Robust Self Embedding Watermarking Technique in the DWT Domain for Digital Colored Images

Abdallah Al-Tahan Al-Nu'aimi[1], Rami Qahwaji[2]
School of Informatics, Bradford University
UK
[1]abdstn@yahoo.com
[2]r.s.r.qahwaji@bradford.ac.uk

Uncorrected Proof

Journal of Digital Information Management

ABSTRACT: *In this work, a robust watermarking algorithm is proposed for colored digital images. The 24 bits/pixel RGB images are converted to YCbCr color format, and the Y part is converted to Discrete Wavelet Transform (DWT). The resulted LL part is resized to the original size of the host image and its blocks are scrambled using certain key. The watermark is another copy of the LL part and its pixels are, also, scrambled and each pixel is embedded in one of the scrambled blocks of the LL part. The algorithm takes into account the Human Visual System via relating the embedding process to the intensity of each block of the host image. We have used the average PSNR as a quality measure for the embedding stage. In all our experiments we got more than 68 dB which satisfies the PSNR bench mark. Also we got an average value of 0.15 for MAE, which is the robustness measure. This means that our algorithm is very robust and the watermark is still recognizable.*

Categories and Subject Descriptors
I.4 [Image processing and computer vision]; I.3.3[Image and Picture generation];

General Terms
Watermarking algorihm, Discrete Wavelet Transform

Keywords: Digital Images, Embedding, Watermarking, Robustness, Scrambling, Copyright

Received 17 December 2006; Revised and Accepted 12 February 2007

1. Introduction

In previous times of history, every designer/creator was sure of his/her rightful ownership because of uniqueness of, almost, every work. But, in our days, its becoming very easy to copy the original works of others, which creases all kind of copy right problems.

One image can provide better description than thousands of words. So, the protection of images from illegal copying, manipulation and distribution is a very important issue. The protection process for analog images is not of serious concern compared to digital images, since the original copies of analog images are stored in their original negatives, recording tapes, films, ….etc, and there are ways to distinguish an original image from a tampered one. Also, copying analog images is not easy nor fast compared to the copying of digital images. In contrast, digital images can be easily copied, stored, manipulated, retransmitted and distributed, which creates a huge copyright problem [1].

Furthermore, electronic commerce and electronic publishing are discouraged because there is no agreed upon mechanism for tracing any possible illegal copying or modifications of the content. Thus, the watermarking technology seems to be the answer to the problems of ownership and authenticity. Watermarking is a new digital technology for embedding certain information in multimedia products to preserve the copyright and authentication, and to overcome the problem of theft and tampering. For images, watermarking depends on embedding certain stream of bits or small images within the pixels of the original image.

Although watermarking and cryptography both need secret keys to hide some information from human senses, watermarking is different from cryptography, since cryptography needs to protect the information via the transmitting channel, while watermarking embed certain watermarks within the original content. It can also embed some information about the owner, recipient, distributor, transaction dates, serial numbers,…etc.

The presence of an established key management system is assumed, which assigns required codes to the rightful watermark embedding and extraction parties. Cryptography systems restrict access to the information to prevent illegal acts. But watermarking gives evidence of attacking after it has taken place. This is similar to the operations of the law enforcement authorities who investigate crimes only after unlawful events occur. The understanding of evented indictment evidence and conviction serves as a deterrent for future crimes. Thus watermarking depends on how copyright infringment cases are prosecuted, besides its dependence on technological factors.

We live in a world that is full of colours. Because of this, we want the images to be colored without any loss of any colour information. However, most of research in visual areas depends on experimental results since the human visual system (HVS) is still under investigation [2].

The digital image watermark may be divided from the human perceptual point of view into: visible and invisible. Visible watermarks has a low number of applications, while invisible watermarks have more applications and represent the desired case. Visible watermark is seen by the human visual system (HVS), and the human eye sees the watermark within the background of the image. This visible watermark can be filtered and removed. Invisible watermark is embedded in the host image and the human eye cannot see it. Thus the existence of it cannot be determined unless some operations are carried out. Many papers dealing with watermarking were presented, some of them are listed in [3]-[13].

Some of the important applications for watermarking technology are [3], [11]:

- Image and video watermarking.
- Audio watermarking.
- Hardware/software watermarking.
- Text watermarking.
- Executable watermarks.

- Labeling.
- Transactional watermark
- Authentication.
- Copy and playback control.
- Signaling.
- Covert communications.
- Proof of ownership.

From the resistance of intentional and unintentional attacks point of view, the digital image watermarks may be divided into: robust, fragile and semi fragile. Robust watermarks resist unintentional attacks (like JPEG compression) as well as intentional attacks (like geometric transformations), and remain unchanged. In contrast, fragile watermark can be detected and extracted using public keys and it is not robust against attacks. While semi fragile represents a case in between.

Watermarks can either be a binary bit stream or a logo image. The binary bit stream may be of random numbers, or it may characterize meaning-ful information like serial number, name, date, ...etc. while the logo characterize a meaningful shape like a legend, seal or any other image.

From the detection point of view, the watermarking system may be divided into: blind and nonblind systems. The blindness means that the host image is not needed in the detection and extraction part, which makes it more popular and practical. But, this blindness affects the robusness issue. Nonblind watermarking system is the opposite of the blind one, with better robustness. One may choose between blindness with less robustness or more robustness with nonblind system.

Depending on the embedding domain, the watermarking system may be divided into: spatial domain or transform (frequency) domain watermarking. In spatial domain watermarking, the values of the watermark pixels are added directly (with scaling factors) to the values of the pixels of the host image. While in the transform domain, the host image is transformed firstly to the required domain (e.g. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), ...etc.) then, the watermark is added to the image coefficients resulting from the transformation operation .

The host images may be of various types, examples of which are: gray images, colored images, halftone images and progressive images. RGB, YIQ and YCbCr are examples of different color formats for colored images. The format of Halftone images is more suitable for newspapers and journals. While, progressive images means images that are downloaded progressively via Internet. The number of color levels on the pixel depends on the bit numbers that characterizes the pixel. For example with 8-bit pixel in gray image, the number of colors (shades of gray) are 2^8=256. While for RGB image the 24-bit pixel gives more than 16 million colors. Any watermmarking algorithm must satisfy the following conditions [5], [14]-[19] :

- it must be invisible.
- it must not affect the quality of the original host image.
- it must be easily extracted in a reliable and convenient way.
- it must be resilient to standard manipulations.
- it must be compatible with the host.

The embedding process makes small changes in the value of the host image pixels, and these changes are imperceptible and determined by the watermark and the key.

The extraction process is the inverse of embedding process and it usually requires a key to detect and extract the watermark.

In this paper, we extend our previous work [17], to provide watermarking scheme that is content dependant, by embedding a reduced version of the host image as a watermark. Our system depends on the discrete wavelet transform domain (DWT) to increase the robustness while maintaining a high quality for the watermarked images after the embedding process.

In Section 2 of this work, the proposed DWT algorithm of watermarking is explained. The Scrambling and embedding processes is introduced in Section 3 and the extraction process is explained in Section 4. Implementation and results are in Section 5 and conclusions in Section 6.

2. Discrete Wavelet Transform Embedding

This method depends on transforming the host image into discrete wavelet transform (DWT), and embedding the watermark within the coefficients resulting from this transform. The inverse discrete wavelet transform (IDWT) is applied later to obtain the watermarked image. We use the discrete wavelet transform because its characteristics are well localized both in spatial and frequency domain [16], [17], [20] and it is a part of recent compression standards. In addition to all that human perception research indicates that the retina of the eye splits an image into several components which circulate from the eye to the cortex in different channels or frequency bands. These channels can only be excited by the component of a signal with similar characteristics. In different channels, the processing of signals is independent. The 2D-DWT divides the information contained in the image into an approximation sub-image and three detail sub-images, each with half the resolution of the original image in each direction [16].

The transform can be iteratively applied to the approximation sub-image obtained in this way. Similarly in discrete wavelet multi-resolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. Thus, independent processing of the resulting components without significant perceptible interaction between them is achieved using discrete wavelet transform.

An algorithm for digital image watermarking that depends on scrambling the bits of the watermark and then embedding them in the scrambled blocks of the host image [18] is used to embed binary images watermarks in gray host images. In this paper, this algorithm is extended; colored images are used instead of gray images and the Discrete Wavelet Transform is the embedding domain instead of the spatial domain. Also, a copy of the original image itself is used as the watermark [15].

In this algorithm, the 24 bits/pixel RGB images are converted to YCbCr [16], which gives one luminance signal Y and two color signals Cb & Cr. The values of Y, Cb and Cr can be calculated from the values of RGB as follows:

$$\begin{aligned} Y &= 0.299\ R + 0.587\ G + 0.114\ B \\ Cb &= 0.596\ R - 0.275\ G - 0.321\ B \\ Cr &= 0.212\ R - 0.528\ G - 0.311\ B \end{aligned} \qquad (1)$$

Such a conversion allows us to use the most useful image data in the Y-layer to embed the watermark within it.

After the RGB colored image is converted to the YCbCr format, the Y part is converted to DWT domain. Imagery results for transforming the test image (Two plains) to DWT is seen in figure 1, and for test image (Petra) is seen in figure 2. The upper left of the resulted image after DWT converting, represents the low frequency part (LL), the upper right (HL) and the lower left (LH) represents the median frequencies and the lower right (HH) represents the high frequency of the image. The watermark is embedded in the upper left part since it contains most of the important visual information of the image for the human visual system (HVS). Also, it is compatible with the important Joint Photo graphics Experts Group (JPEG) standards for image compression, which represents the main unintentional attack facing watermarked images.

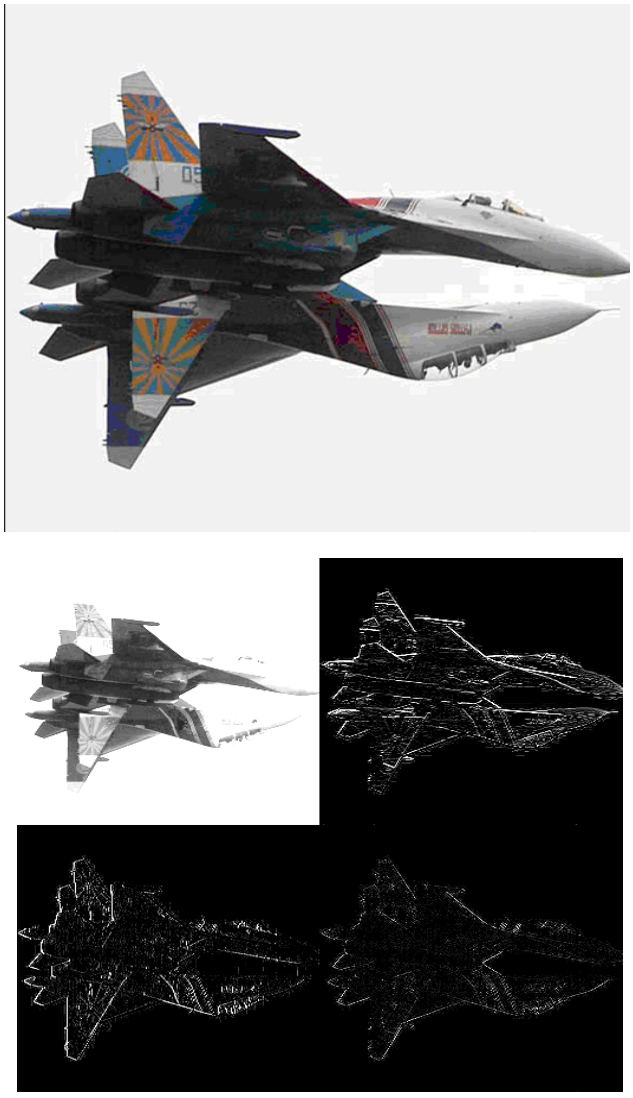

Figure 1. The imagery results for transforming the test image (Two plains) to DWT, (a) represents the original image and (b) represents the four DWT parts of the resulted image.

The lowest frequency part (LL) is scrambled in a block level. Then, another copy of the (LL) part is used as a watermark and scrambled in a pixel level. Each pixel of the scrambled watermark is embedded in one of the scrambled blocks of the (LL) part. The two scrambling processes give double uncertainity which make the system very secure. The size of each block is 4×4 pixels. The embedding process is dependant on the intensity values of each scrambled block. The following block diagram, Figure 3, explains this process.

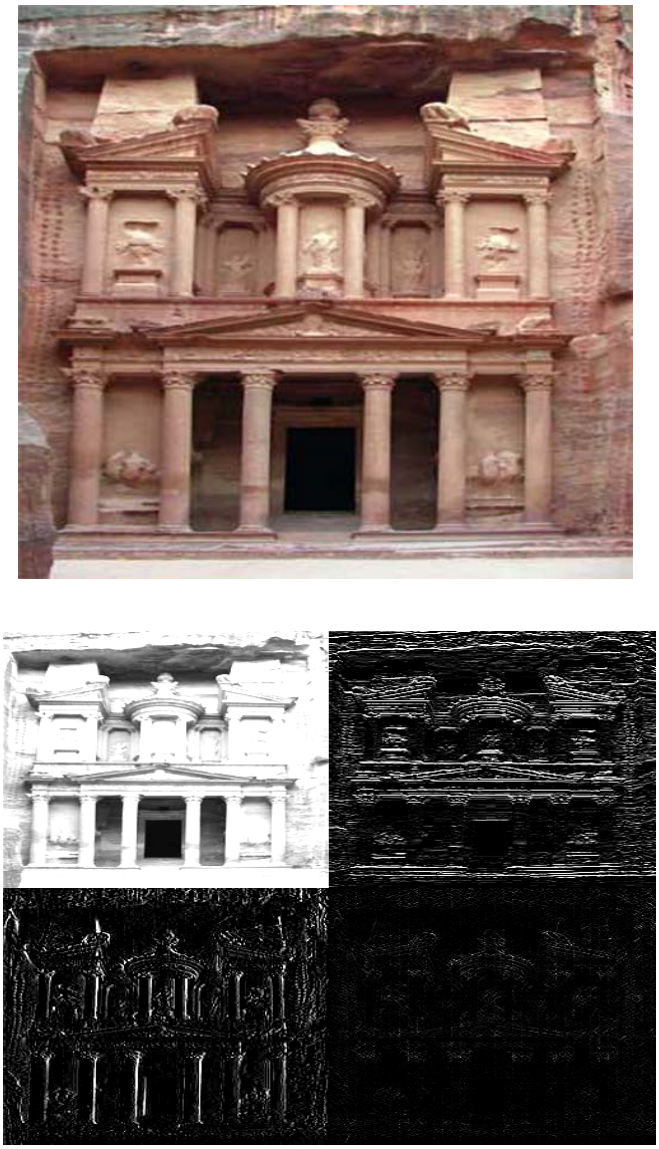

Figure 2. The imagery results for transforming the test image (Petra) to DWT, (a) represents the original image and (b) represents the four DWT parts of the resulted image.

3. Scrambling and Embedding Processes

The watermark pixels which are part of the host image itself, (each one consists of one bit) are pseudo-randomly permuted to a new watermark image. The permutation by pseudo-random can be carried out using shift register with linear feedback. A pseudo-random sequence can be obtained by setting the state of the shift register which can be recovered later by resetting the shift register to its original state [14]. A single row vector is generated from the watermark by performing a raster scan of the watermark.

Pseudo-random permutation is done on the elements of this row vector to get a new row vector via a single execution cycle of the linear shift register. Only one permutation of the indices of the raster scan vector must be performed by the shift register. By assigning the elements from the old raster scan vector to the positions of the new vector, as given by the newly generated indices, a new raster scan vector is generated. Then, the scrambled watermark is constructed by performing the inverse raster scan process on this vector during the extraction process. After the scrambling process, the watermark is inserted into LL part of the transformed host image. Individual insertion of watermark pixels is

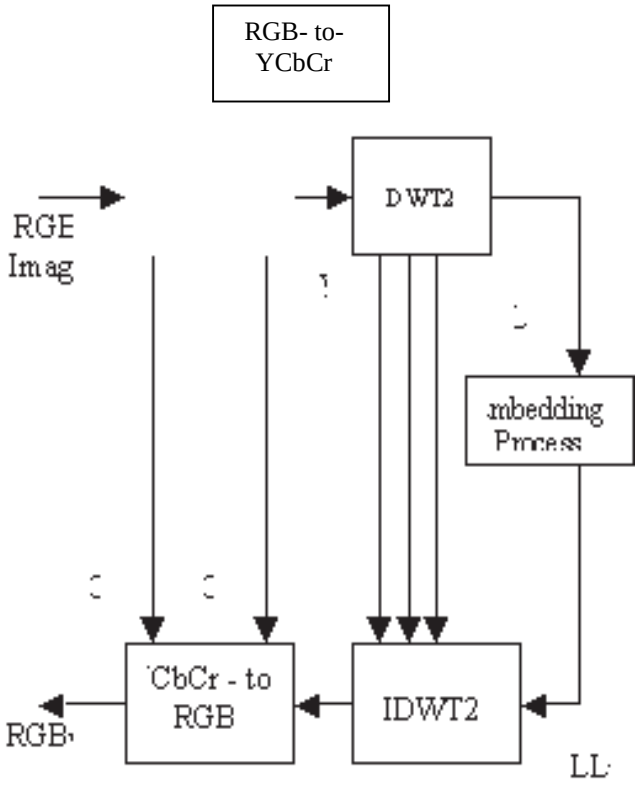

Figure 3. Changing Image to DWT Domain

applied onto blocks of pixels of the host image.

This insertion is done in a pseudo-random fashion. The host image is divided into n×n blocks, and the value of n depends on the size of the host image and the number of watermark pixels. Every watermark bit is embedded in a certain n×n block of the host image. In order to reduce the effects of the modifications taken place on the host image, after embedding the watermark, as seen by the human eye, the algorithm takes into account the contrast of each individual n×n block when embedding each bit. During the embedding process, the bits from the scrambled watermark are selected in a raster scan order from the watermark image. For one n×n block of the host image, a single watermark bit is embedded onto it, and the n×n block itself is selected from a randomly permuted set of indices that index the n×n blocks throughout the host image. The size of these n×n blocks is determined by the sizes of both the host image and the watermark. The host image, in this experiment, is a 512 × 512 RGB colored images with pixel depth of 24 bits (8 bits per pixel for each color channel), and the watermark is a reduced copy of the host image with 128 × 128 pixels. Thus, each bit from the watermark is embedded onto 4×4 block of the host image. Using the same watermark scrambling procedure, the location of every 4×4 embedded block is obtained. Hence, two keys are required to recover the watermark from the watermarked image which represents double uncertainity.

To insert each watermark bit, b_w, within the host block, B, we first sort the pixels in the block in an ascending order based on their intensity values, and the minimum i_{min}, average i_{mean} and maximum i_{max} intensities are computed [18]. Then, each pixel of the block is classified onto one of two classes based on whether its intensity is above or below the mean of the block.

The mean to both the low and high intensity classes is computed to get i_L and i_H. The contrast value of the block, which is defined as the difference between the maximum and minimum intensities of the block scaled by a changeable factor as seen in equation 2, is computed.

$$C_B = \max(C_{\min}, \alpha(i_{\max} - i_{\min})) \quad (2)$$

Where $C_{\min}$ and α are both constants that control the value of the block contrast.

Now, the embedding takes place as follows:

$$\begin{aligned}
&\text{if } b_w = 1,\\
&\quad i_{new} = i_{\max} \quad \text{if } i > i_H\\
&\quad i_{new} = i_{mean} \quad \text{if } i_L \le i < i_{mean}\\
&\quad i_{new} = i + \delta \quad \text{otherwise}\\
&\text{if } b_w = 0,\\
&\quad i_{new} = i_{\min} \quad \text{if } i < i_L\\
&\quad i_{new} = i_{mean} \quad \text{if } i_{mean} \le i < i_H\\
&\quad i_{new} = i - \delta \quad \text{otherwise}
\end{aligned}$$

Where i_{new} is the new intensity value for the pixel with original intensity value i and ä is a random value between 0 and C_B that controls the increase or decrease of the blocks' intensity. Figure 4 explains the scrambling and the embedding processes.

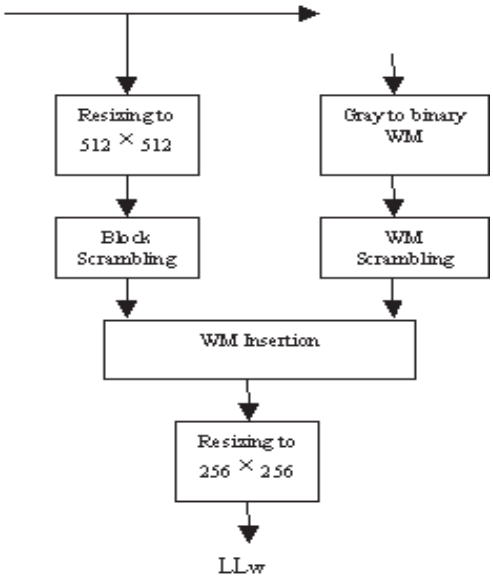

Figure 4. The Scrambling and Insertion Processes

4. The Extraction Process

The extraction process requires the host image only which makes the extraction process simple and straight forward. The sum of the intensity values for the blocks of both the host image and the watermarked image is computed. A bit is decoded as explained in equation 3 below.

$$if\ S_w > S_0 \quad then \quad bw = 1$$

$$if\ S_w \leq S_0 \quad then \quad bw = 0 \qquad (3)$$

Where, S_w is the sum of the pixel values for the block of the watermarked image, while S_0 is the sum of the pixel values for the block of the host image. By using the same key used to select the blocks of the host image, the decoded bits are entered into the inverse permuted order as the n×n blocks were selected. This gives the scrambled watermark that is recovered from the watermarked image. According to the key in the initial scrambling operation, the scrambled watermark is descrambled to obtain the original watermark image.

5. Simulation and Results

This algorithm is examined using 16 different colored test images, (Lena, Mandrill, Barbara, Peppers, Air-plain, Aerial, RGB_ptrn, Cells, Carpet, Petra, Factory, Mountain, Window, Jordan, Texture, and Two plains). Every image is of size 512 × 512 with 24 bits per pixel (three 8-bit color channels). The watermarks are reduced versions of the host images, In our testing process, 9 types of attacks are carried out. These attacks are: low pass filtering, median filtering, scaling, cropping, rotation, JPEG 100 , JPEG 75 , JPEG 50 and JPEG 25. Some of the results are shown in figures 5, 6, 7 and 8 for the famous test images Lena, Mandrill, Barbara and Petra, respectively. In all these figures, the original host images is shown in part (a), the watermarked images in part (b) and the error images, that represent the difference between the original host images and the watermarked images, are seen in part (c).

The high similarity between the original host image and the watermarked image is obviously seen for all the test images used. This means that the quality of the original host image is not affected by the embedding of the watermark. Also, it means that the watermark is invisible to the human visual system.

Figure 5. The imagery results for image Lena after embedding the watermark, (a) the host image, (b) the watermarked image and (c) the error image.

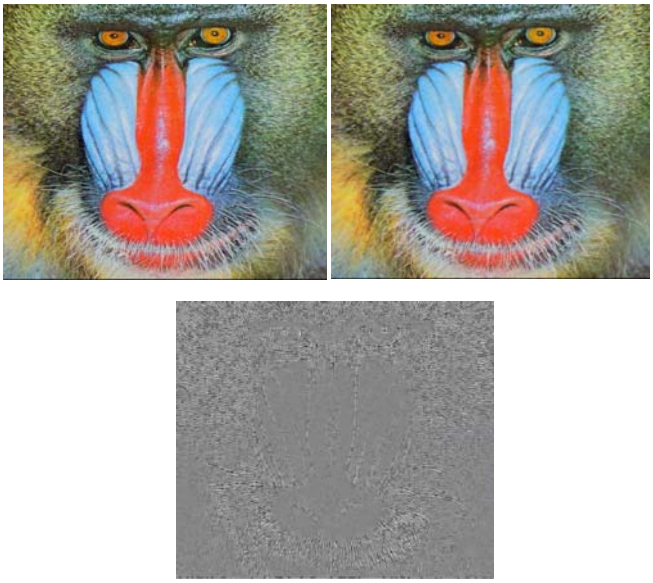

Figure 6. The imagery results for image Mandrill after embedding the watermark, (a) the host image, (b) the watermarked image and (c) the error image.

Figure 7. The imagery results for image Barbara after embedding the watermark, (a) the host image, (b) the watermarked image and (c) the error image.

5.1 Subjective Evaluation

Subjective and objective tests are used to test the algorithm. Subjective testing depends on the visual evaluation of the resultant images after the embedding process has been carried out. Twenty colleagues are chosen and they sit down in front of computer screen individually Three versions of every test image used in the algorithm are displayed in the computer monitor next to each other. The three versions represent two identical copies of the original host image and the watermarked image. The colleagues are asked to determine the image that looks different among the three images. Also, the experiment is repeated several times using different size computer monitors, different resolutions and different distances between the screens and the viewers In addition to this, the three versions of several test images used are printed out using high resolution printer and the

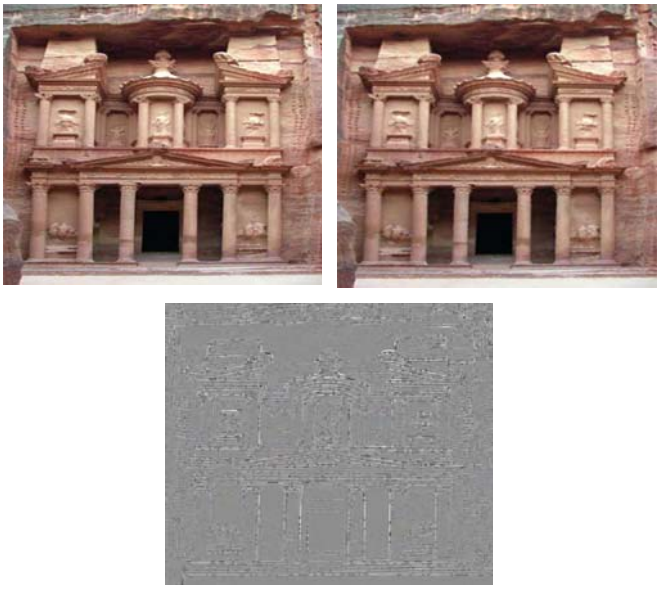

Figure 8. The imagery results for image Petra after embedding the watermark, (a) the host image, (b) the watermarked image and (c) the error image

the viewers are again asked to find the watermarked image. The results for all these experiments are the same; all the viewers can't differentiate between the three versions of the test images, and they cannot decide which version of the three is the watermarked one. This means that our watermarking scheme is compatible with the human visual system (HVS). It also means that the quality of the image is preserved and the watermark is invisible.

5.2 Objective Evaluation

Several objective tools are used to evaluate the algorithm and the quality of the watermarked images. One of the famous tests is to compute the peak signal to noise ratio (PSNR) of the watermarked image. PSNR for the gray images is computed as:

$$PSNR = 20Log_{10}\frac{(255)^2}{MSE} \quad (4)$$

Where, MSE is the mean squared error in the watermarked image. For a colored image, PSNR can be calculated as the mean for all the three RGB layers as seen in equation 5.

$$PSNR_{RGB} = \frac{1}{3}\sum_{i=1}^{3} PSNR(i) \quad (5)$$

Using this powerful tool to evaluate the watermarked image quality, the average resultant PSNR for 16 different colored images, is about 67.7 dB ,which is a very high value indicating a good quality for the watermarked images. The highest PSNR value during our experiments is about 77 dB.

To compute the similarity between the original host images and the watermarked images, the similarity measure (SIM) is computed, as shown below:

$$SIM(X_{org}, X_{wat}) = \frac{X_{org} \cdot X_{wat}}{\sqrt{X_{org} \cdot X_{wat}}} \quad (6)$$

Where, X_{org} and X_{wat} are the original host image and the watermarked image, respectively. A normalized version SIM_{norm} is calculated as follows:

Rgb vy

$$SIM(X_{org}, X_{wat}) = \frac{\frac{X_{org} \cdot X_{wat}}{\sqrt{X_{org} \cdot X_{wat}}}}{\frac{X_{org} \cdot X_{org}}{\sqrt{X_{org} \cdot X_{org}}}} \times 100 \quad (7)$$

The multiplication here is done on a bit level.

A new improved powerful assessment tool to evaluate the similarity between images, is the Structural Similarity (SSIM) method. This tool is more accurate than other traditional tools because it depends on factors related to the Human Visual System (HVS) to determine the similarity between images [21]. Similarity tests based on SSIM is carried out to evaluate the percentage similarity between the original host and the watermarked images. After carrying out all the experiments on all the test images, we find that the percentage similarity ranges between 95% to 98%. This conforms with the results obtained using subjective evaluation. In table 1, the values of PSNR and the values of percentage SSIM for all the 16 test images used are shown.

This algorithm is compared with the DWT watermarking algorithm presented in [3]. The quality of the watermarked images in our algorithm is better compared to [3] because the PSNR values are higher for this work. Table 2 contains the PSNR values for both algorithms for several test images. The test images used in this table are the most famous images in watermarking technology and image processing. The average value of PSNR for our system for these images is 67.7 dB, while it is 42.1 for the other system. The comparison proves that our algorithm gives better watermarking performance. Also, another watermarking system presented in [5], has an average value of 42 dB for the same images, while it is 28.5 for the algorithm of [7].

Image	PSNR	SSIM, %
Lena	67.35	97.60
Mandrill	60.33	95.03
Barbara	62.43	95.64
Peppers	73.86	97.42
Airplane	63.71	95.66
Aerial	64.96	95.65
RGB_ptrn	77.09	97.61
Cells	75.28	97.94
Carpet	65.14	96.82
Petra	72.48	96.56
Factory	62.40	96.78
Mountain	65.06	98.06
Window	65.96	97.66
Jordan	66.61	94.98
Texture	64.90	96.60
Two plains	75.33	97.63

Table 1. The PSNR values and the percentage SSIM of the 16 test images used.

Image	PSNR (dB) This work	PSNR (dB)] System of [3]
Lena	67.35	42.50
Mandrill	60.33	41.90
Barbara	62.43	42.20
Peppers	73.86	41.80

Table 2. The PSNR values for the watermarked images of the 16 test images used

An objective measure of the degradation of the recovered watermark caused by the embedding-extraction procedure is obtained by calculating the mean absolute error (wMAE) of the extracted watermark.

$$wMAE = \sum_{ij \in X} \frac{\left| W_{org} - W_{rec} \right|}{M \times N} \qquad (8)$$

Where W_{org} and W_{rec} are the original and the reconstructed watermarks, respectively, and M×N is the watermark size. In all mentioned experiments M=N=128.

We assumed that the watermarked images are been corrupted by several types of intentional and unintentional attacks. The examined intentional attacks are low pass filtering, median filtering, scaling, cropping and rotation. While, the unintentional attack is the JPEG compression with different quality factors. Table 3. shows the wMAE results for the extraction stage, after attacking the watermarked images by the filtering attacks (low pass and median) for the 16 test images used.

Image	Low Pass	Median
Lena	0.174	0.133
Mandrill	0.208	0.216
Barbara	0.189	0.221
Peppers	0.161	0.137
Airplane	0.179	0.156
Aerial	0.175	0.174
RGB_ptrn	0.138	0.089
Cells	0.158	0.113
Carpet	0.182	0.144
Petra	0.169	0.159
Factory	0.165	0.143
Mountain	0.181	0.171
Window	0.192	0.147
Jordan	0.187	0.170
Texture	0.196	0.199
Two plains	0.160	0.130

Table 3. The wMAE values for the watermark-ed images after being corrupted by low pass and median filtering.

Despite of dangers of the filtering attacks, the watermarks are robust and still recognizable. The wMAE is low for all test images. The average value, using all test images, of wMAE for low pass filtering and median filtering attacks are 0.164 and 0.156, respectively.

The most dangerous intentional attacks are geometrical attacks, (scaling, cropping and rotation). A lot of existing algorithms may not survive these strong attacks. The wMAE results for the extraction stage, is shown in table 4 for the 16 test images. Similar to the filtering attacks, the wMAE values for geometrical attacks are very low which means high robustness is achieved. The average value of wMAE after applying scaling, cropping and rotation for the 16 images are 0.202, 0.156 and 0.128, respectively.

Image	Scaling	Cropping	Rotation
Lena	0.192	0.160	0.128
Mandrill	0.241	0.154	0.145
Barbara	0.216	0.161	0.142
Peppers	0.169	0.150	0.111
Airplane	0.215	0.159	0.132
Aerial	0.221	0.151	0.127
RGB_ptrn	0.157	0.149	0.086
Cells	0.171	0.155	0.108
Carpet	0.229	0.151	0.124
Petra	0.173	0.152	0.119
Factory	0.211	0.150	0.117
Mountain	0.187	0.165	0.139
Window	0.216	0.155	0.141
Jordan	0.205	0.165	0.143
Texture	0.239	0.158	0.154
Two plains	0.183	0.157	0.130

Table 4. The wMAE values for the watermark-ed images after being corrupted by scaling, cropping and rotation attacks

The compression attacks are the most important unintentional attacks facing the watermarked images. The most famous compression technique for images is JPEG compression. The main job for JPEG is to reduce the file size of the images. This process affects partially the image and the embedded watermark. So, the watermarking system must be robust to face the effects of the cmpression. Our system is examined using JPEG compression with different quality factors (100%, 75%, 50% and 25%) as attacks on the different watermarked images. The values of wMAE resulting from applying these unintentional attacks are low enough to indicate that the watermarks are robust and recognizable by legal users or authorities. Detailed results are shown in table 5. The average wMAE value computed for the 16 test images and for the four JPEG tests with quality factors of 100, 75, 50 and 25, are 0.148, 0.137, 0.139 and 0.149, respectively. Figure 7 represents the values of wMAE for the six selected test images that afterf applying the nine stated attacks. This figure gives better visually comparison between different images and attacks.

The amount of hidden data that represent the watermark is 16384 bits which is a large quantity compared to most of the existing watermarking algorithms.

This algorithm gives a watermarked image that is very similar to the host image with a high quality. Besides this, it is robust to several image intentional and unintentional attacks. The existence of double uncertainty in the way of scrambling the watermark and the way of embedding it in the host

Image	J100	J75	J50	J25
Lena	0.164	0.153	0.154	0.164
Mandrill	0.102	0.087	0.090	0.102
Barbara	0.142	0.133	0.139	0.142
Peppers	0.112	0.104	0.107	0.113
Airplane	0.160	0.159	0.144	0.160
Aerial	0.108	0.103	0.103	0.108
RGB_ptrn	0.127	0.114	0.118	0.128
Cells	0.203	0.188	0.190	0.203
Carpet	0.099	0.092	0.094	0.099
Petra	0.137	0.123	0.125	0.139
Factory	0.104	0.093	0.096	0.105
Mountain	0.220	0.201	0.201	0.220
Window	0.157	0.146	0.151	0.157
Jordan	0.191	0.183	0.185	0.192
Texture	0.170	0.154	0.156	0.170
Two plains	0.173	0.162	0.166	0.174

Table 5. The wMAE values for the watermark-ed images after corrupted by JPEG compress-ion attacks

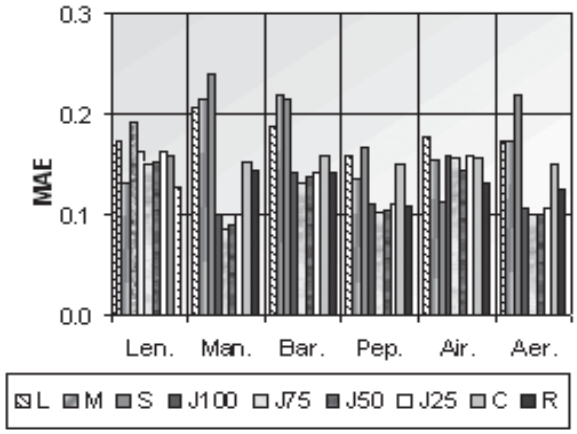

Figure 9. wMAE response resulted using the test images (Lena, Mandrill, Barbara, Peppers, Airplane and Aerial), suffered from low pass and median filtering, JPEG compression of quality factor (100, 75, 50, 25), scaling, cropping and rotation attacks.

image makes the algorithm very secure. The system can be used to prove the ownership and to check the authenticity. But, it uses binary images as watermarks. For our future work, we would like to modify our alorithms to use gray watermark images.

6. Conclusions

In this paper, a DWT-based non blind watermarking algorithm for embedding colored images is proposed. This algorithm is robust and it maintains the quality of the watermarked images. The Human Visual System and its sensitivity are taken into consideration when designing this system. PSNR bench mark (38 dB) [22] is satisfied in all our experiments and the quality of the watermarked images is not spoiled by the embedding process. An average value of 67.7 dB is obtained for PSNR and 0.153 of MAE are obtained after carrying out intensive objective evaluation. Subjective evaluation is carried out as well and excellent results are obtained. The algorithm is very secure since the recovering of the watermark requires two scrambling keys. Comparison with other watermarking schemes is carried out, and our system has shown that it gives better results. For the future, we will extend our technique to embed gray watermark images.

References

[1] Celik, M.U., Sharma,G,. Saber, E., Tekalp, A.M (2002).Hierarchical watermarking for secure image authentication with localization, *IEEE Transactions on Image Processing,* 11 (6) 585-595.

[2] Sharma, G (2003). Digital Color Imaging Handbook, Library of Congress Cataloging-in-Publishing Data, by CRC Press LLC, USA.

[3] Wang, Y., Doherty, J.F., Van Dyck, R.E (2002). A Wavelet-based watermarking algorithm for ownership verification of digital images, *IEEE Transactions on Image Processing,* 11 (2) 77-88.

[4] Tzeng, J., Hwang, W.,Chern, I.L (2002). Enhancing image watermarking methods with/without reference images by optimization on second-order statistics, *IEEE Transactions on Image Processing,* 11 (7) 771-782.

[5] Lu, C.S., Liao, H.M., Kutter, M (2002). Denoising and copy attacks resilient watermarking by exploiting prior knowledge at detector, *IEEE Transactions on Image Processing,* 11(3) 280-292.

[6] Kutter, M., Winkler, S (2002). A Vision-based masking model for spread-spectrum image watermarking, *IEEE Transactions on Image Processing,* 11 (1) 16-25, Jan. 2002.

[7] Fu, M.S., Au, O.C (2002). Data hiding watermarking for halftone images, *IEEE Transactions on Image Processing,* 11 (4) 477-484.

[8] Anderson R.J., Petitcolas, F.A (2001). On the limits of steganography, *IEEE Journal on Selected Area in Communications,*16 (4) 474-481.

[9] I. Cox, I., Kilian, J., Leighton, F., Shamoon, T (1997). Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing,* 6. 1673-1687.

[10] Pitas, I (1998). A Method for watermark casting on digital image, *IEEE Transactions on Circuits System and Video Technology,* 8. 775-780.

[11] J. Hernandez, J., Amado, M., Perez-Gonzalez, F (2000). DCT-domain watermarking techniques for still images, detector performance analysis and a new structure, *IEEE Transactions on Image Processing,* 9, 55-68.

[12] Zeng, W.,Liu, B (1999). A Statistical watermark detection technique without using original images for resolving rightful ownerships of digital images, *IEEE Transactions on Image Processing,* 8. 1534-1548.

[13] Lu, C.S., Liao, H.Y (2001). Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing,* 10. 1579-1592.

[14] Al-nu'aimi, A.,Qahwaji, R (2006). An adaptive watermarking technique for digital colored images, *In*: *Proc. IEEE 2nd International Conference on Information & Communications Technologies: from Theory to Applications,* Syria, Apr. 2006, v. I, p. 729-730.

[15] Al-nu'aimi, A., R. Qahwaji, R (2006). A New digital colored images watermarking technique using self embedding, *In*: *Proc. The Convergence of Telecommunications, Networking & Broadcasting,* UK, Jun. 2006, v. 1, p. 411-414.

[16] Xia, X., Bancelet, C., Arce, G (1997). Multi resolution watermarking based on wavelet transform for digital images,*In*: *Proc. International Conference on Image*

Processing, USA, Feb. 1997, vol. III, pp. 26-29.

[17] Al-nu'aimi, A., Qahwaji, R (2006). Digital colored images watermarking using YIQ color format in discrete wavelet transform domain, *In*: *Proc. The Fourth Saudi Technical Conference and Exhibition,* Saudi Arabia, Dec. 2006, v. II, p. 383-388.

[18] Gulstad, G.S., Bruvold, K (2003). An Adaptive Digital Image Watermarking Technique for Copyright Protection, www.enginerring.ucsb.edu/bruvold,/ec/report/team6report.html.

[19] Das, T S., Maitra, S., Mitra, J (2005). Cryptanalysis of optimal differential energy watermarking (DEW) and a modified robust scheme, *IEEE Transactions on Image Processing,* 53 (2) 768-775.

[20] Al-Tahan Al-Nu'aimi, Abdallah Qahwaji Ramiand Al-Otum, Hazem"Discrete Wavelet Transform Watermarking Algorithm for Digital Colored Images, *In*: *Proceedings of the Seventh Informatics Workshop,* (p. 50-53). Bradford, UK. 2006. p. 50-53.

[21] Wang, Z., Bovic, A., Sheikh, H.,Simoncelli, E (2004). Image quality assessment: from error visibility to structural similarity, *IEEE Transactions on Image Processing,* 13 (4) 600-612.

[22] Petitcolas, F., Anderson, R (1999). Evaluation of copyright marking systems, *In*: Proc. of *IEEE Multimedia Systems'99,* v. 1, p. 574-579, Jun. 1999.