watermarked image, it will call extraction function which extracts the watermark information from the DC coefficients of watermarked image.

This proposed digital watermark scheme save the watermark from the affects of common image processing processes.

DCT will be used in the proposed method, and the two important facts in DCT transform which we need in the proposed method are [2]:

1. Much of the signal energy lies at low frequencies sub-band which contains the most important visual parts of the image.
2. The high frequency components of the image are usually removed through compression and noise attack.

3. Problem Statement

From the two previous methods, we sees, that the LSB Replacement method is inefficient to protect the digital image because the attacker can replace all LSB bits in each pixel of watermarked image with 0 value, with no large effect on the human eye view, that means the loss of watermark is possible, which weakness to this copyright system. On the other hand the previous DCT algorithm is better than LSB method, brings about more robustness and is difficult to drop the watermark by it, but it needs a larger number of locations in the original image to embed each bit of the watermark. The other problem is the large number of blocks which take a long time to process the entire image. In other words, it is a slow method as compared to the new proposed algorithm which we will propose in next section. It will be a strong digital watermarking scheme trying to solve the previous mentioned problems.

The proposed algorithm will answer the following questions

- 1) How to insert invisible digital watermark in an original image (cover image) with acceptance robust degree;
- 2) How to protect the digital watermark against an extract with illegal methods to reuse it in counterfeiting another digital media, which means how to develop high secure watermarking scheme;

- 3) How to extract the high quality digital watermark from the marked image depending on the original image;
- 4) How to prove the buyer's rights for the image that he/she has bought and how to identify the users who replicated the content illegally; and
- 5) How to save the watermark from the effects which are generated by processing the watermarked image.

4. Proposed Algorithm

The proposed algorithm consists of two sides, the first one is the encrypting and embedding the watermark, the second one is the extracting the watermark and the information of the image's buyer from the modified image, as shown in Fig.4.

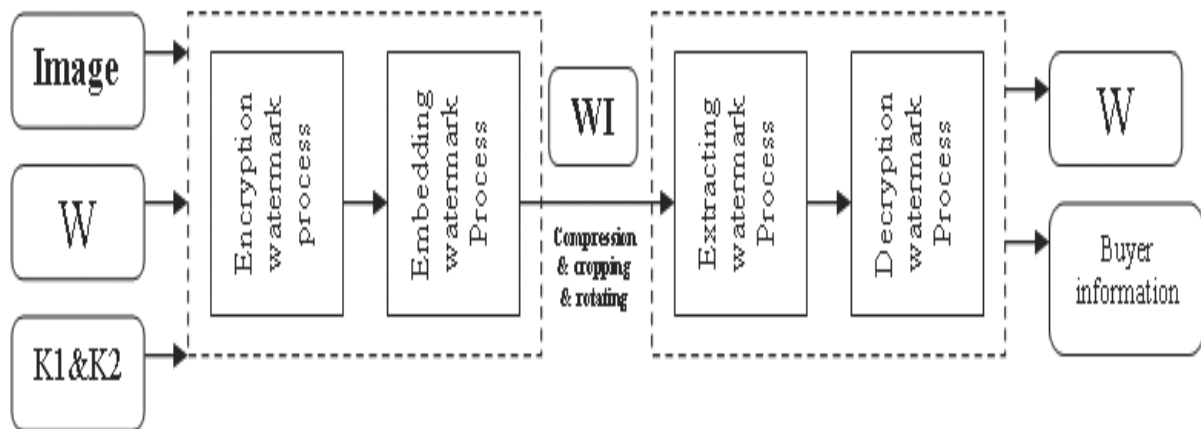


Figure 4. Processes of proposed scheme

Functionality of proposed algorithm

This proposed copyright protection and fingerprinting scheme operates to encrypt the watermark by the Merchant depending on Buyer information such as Buyer_ID, bill_ID, and image_ID ... etc, that is to confirm each image ownership, then the encrypted watermark will be re-encrypted by the third party using the CPU_ID of the encrypted device. After that the encrypted watermark will be embedded using DCT domain in the original image, DCT domain is used to increase the robustness, which is through resisting the distortion which occurs when the watermarked image is compressed by using the JPEG form. The general scheme of protecting copyrights is illustrated in Fig. 5.

At merchant side the watermark bits will be collected with fixed size units (Bytes) and then each unit is converted into decimal number, then each decimal number will be embedded into fixed size $n \times n$ DCT blocks from the original image. The proposed algorithm depends on the values of two secret keys to strong watermark encrypt scheme, one is generated by the buyer information, and the other is generated by the third party device; such key will be the CPU_ID of that device. Using two keys is necessary to provide more secure watermarking scheme. The main objectives of this proposed algorithm is to:

- Minimize the number of the original image blocks when we use the DCT transform in order to increase the speed of embedding process. (treatment of the capacity issue),
- Raise the level of security by using unique Key to encrypt the watermark,
- Increase the robustness to compression by JPEG and cropping, and
- Identify each image through buyer information (fingerprinting).

Watermark Encrypting and Embedding Method

In this proposed method, as shown in Fig. 5, the watermark must be more secure and impede the trials of the attacker to decrypt it. The embedded watermark must be invisible to human eyes and robust to most image processing operations. Moreover to that each watermarked image must carry the consumer (buyer) information to distinguish who has recopied and distributed the illegal image copies. The proposed method as shown in Fig. 6 consists of the following main steps:

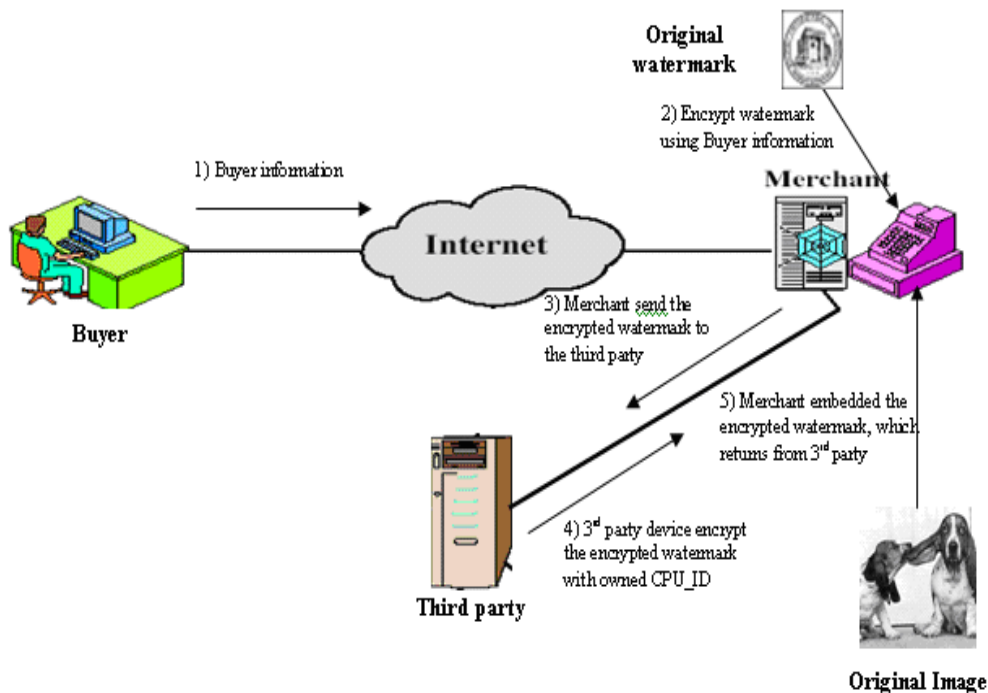


Figure 5. The proposed copyrights protection and fingerprinting scheme

- Step1.** At merchant side convert the watermark image to the binary watermark image; vector of 0's and 1's.
- Step2.** Use the buyer graphical information as a secret key (k_1) to encrypt the watermark, XORed (k_1) and watermark (W). The result is encrypted watermark (W'). This step represents the fingerprinting process,
- Step3.** Merchant send the encrypted watermark (W') to the 3rd party to re-encrypt it using its own CPU_ID as a secret key (k_2) with different block sizes, and 3rd party returns the encrypted watermark (W'') which have the highest entropy to the merchant. **Entropy value** is the degree of randomness in variable. If (x) is a random variable which takes value according to a probability distribution $p(x)$ then the entropy value $H(x)$ can be computed by using the following equation 3:

$$H(x) = - \sum p_i \log_2 p_i \quad (3)$$

Where p_i is the i^{th} plaintext block

Depending on entropy, when it is increasing, the break of a cryptosystem will be hard [8].

- Step4.** At merchant, group each n -bits of encrypted watermark (W'') which is encrypted in 3rd party in fixed length units,
- Step5.** The original image will be divided into a number of non-overlapping fixed size blocks; number of blocks equal to the number of watermark's units, the size of each block is 16×16 pixels or large,
- Step6.** Convert each unit in step4 into a decimal number (X_i),
- Step7.** For each original image block compute the DCT Transform coefficients,
- Step9.** Each decimal number (X_i) results in step6 will be dividing on embedding factor to reduce its intensity value. The result will be ($X'i$),
- Step10.** ($X'i$) will be embedding in the i th original image block, exactly in DC coefficient I_{dc} , in order as follow:

$$I'_{dc} = I_{dc} + X'i$$

Where $i = 1, 2, 3, \dots, s$, where $s = \text{number blocks}$.

- Step11.** After embedding the watermark, apply the IDCT for each block, then the result is the watermarked image.

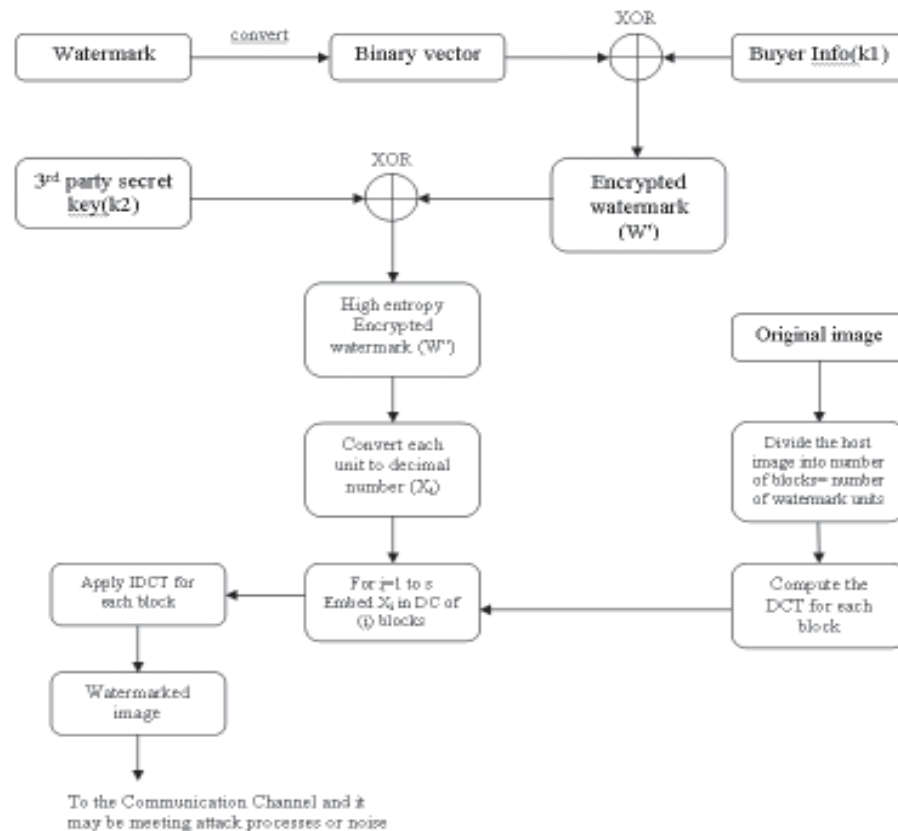


Figure 6. Watermark encryption and embedding scheme

Watermark Extracting Method

Fig. 7 demonstrates how the merchant verifies whether the copies of images are legal or illegal copies, and the following steps will be played:

- Step1.** At merchant side convert the watermark image to the binary watermark image; vector of 0's and 1's,
- Step2.** At merchant, group each n-bits of watermark (W) into fixed length units,
- Step3.** The watermarked image and the original image will be divided into a number of non-overlapping fixed size blocks; number of blocks is equal to the number of watermark's units, the size of each block is 16×16 pixels or large,
- Step4.** For each original and watermarked image block compute the DCT Transform coefficients,
- Step5.** Subtract the DC coefficients values of original image from the DC coefficients values of the watermarked image,
- Step6.** The differences which are generated in step5 will be multiplied by 10, the results will be (X'i),
- Step7.** All X'i values will be converted to the binary digits units. The concatenation between their digits units in one vector will represent the encrypted watermark (W''),
- Step8.** The merchant sends the encrypted watermark vector (W'') which is generated in Step7 to the 3rd party to decrypt it with 3rd party CPU_ID (secret key), and then, the 3rd party sends the decrypted watermark (W') to the merchant,
- Step9.** The merchant uses the buyer information as a secret key (k1) to decrypt the watermark by XORing the (k1) with (W'). The result is original watermark (W),
- Step10.** If the merchant wants to know who is the owner of the image, merchant will XORed original watermark (W) and encrypt watermark (W'). The result is buyer information,

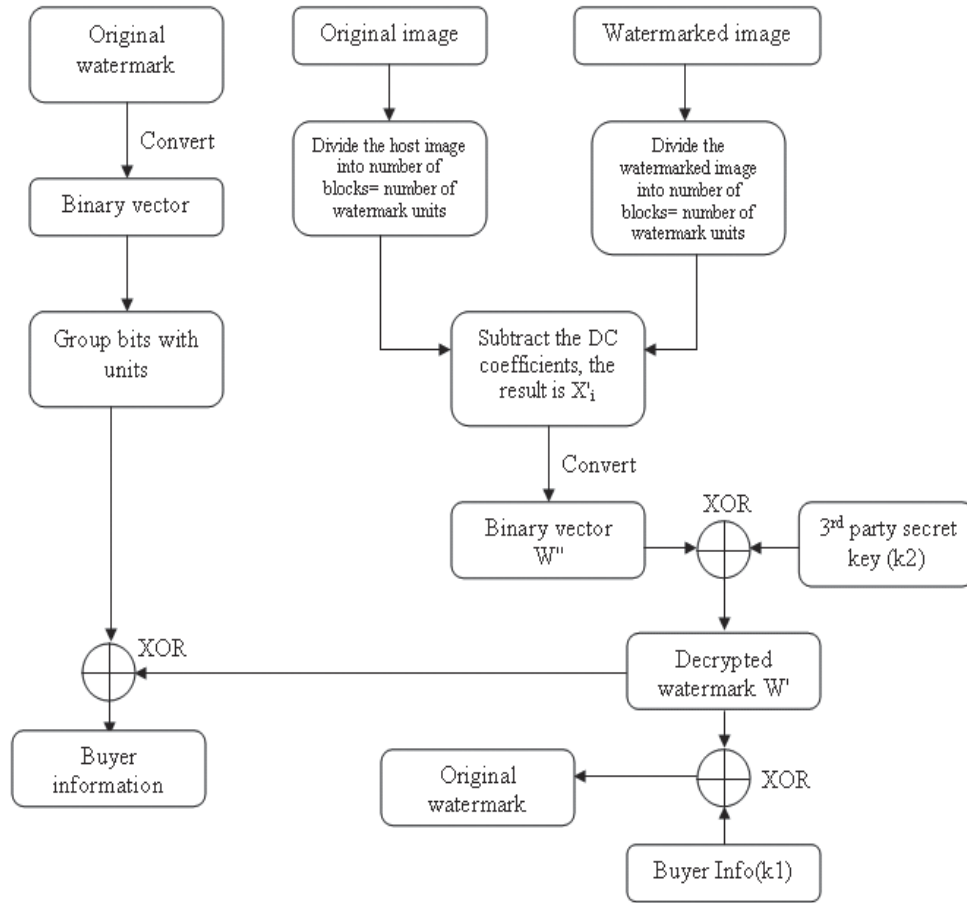


Figure 7. Watermark and buyer information extraction scheme

5. Simulation Results

Watermarking algorithms are usually evaluated with respect to two metrics: imperceptibility and robustness.

1. Imperceptibility: it means that the perceived quality of the original image should not be distorted by the presence of the watermark. To measure the quality of a watermarked image, the Peak Signal to Noise Ratio (PSNR) is used. PSNR in decibels (dB) is given below. [2]

$$PSNR_{dB} = 10 \log_{10} \left(\frac{255^2}{\sum_m \sum_n (I(i, j) - D(i, j))^2} \right) \quad (3)$$

Where:

I is the original image, and **D** is the watermarked image [13].

Generally, when PSNR is 40 dB or greater, the original and the watermarked images are virtually indistinguishable by the human observers [16].

2. Robustness: is a measure of the immunity of the watermark against attempts to remove or degrade it, intentionally or unintentionally, by different types of digital signal processing attacks. [2] The similarity of extracted watermark (W') and original watermark (W) is computed by the following equation.

$$NCC = \frac{\sum_{i=1}^M \sum_{j=1}^N [W(i, j) \cdot W'(i, j)]}{\sum_{i=1}^M \sum_{j=1}^N [W(i, j)]^2} \quad (4)$$

As NCC can take values from 0 to 1, and as long as NCC more closed to 1, this means that the extracted watermark is more similar to the original watermark[16].

Simulation results without attack

The PSNR is calculated to find the similarity between the original image and the watermarked image. When no attack was made on the watermarked image, we found, that the PSNR at EF=1 is 49.6 dB. This value means that the original image is similar to the watermarked image, but when we increase the EF to 3000 we improve the similarity between the original image and the watermarked image so that they become identical, with PSNR = 99.01 dB, as shown in Fig. 8. The human eye does not distinguish any differences between the original image and the watermarked image.

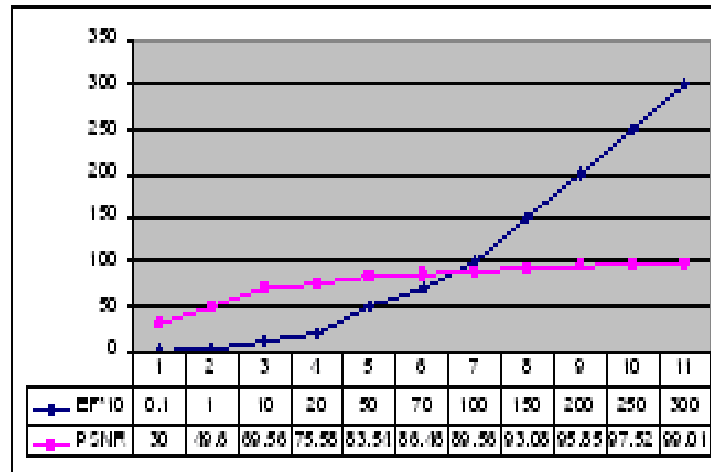


Figure 8. The relationship between embedding factor (EF) and PSNR

In the other hand, this proposed algorithm reduces the number of blocks which we need to embed the bits of the watermark. When the number of the host image blocks is reduced, the time which we need to embed the bits in these blocks is reduced also. To reduce the number of blocks in the original image, as shown in Fig. 9, we must expand the units of the watermark; in other words, when we chop-in the bits of the watermark in fixed length units, we will expand the number of bits in each unit, for example with the 32×64 bits binary watermark image, chopping-in the bits in units with 4 bits, 8bits, 10 bits, 12 bits, 14, bits, and 16 bits, as shown in Fig.9.

Simulation results with attack

-JPEG compression

On the other hand, the watermarked image is distorted by raising the ratio of JPEG compression as shown in Appendix, table 1. We noticed that the PSNR decreases when JPEG compression ratio is increased and the human eye can distinguish the differences between the original watermarked image and the compressed watermarked image. Also we found out that when the watermarked image is attacked with JPEG compression by using multi levels of image compression, the watermark and buyer information are not affected. That is obvious from the NCC results which are illustrated in table 1. The NCC results are still (1) at any compression level, that is, the embedding watermark is exactly similar to the extracted watermark. And the human eye does not distinguish any differences between the original watermark and the extracted watermark; also it does not distinguish any differences between the original graphical buyer information and the extracted graphical buyer information.

From the previous results, this proposed algorithm is robust to JPEG image compression. Fig. 10 illustrates the relationships between the JPEG compression ratio, PSNR, and NCC.

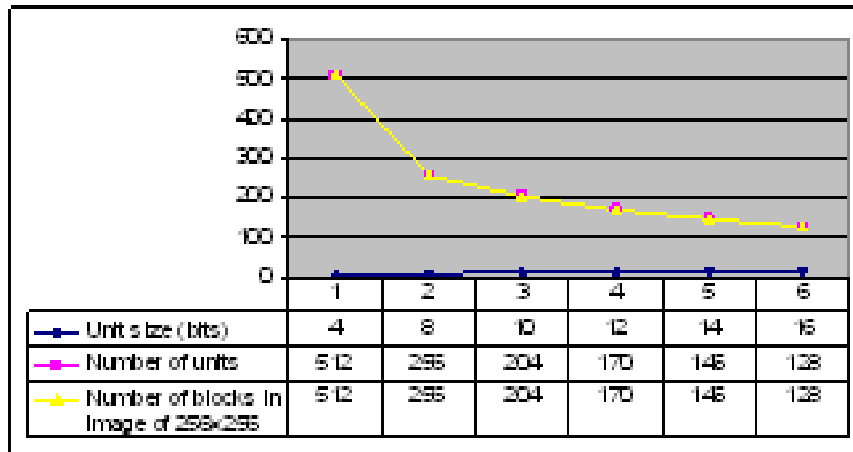


Figure 9. Relationship between the number of units in watermark and host image blocks

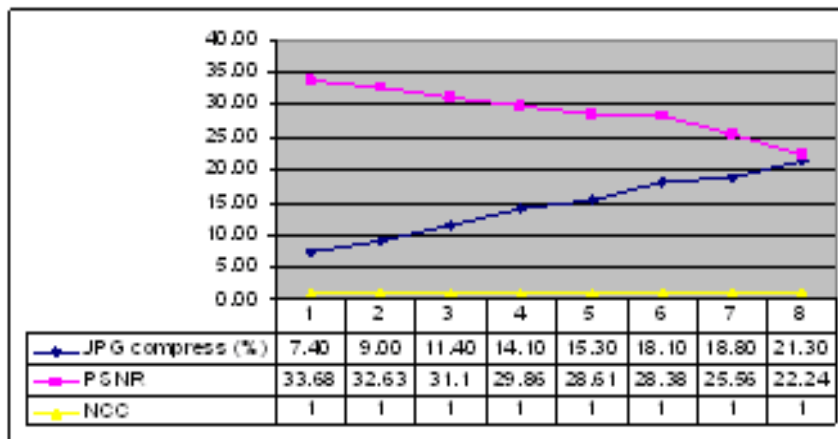


Figure 10. Relationship between compression ratio and its effect on the watermark

-Cropping

In another way, we use the cropping as a distorting process to examine the robustness of the proposed algorithm to other image operations. We applied the cropping operation on the watermarked image with different ratios and in variant areas of the image. The human eye can distinguish the effect of cropping on the watermarked image as in the form of a shaded area (black area) as shown in Appendix, table 2. This process will decrease the PSNR on increasing the ratio of cropping as shown in Fig. 11. On the other hand, the distortion of the watermark and the graphical buyer information will be increased with the increase of the ratio of cropping.

But the location of cropping will play a role in clearness of the extracted watermark and the buyer information. We see in table 2 when the cropping ratio is 25% and the location of cropping is at the center of the watermarked image, the distortion of the watermark and graphical buyer information will be more obvious than when the cropping location is on the bottom-right or top-left of the watermarked image.













JPEG Compression ratio	Mask	Compressed Watermarked image (256×256)	Extracted buyer information	Extracted watermark	NCC	PSNR Between Compressed watermarked image and original image
7.4%	36 (1's) 220(0's)		ID: 1121511 DATE: 2/2/2001		1	33.68dB
9.0%	28 (1's) 228(0's)		ID: 1121511 DATE: 2/2/2001		1	32.63dB
11.4%	21 (1's) 235(0's)		ID: 1121511 DATE: 2/2/2001		1	31.10dB
14.1%	15 (1's) 241(0's)		ID: 1121511 DATE: 2/2/2001		1	29.86dB
15.3%	10 (1's) 246(0's)		ID: 1121511 DATE: 2/2/2001		1	28.61dB
18.1%	6 (1's) 250(0's)		ID: 1121511 DATE: 2/2/2001		1	28.38dB

Table 1. Watermarked image compression levels and effects on watermark & buyer information

As a result to the cropping process, the NCC values will decrease when the cropping ratio increases; that means the differences between the original watermark and the extracted watermark are viewed.

The big difference will be viewed when the cropping location is at the center of watermarked image, at any cropping ratio, as shown in Fig. 11.

Also we found from Fig. 11 the relationship between the NCC and the PSNR: when the PSNR increases, the NCC increases, and when the PSNR decreases the NCC decreases, too.

-Rotation

Finally, from the results which are demonstrates in Appendix, table 3, we see the watermark does not robust to the rotate process, and both NCC and PSNR are decreases when the degree of rotating is increasing, so this proposed method is not robustness to geometric image processing.

6. Conclusion

The proposed image watermarking scheme has met all the objectives which we set in the proposed algorithm section. This













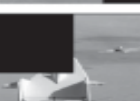

cropping ratio	Compressed Watermarked image (256×256)	Extracted buyer information	Extracted watermark	NCC	PSNR Between cropped watermarked image and original image
10%		ID: 1121511 DATE: 2/2/2001		1	26.63dB
		ID: 1121511 DATE: 2/2/2001		0.9889	21.96dB
		ID: 1121511 DATE: 2/2/2001		1	24.59dB
30%		ID: 1121511 DATE: 2/2/2001		0.9602	15.03dB
		ID: 1121511 DATE: 2/2/2001		0.8982	13.97dB
		ID: 1121511 DATE: 2/2/2001		0.9602	16.15dB
50%		ID: 1121511 DATE: 2/2/2001		0.885	10.83dB

Table 2. Watermarked image compression levels and effects on watermark & buyer information







Rotate angle	rotated Watermarked image (256×256)	Extracted buyer information	Extracted watermark	NCC	PSNR Between rotated watermarked image and original image
1 degree				0.50	18.59dB
2 degree				0.46	16.29dB

Table 3. Watermarked image rotation and effects on watermark & buyer information

scheme provides a good security system to secure the watermark, where the 3rd party is responsible for protecting the watermark of merchant by using its own CPU_ID as a secret key to protect the watermark, and then select the best encrypted watermark to embed it in host image.

Also the scheme executes the fingerprinting process with high performance, when the buyer information is embedded into the watermark. The proposed watermark embedding algorithm reduces the spaces in the host image in which we need to embed the watermark, which is performed to decrease the time which we need for the embedding process.

Experimental results show that the proposed embedding algorithm saves the host image highly intact after embedding the watermark. In other words, the human eye cannot distinguish any differences between the original image and the watermarked image. Also, the experimental results show that the proposed algorithm is robust to common image operations such as JPEG image compression and cropping operations. But the proposed algorithm is not robust to rotating operation.

References

- [1] Alhaj, "Combined DWT-DCT Digital Image Watermarking, *Journal of Computer Science* 3(9): 740-746, 2007
- [2] Hassanien, E ("A Copyright Protection Using Watermarking Algorithm", *INFORMATICA*, Vol. 17, No.2, 2006
- [3] Nguimjeu, A.S."Digital Watermarking", Seminar Series Selected Topics of IT Security, summer term 2007, Faculty of Security in Information Technology, Technical University of Darmstadt
- [4] CHAN, CCHANG, C."A Survey of Information Hiding Schemes for Digital", *IJCSES*, 2007
- [5] Lee, C-H..Lee, Y-K"An Adaptive Digital Image Watermarking Technique for Copyright Protection", 1998
- [6] Taskovski, D., Bogdanova, S., Bogdanov, M. (2004). Digital Watermarking in Wavelet Domain", *Digital right management and the crumbling norms of copyright*.
- [7]F.Y. Duan, I.King, "A Short Summary of Digital Watermarking Techniques for Multimedia Data",RGC Earmark Grant, 1997
- [8]H. J. Jarrar, "Image Encryption and Decryption with Residual Intelligibility Measurements", Ph.D thesis, 2004
- [9]H. Wollan, "Digital Watermarking in Still Images", 1999
- [10] Cox, J. Bloom, *Digital Watermarking*, Morgan Kuffman Publisher, 2002
- [11] J. Cox, M. L. Miller, "A Review of Watermarking and the Important of Perceptual Modeling", *Proc. of Electronic Imaging*, 1997
- [12] Seitz, J (2005). Digital Watermarking for Digital Media, *INFOSCI*.
- [13] Liu, L. (2002). A Survey of Digital Watermarking Technologies.
- [14] Qureshi, M. A. Tao, R.(2006).A Comprehensive Analysis of Digital Watermarking, *Information Technology Journal*, 5(3).
- [15] El-Goneimy, M. M (2008).Comparison Between two Watermarking Algorithms Using DCT Coefficient, And LSB Replacement, *JATIT*.
- [16] Maheshwari, M.,Arora, R., Signal, G. (2004). Invisible Image Watermarking Using a Public Key Algorithm.
- [17] Lam, P., Winkelmeyer, O., Abbas, S.,Kamoosi, N (2005). Watermarking Technologies-Analysis and Design Report, Dec.
- [18] Chandramouli, R., Memon, N Rabbani, M. (2001). Digital Watermarking.
- [19] Potdar, V. M., Han, S., Chang, E. (2005). A Survey of Image Watermarking Techniques, *In: 3rd IEEE International Conference on INDIN*, 2005
- [20] Wipro (2004). Digital Watermarking: A Technology Overview, white paper.

Author Biographies



Muath Shakir Al-Ubaidy received his B.Sc degree in Electrical Engineering with a specialization of Computers and Control from Sana'a University, Yemen. Master of Computer Information Systems (CIS) from Arab Academy, Yemen. He is Instructor at the Department of Information Systems, Faculty of Humanities and Administrative, University of Science and Technology, Yemen.



Ahmed Sultan Al-Hegami received his B.Sc degree in Computer Science from King Abdul Aziz University, Saudi Arabia, MCA (Master of Computer Application) from Jawaharlal Nehru University, New Delhi, India; and Ph.D. degree from University of Delhi, Delhi, India. He is Assistant professor at the Faculty of Computers and Information Technology, Sana'a University, Yemen. His research interest includes artificial intelligence, machine learning, temporal databases, real time systems, data mining, and knowledge discovery in databases.



Taha Hussian Al-Rawhani received his B.Sc degree in Computer Science from Al-Yarmok University, Jordan, Master of Computer Information Systems from Arab Academy, Jordan, and Ph.D. degree from Arab Academy, Jordan, He is Assistant professor at the Faculty of Computers and Information Technology, Thamar University, Yemen. His research interest includes System analysis and Design, Quality Assurance, Real Time Systems and software engineering.