Image Copyright Protection Using Digital Watermark Based On Wavelet Transform

Bushra A. Sulttan and Muna M. Lafta*
Department of Computer Science, College of Science, University of Baghdad. Baghdad-Iraq.
** Department of Computer Science, College of education for women, University of Baghdad. Baghdad-Iraq.*

Abstract

Digital watermarking is a technique that can be used to embed a know piece of digital data (watermark data) within another piece of digital media (media to be protected) to act as a copyright protection and tracing for illegal copies for the digital media.

In recent years, it has been recognize that embedding information in transform domain leads to more robust watermarks, so in this paper wavelet transform used as transformation domain of digital image (i.e. cover image). The main concern of the proposed watermark algorithm in this paper is to embed a watermark text in the selected color image during adaptive wavelet transformation. The embedding of the watermark text (digital 0, 1) makes by separating sequential text into different groups and hidings them in specified wavelet levels in geometric manner. The embedding and extracting techniques described in this paper, and the experimental results provided as well.

Keywords: (watermarking, wavelet transform)

الخلاصة

تعتبر العلامة المائية الرقمية أحدى التقنيات المستخدمة لإخفاء بيانات رقمية ضمن وسط رقمي آخر (المراد حمايته) وذلك لحماية حقوق النشر للوسط الرقمي. تستعمل تقنية إخفاء علامة مائية(watermarking) لتمييز النسخ غير الشرعية للوسط المخزونة فيه. لوحظ في السنوات الأخيرة إن إخفاء المعلومات في المدى الترددي يؤدي إلى علامة مائية رصينة. في هذا البحث تم استخدام تقنية تحويل المويجة كمدى ترددي للصورة الرقمية المراد حمايتها. الهدف الاساسي لخوارزمية العلامة المائية المقترحة في هذا البحث هو لاخفاء علامة مائية رقمية خلال تقنية تحويل المويجة للصورة الرقمية. تتم عملية الاخفاء للعلامة المائية الحرفية(بعد تحويله الى رقمية (0،1)) بواسطة ترتيبها في مجاميع واخفاء كل مجموعة في مستوى محدد من تقنية تحويل المويجه وبشكل هندسي. تقنيات الإخفاء والاستخلاص للعلامة المائية موضحة في هذا البحث بالإضافة إلى الاختبارات والنتائج.

Introduction

Digital watermark has been introduced as a mean of effectively protecting copyrights on the digitize media such as image, audio and multimedia data. Watermark technique used to hide secret information in the digital signal to discourage unauthorized copying attest the origin of the media [1].

Watermark is a special case of general information hiding problem. The central idea is to robustly embed information in the media known as the cover object in order to produce the stego object. The embedding is done in such a way that the cover and the stego object are indistinguishable. Cover object includes: images, 3D graphics, and video [2].

Digital watermarking can be described as a communication method in which information W is embedded directly and imperceptibility into digital data *I* (e.g. images in our case), also called original data or host data, to form watermarked data $\hat{I}$, as shown in figure (1). The embedded information is bound to the watermarked data whenever it goes. The embedded information should still be decodable from the watermarked data, even if the watermarked data is processed, copied or redistributed. Thus, the information *W* could be a user-ID, a serial number for a certain copy of a document or authentication [3].

The generic watermark recovery process is depicted in figure (2). Inputs to the scheme are the watermark data $\hat{I}$, the secret or public key and, depending on the method, the original data *I* and/ or the original watermark *W*. The output is the recovered watermark. Or some kind of confidence measure indicating how likely it is for given watermark at the input to be present in the data $\hat{I}$ under inspection [1].

Watermarking categories

Image watermarking techniques can be divided into two categories according to the processing domain of the host image that the watermark is embedded in: one is to modify the intensity value of the luminance in the spatial domain. In this case, the watermark is embedded into the pixels value. The others are to change the image coefficients in the frequency domain. The frequency domain approaches are the most successful for image watermarking. The transforms that are usually used are the DCT (Discreet Cosine Transform), the DWT (Discreet Wavelet Transform) and the DFT (Discreet Fourier Transform). The watermarked image is obtained after performing an inverse transform [2].

The embedding watermark in the frequency domain of a signal can provide more robustness than the spatial domain. It is strong against attack like compression and copying, where the spatial domain is not [2].

In frequency domain the image data (BMP image) is transformed from RGB space to the YC_bC_r space (see equation (1)). Generically, YC_bC_r space consists of a luminance component Y and two color difference components C_b and C_r. The Y component contains the luminance and (black and white) image information. In YC_bC_r space, most of information is resides in the Y component. This representation used during JPEG compression. The JPEG algorithm removes large portions of the C_b and C_r component without damaging the image.

Figure (3) illustrates the frequency encoding technique; performing the 2D WT of the YC_bC_r image data creates the frequency representation. In this technique the message is added to specific locations, the chosen area represents the middle frequencies of image. It is balance between the high frequencies, which can be removed by minor JPEG compression and the lower frequencies whose modification is easily seen by the human eye. Once all of the points have been added to the magnitude image, the inverse WT is computed. Finally the image is transformed from the YC_bC_r space back to the RGB space (see equation (2)). The resulting image now has the watermark encoded in it. The message is recovered by computing the WT of the marked image; the frequency-decoded method is illustrated in figure (4) [4].

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.3 & 0.59 & 0.11 \\ 0.6 & -0.28 & -0.32 \\ 0.21 & -0.52 & 0.31 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} \text{.....(1)}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.948 & 0.624 \\ 1 & -0.276 & -0.64 \\ 1 & -1.105 & 1.73 \end{bmatrix} \times \begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} \text{....(.2)}$$

Wavelet Transforms:

Wavelets are functions defined over a finite internal and having an average value of zero. The basic idea of the wavelet transform is to represent an arbitrary function F(t) as a super position of a set of such wavelets or basis functions. These basis functions obtained from a single proto type wavelet called the mother wavelet, by dilation or contractions (scaling) and transitions (shifts). The discrete wavelet transform of a finite length signal X (n) having N components, for example is expressed by NxN matrix. The last array called the wavelet transform of the original array [5].

1- Harr wavelet transforms:

The simplest wavelet imaginable and certainly the earliest. The main properties of this wavelet:

- The support length of wavelet function (ψ) and the scaling function (φ) is 2N-1. The number of vanishing moment of ψ is N.
- The asymmetry is very pronounced.

- The regularity increase with the order. When N becomes very large,
- The analysis is orthogonal [6]

The Design of the Proposed System:

In this section, a new approach to stamp a watermark in an image is proposed, our main concerns in the design of a watermark algorithm proposed here, is to embed a Watermark text in the selected cover gray or color image during the adaptive wavelet transform. It is necessary to determine in which bands the prominent information is hidden. In the wavelet transform the most important information is held in bands with the lowest frequencies (LL). So if embed of the information about the watermark is into this band, the watermark recovery very robust; but a modification of coefficient produce great change in the final image could be seen with the naked eye. So another possibility, which is more safety to embed a watermark in the other bands

The stages of work of the proposed system will be explained briefly using the following two algorithms: the watermark embedding and the watermark recovery.

1- Watermark embedding algorithm:

Input: input image (cover image), the watermark text

Output: watermarked image.

Step1: Convert the watermark text to binary and divide it to 3 groups.

Step2: Convert the original image from RGB space to YCbCr space.

Step3: Perform the wavelet transform on Y array: at least 2 decomposition step of wavelet transform are performed to split the image to following sub bands (LL_n,LH_n,HL_n,HH_n,LH_{n-1},HL_{n-1},HH_{n-1},………,LH_1,HL_1,HH_1).

Step4: Specify 3-areas from the above sub band (choose the area in the middle frequencies band) for hiding 3-groups of binary data (watermark) using 3 different styles [see figure 5]:

- Using main diagonal.
- Using second diagonal.
- Using the cross of diagonal.

Step5: Perform the wavelet reconstruction (inverse wavelet transform) of y.

Step6: Convert the YCbCr space to the RGB space.

The embedding of step 4 is done as follows:

If the binary bit (need to be embedded) =0 then increment one to the pixel value else (if it =1) decrement one from the pixel value.

2- Watermark recovery algorithm:

Input: input image (cover image), the watermark image.

Output: watermark text.

Step1: Convert the watermarked image from RGB space to the YCbCr space as well as the original image.

Step2: Perform the wavelet transformation on Y array as well as for original image.

step3: Subtract the original image and the watermarked wavelet images in the regions of hiding specified before. The values of subtraction will be composed to one list of 0's and 1's.

step4: Convert the binary text (result of subtraction) back to characters watermark text and print it.

Step5: Repeat steps 5, 6 in the embedding algorithm.

Experiments and Results:

To evaluate and enhance the performance of the proposed system, some experiments were performed.

Two different color images of size (256x256) used in these experiments as cover image. The first "winter" was a rough image (i.e. contains more details) and the second "blue hill" was a smooth and flat image. The lengths of the watermark text are range from five to thirty characters.

<u>Experiment(1):</u> in the first experiment as shown in figure (6), we chose the watermark "copyright" and the color image "winter" as cover image .

<u>Experiment(2):</u> in the second experiment as shown in figure (7) , we use the watermark "copyright authentication" , and the color image "blue hill" as cover image .

Results:

To judge the proposed concealment algorithm for the previous two experiments, mean square error (MSE) is used between the cover and watermarked images formulated below [7]:

$$MSE=\frac{\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(p_c(i,j)-p_w(i,j)\right)^2}{m\times n}$$

Where n: depth of image.

m: width of image.

P_c(i,j): pixel value of cover image.

P_w(i,j): pixel value of the watermarked image.

For all experiments performed on the proposed system tables (1) summarize the results in error measurement as an average of ten runs.

Table (1): comparison between the error in image and the number of character in the watermark text

	MSE with different number of character in the watermark as an average of ten runs			
Images	***5 Characters***	***10 characters***	***20 characters***	***30 characters***
winter	0.0024	0.0028	0.0062	0.0116
Blue hill	0.0126	0.0318	0.0631	0.0629

The imperceptibility results above according to the experiments are very high as the resulted MSE was very low.

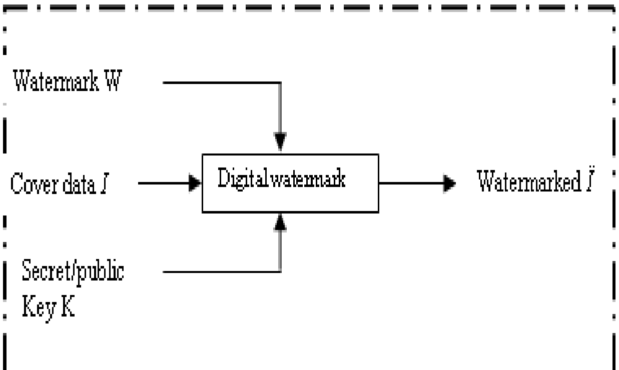


Figure (1): Generic digital watermark scheme

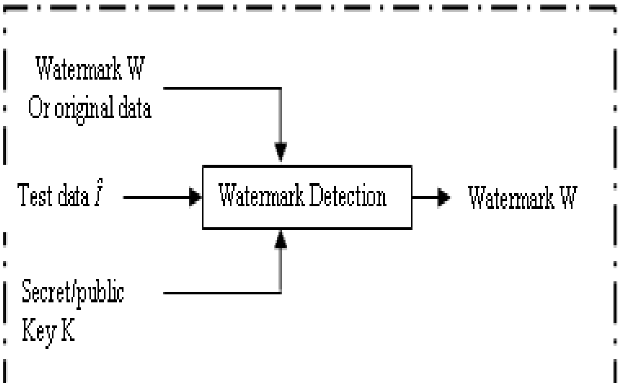


Figure (2): Generic watermark recovery scheme

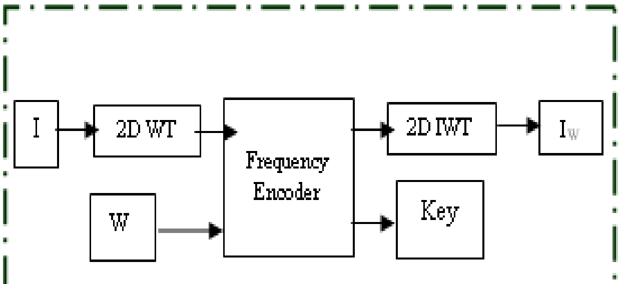


Figure (3): Frequency encoder

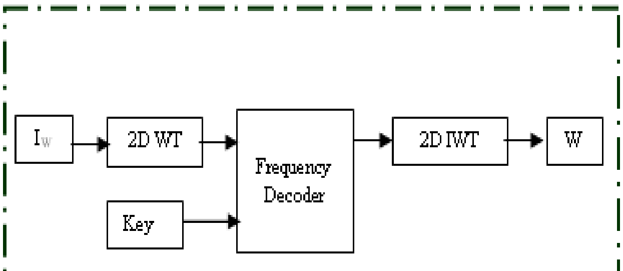


Figure (4): Frequency decoder

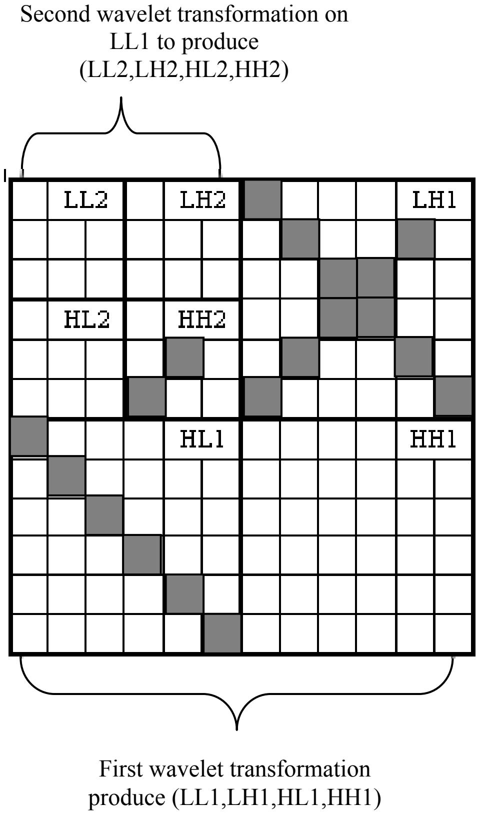
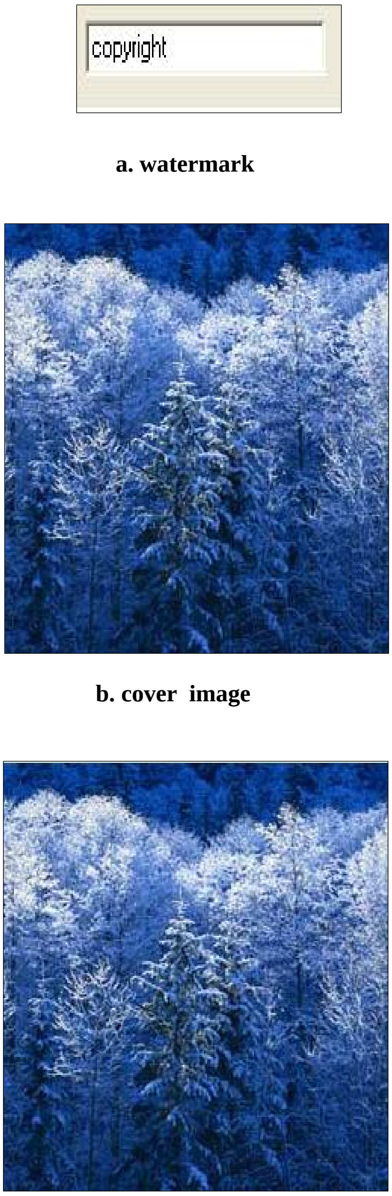

Second wavelet transformation on
LL1 to produce
(LL2,LH2,HL2,HH2)
LL2
LH2
LH1
HL2
HH2
HL1
HH1
First wavelet transformation
produce (LL1,LH1,HL1,HH1)

Figure 5. Illustrate the number of wavelet transformation that performed and the decomposition of an image and the style of hiding in the selected regions. The shaded positions represent pixel contain watermark bit.



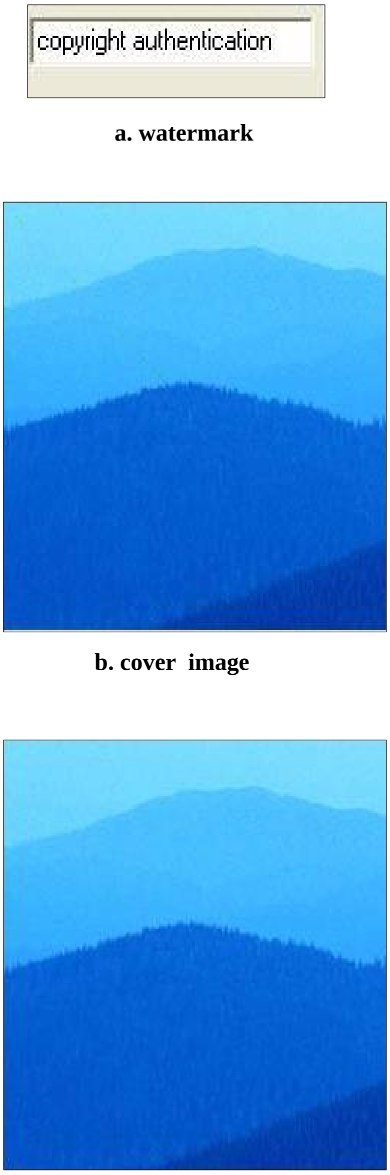
copyright

a. watermark

b. cover image

c. watermarked image

Figure6. Experimental result winter as the cover image



copyright authentication

a. watermark

b. cover image

c. watermarked image

Figure7. Experimental result blue hill as the cover image

Conclusions

From the result of the proposed system, one can deduce the following:

1. The proposed algorithm can produce imperceptible change to the cover image
2. If one wants to attack the cover image, must know the restriction of the embedding algorithm (number of wavelet transformation times, regions of hiding, positions of hiding and the number of character hide in each regions).
3. This algorithm is suitable when the cover image contains more data, and its palette contains more homogenous colors.

References

1. Stefan Ketzenbeisser and Fabien A. P. Perircolas, **2000** **"***Information Hiding Techniques for Steganography and Digital Watermarking***"**, Artech House, London.
2. Ammar T., December **2002**, "*Image Copyright Protection Using Digital Watermark*", M. Sc Thesis, Computer Science Department, Collage of Science , Al-Nahrain University, Baghdad,.
3. Sviatolsav Voloshynovskiy, Shelby Pereira, and Thierry Pun, **2001** **"***Attack on Digital Watermarks: Classification, Estimation-Based Attacks, and benchmarks***"**, IEEE**.**
4. Andrew S. Tanenbaum, **1996** **"***Computer Networks***"**, Prentice-Hall Inc., Third Edition.
5. Strang, G. and Nguyen, T., **1996** **"***Wavelets and Filter Banks***"**, Wellesley-Cambridge Press, Wellesley, AM**.**
6. **"***Help of Mat lab Version 7* **"**, May 06, **2004**.
7. S.E Umbangh, **1998** **"***Computer Vision and Image Processing***"**, prentice-Hall, Inc.