Journal of Applied Sciences

ISSN 1812-5654

Journal of Applied Sciences 10 (19): 2168-2186, 2010
ISSN 1812-5654
© 2010 Asian Network for Scientific Information

Digital Watermarking System based on Cascading Haar Wavelet Transform and Discrete Wavelet Transform

Nidal F. Shilbayeh and Adham Alshamary
Faculty of Information Technology, Middle East University,
P.O. Box 42, Postal Code 11610, Amman, Jordan

Abstract: The aim of this study was to solve problems of modification, forgery, illegal manipulation and distribution of digital image, especially with the rapid growth of transmission techniques. Although, there are many ways to protect the images, the proposed system suggested a new technique to protect the image for the purposes of ownership, copyright and intellectual property. In this study, we present a new robust and secure hybrid watermarking technique based on Haar Wavelet Transformation (HWT) and Discrete Wavelet Transformation (DWT). The proposed method is constructed by cascading two different but complementary techniques: HWT and DWT wavelet transformations to provide a robust resistance to the protected image against different signal processing attacks. Adding a private key to the watermarking will increase the privacy and security, but by embedding watermark in that private key more protection in wavelet transform will result, leading to more resistant against attacks. The new technique has been proposed to solve the problem of illegal manipulation and distribution of digital image, i.e., HWT and DWT system. Performance evaluation of the proposed method showed improved results in terms of imperceptibility, robustness and security in comparison with others systems.

Key words: Image watermarking, watermark embedding, watermark detection, Haar Wavelet Transform (HWT), Discrete Wavelet Transform (DWT), image attacks

INTRODUCTION

In the recent years, a huge amount of digital information is circulating through the world by means of the rapid and extensive growth in internet technology; therefore there is a pressing need to develop several newer techniques to protect copyright, ownership and content integrity of digital media. Most of such data is exposed and can be easily forged or corrupted, consequently the need for intellectual property rights protection arises. This necessity arises because the digital representation of media possesses inherent advantages of portability, efficiency and accuracy of information content on one hand, but on the other hand, this representation also puts a serious threat on easy, accurate and illegal perfect copies of unlimited number. Unfortunately, the currently available formats for image, audio and video in digital form do not allow any type of copyright protection. Digital watermarking has been proposed as one of the possible ways to deal with this problem, to keep information safe.

Digital watermarking, an extension of steganography, is a promising solution for content copyright protection, it imposes extra robustness on embedded information. In other words, digital watermarking is the art and science of embedding copyright information in the original files. The information embedded is called watermarks.

Information hiding is a general practice encompassing a broad range of applications in which the messages are embedded into the other media content for varying purposes, while watermarking and steganography are two types of information hiding. Steganography, which is derived from the Greek words means, covered writing that hides the secret message into innocuous host content to achieve covert communication (Lin and Delp, 1999). In order to act as a successful camouflage to conceal the very existence of the secret message, the host media content is usually chosen to have nothing to do with the hidden information. Similar to Steganography, watermarking is also a procedure of imperceptibly embedding the information, i.e., a digital watermark, into the content. However, a digital watermark usually represents the ownership of the content, the identity of the legitimate content user or other information used to help protect the lost content. In other words, there exists a strong relationship between the embedded digital

Corresponding Author: Nidal F. Shilbayeh, Faculty of Information Technology, Middle East University,
P.O. Box 42, Postal Code 11610, Amman, Jordan

watermark and the host content. Besides, in order to achieve the intended functions, the existence of a digital watermark is usually known to the users, in contrast to the fact that the hidden. between the host media content and hidden information is a differentiating factor between digital watermarking and steganography (Cachin, 1998).

The digital image watermarking techniques in the literature are typically grouped into two classes (Yeung *et al*., 1998): the spatial domain spatial domain and frequency domain watermarking techniques. Compared to spatial domain techniques (Darmstaedter *et al*., 1998) frequency domain techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms

Commonly used frequency domain transforms include the Discrete Cosine Transform (DCT), Wavelet Transform (WT), the Discrete Contourlet Transform (CT) and the Discrete Fourier Transform (DFT). However, DWT has been frequently used due to its excellent spatial localization and multi resolution characteristics, which is very close to theoretical models of the human visual system (Cabir and Serap, 2007; Houng-Jyh *et al*., 1998; Inoue *et al*., 1999). Recent improvements obtained by combining these frequency domain transforms (Al-Haj, 2007):

- Recently, to recognize key ideas, theories and conclusion and sets the difference and similarities. In the following, we will summarize some of such related works
- Stephan (2005) embedding watermarking in still images (BMP) true color, this method applies embedding watermark in large coefficients and in high frequency subbands by using discrete wavelet transform. The watermark in this method is capable of surviving against the JPEG2000 compression and the watermark extracted using original image (non-blind watermark)
- Lepik (2007) demonstrates that the Haar wavelet method is a powerful tool for solving different types of integral equations and partial differential equations. This method with less degree of freedom and with smaller CPU time provides better solutions than classical ones
- Cabir and Serap (2007) a new digital image watermarking algorithm that combines the strengths of the moment based image normalization and two dimensional discrete wavelet transform was proposed by the researchers. Normalization provides robustness against geometrical degradations, whereas, discrete wavelet transform achieves immunity for compression, linear and non-linear filtering by taking the properties of the human visual system into consideration. This method is powerful to resist numerous image manipulations.
- Wu *et al.* (2008) the authors in their work propose a novel watermarking method to solve the problem of. For copyright protection, their new method makes a difference by providing the user with the power to process masses of digital image watermarking tasks using just one private key
- Tsai (2009) the authors studied novel visible watermarking algorithm based on the content and contrast aware (COCOA) technique with the consideration of Human Visual System (HVS) model. In order to determine the optimal watermark locations and strength at the watermark embedding stage, the COCOA visible watermarking utilizes the global and local characteristics of the host and watermark images in the discrete wavelet transform (DWT) domain
- Leung *et al.* (2009) these researchers proposed a selective curvelet coefficient digital watermarking algorithm. The selective band provides an addition security feature against any physical tampering. Their reported goal was to give an intensive study on the robustness of watermarking using selective curvelet coefficients from a single band and to find out the best band for embedding watermark. Wrapping of specially selected Fourier samples is employed to implement Fast Discrete Curvelet Transforms (FDCT) to transform the digital image to the curvelet domain
- Bayram and Selesnick (2009) they developed an over complete discrete wavelet transform (DWT) based on rational dilation factors for discrete-time signals. It was implemented using self-inverting FIR filter banks. It is approximately shift-invariant and can provide a dense sampling of the time-frequency plane. This algorithm is based on matrix spectral factorization

In this study, we propose a robust method for digital watermarking and secure copyright protection of digital images. The proposed watermarking system is based on cascading two transforms; HWT and DWT. The system is proofs resist against numerous image attacks. Furthermore, the method is easy to implement and suitable for real time application. Adding a private key to the new technique gives more robustness and security to the watermarked image against attacks.

WATERMARKING OVERVIEW

Digital watermarking means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. It is a signal added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data (Amin *et al*., 2003).

Watermarking applications: Digital watermarking is described as a viable method for the protection of ownership rights of digital image and other data types. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control and secret communication (Cox *et al*., 1997, 2000; Karzenbeisser and Perircolas, 2000).

Properties of watermarking system: When designing a watermarking system, several properties must be observed, among which are the following (Kutter and Hartung, 2000):

- Imperceptibility-the watermark should be invisible not to degrade data quality and to prevent an attacker from finding and deleting it
- Readily detectable-the data owner or an independent control authority should easily detect the watermark
- Unambiguous-retrieval of it should unambiguously and unequivocally identify the owner of the data with a high degree of confidence
- Robust-difficult to remove without producing a remarkable degradation in data fidelity
- Security-unauthorized parties should not be able to read or alter the watermarking

Watermarking techniques: There are many different watermarking techniques and they range from the very simple to the complex (Das *et al*., 2010). Obviously the type and the value of the content would determine the watermarking technique to be used. For the image watermarking, there are a number of schemes of varying robustness that have been implemented (Haldar, 2008). These techniques have their strong and weak points. Typically they fall into two categories: Spatial and Transform domain (Yeung *et al*., 1998).

Spatial domain watermarking: Watermarking was the first scheme that introduced works directly in the spatial domain. By some image analysis operations (e.g., edge detection) it is possible to get perceptual information key, directly in the intensity values of predetermined regions of the image (Paquet, 2001). Those simple techniques provide a simple and effective way for embedding an invisible watermark into an original content but don't show robustness to common alterations (Cox *et al*., 2002; Wolfgang *et al*., 1999). One of the most famous spatial techniques is Least Significant Bit (LSB) (Hanjalic *et al*., 2000).

One straightforward and rapid technique is based on the principle of generating a pseudo-generated noise pattern and integrates it into specific chrominance or luminance pixel values (Darmstaedter *et al*., 1998). Such pseudo-random noise patterns consist of black (1), white (-1) and neutral values (0). The pseudo noise is generated with a secret key and algorithm. Additionally, the process could be adjusted to the image components or feature vectors to achieve a higher level of invisibility. In general, the watermark W(x, y) is integrated into the image components I(x, y) by a factor that allows amplification of the watermarking values in order to obtain the best results as shown in Eq. 1:

$$I_W(x,y) = I(x,y) + k * W(x,y) \qquad (1)$$

Frequency domain watermarking: It is also known as transforming domain watermarking (Grans, 2003). Another way to produce high quality watermarked content is by first transforming the original content (e.g., Image) into the frequency domain by the use of Fourier, Discrete cosine or wavelet transform. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients (Robi, 2004), then inverse transforming the marked coefficients from the watermarked image. The use of frequency based transforms allows the direct understanding of the content of the image (Grans, 2003). Therefore, characteristics of the Human Visual System (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermarks to be applied to a given image (Kunder and Hatzinkos, 2001). Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original image (Murtag, 2007). The following are some techniques of the frequency transform domain.

Discrete Fourier Transform (DFT): The scholar Joseph Fourier in 1822 produced what is known as Fourier analysis, which is a method to present periodic signals by using a series of sine and cosine.

The transformer transfers the signal from the space of time to space of frequency and vice versa and Fourier transform is mathematically defined as in Eq. 2:

$$x(f) = \int_{-\infty}^{+\infty} x(t).e^{-jwt}.dt \tag{2}$$

But the problem is that the Fourier transform becomes inactive for the non-stationary signals (variable frequency) because it does not provide us with information on the frequency content over time (Dittmann, 2000).

The Discrete Cosine Transform (DCT): DCT is a real domain transform which represents the entire image as coefficients of different frequencies of cosines (Which are the basis vectors for this transform). The DCT of the image is calculated by taking (8×8) blocks of the image, which are then transformed individually. DCT also forms the basis of JPEG image compression algorithm, which is one of the most widely used image data storage formats. The DCT approaches are able to withstand some forms of attack (Hsu and Wu, 1998; Dittmann, 2000).

The Wavelet Transform based techniques (WT): The wavelet transform provides the time frequency transformation of a given signal (Paquet, 2001). Wavelet transform is capable of providing the time and frequency information simultaneously, hence giving a time-frequency representation of the signal.

The problem is the huge number of wavelet resulting from the use of all the gradations in the process of analysis and the reams of information, which also produced for the same reason and therefore the treatment process requires a very long time.

Two transformers are using unlimited number of gradations, rather than make the conversion for all the gradations and are done by selecting time domains in the signal (Kunder and Hatzinkos, 2001; Inoue *et al*., 1999; Radomir and Bogdan, 2003). This conversion produces a sufficient quantity of information, with less time of accounting and maintaining the basic information of the depicted reference (i.e., without the loss of important information).

Attacks on digital watermarks Watermarking research has produced a wide range of watermarking techniques that can be subdivided into various methodological complexity levels. Each of these methods attempts to reduce vulnerability in various attack scenarios. Attacks on digital watermarks can be mainly classified into two major groups:

- Friendly and malicious attacks (Hanjalic *et al*., 2000; Hartung *et al*., 1999)
- Conventional image or data operations applied in the normal use of computer technology can destroy the watermark information. Different operation of the classical image processing field, such as scaling, color and gamma corrections and so forth, can be identified at this point. Today, compression techniques can also be placed in the field of classical operations, but often separated as a single element in watermarking research. The friendly attack has two common features. It is generally described as an unintentional event where the user has no suppose and/or knowledge of the watermark and its embedded procedure. The second type of attack, the malicious attack, occurs with the intention of eliminating the information (Hanjalic *et al*., 2000)

THE PROPOSED SYSTEM

The proposed system generally consists of two independent, but complementary subsystems. The first subsystem is called the Haar Wavelet Transform (HWT) and the second subsystem is called the Discrete Wavelet Transform (DWT). The general structure of the proposed system is shown in Fig. 1.

Haar Wavelet Transform subsystems (HWT): The main tasks of the HWT subsystems:

- A standard decomposition of a 2-D signal (image), this is done by performing a one dimensional transformation on each row followed by a one dimensional transformation of each column
- Construct a function that Haar Transforms an image for differed levels

Figure 2 shows the general structure of the HWT and shows its main parts. Essentially, each part is a complementary for the other parts and represents a task in the HWT Process.

This subsystem applies wavelet transform by using Haar Wavelet. The main function of Haar Wavelet Transform can be explained through the following steps:

- Load an image (300×300 pixel)
- Apply HWT Process. It consists of the following processes:

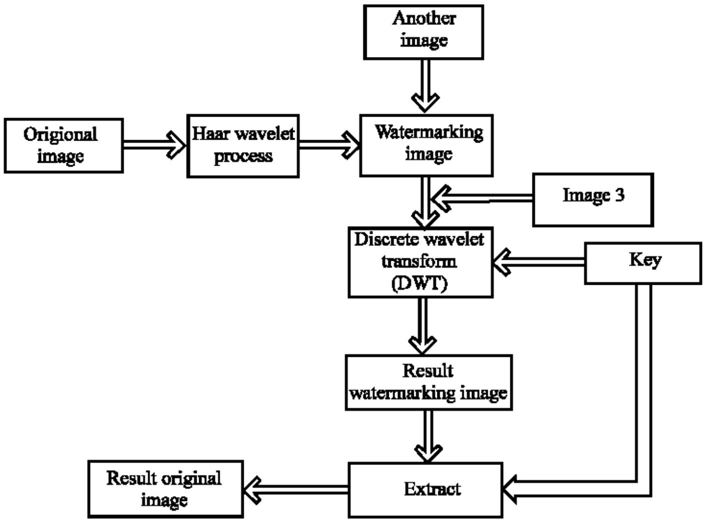


Fig. 1: General structure of the proposed system

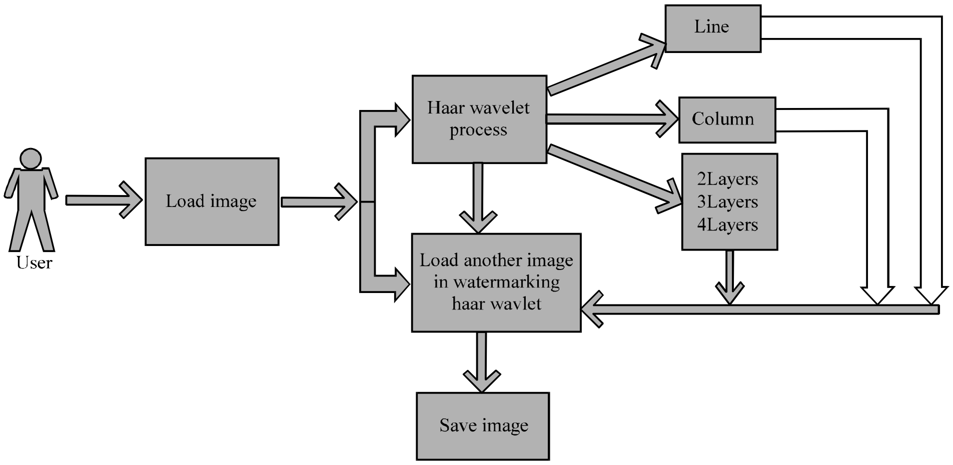


Fig. 2: HWT subsystem

Line transformation: This also is called row. It decompose the image into rows using the flowing code:

```
/*row transformation*/
for(i = 0;i<row;i++){w = col;
do{ k = 0;
/*averaging*/ for(j = 0;j<w/2;j++)
a[j] = ((mat[i][j+j]+mat[i][j+j+1])/2);
/*differencing*/ for(j = w/2;j<w;j++,k++)
a[j] = mat[i][j-w/2+k]-a[k];
for(j = 0;j<row++) mat[I] [j] = a[j];
w = w/2;
}while(w! = 1);
}
```

Columns transformation: It decompose the image into columns using the following code: another image:

```
{
/*column transformation*/
for(i = 0;i<col;i++){ w = row;do      {k = 0;
/*averaging*/ for(j = 0;j<w/2;j++)
a[j] = ((mat[j+j][i]+mat[j+j+1][i])/2);
/*differencing*/for(j = w/2;j<w;j++,k++)
a[j] = mat[j-w/2+k][i]-a[k];
for(j = 0;j<w;j++) mat[j][i] = a[j];
w = w/2;
} while(w! = 1);
}
```

Two, three, four layers wavelet transform: It decomposes the image into two layers, three layers, or four layers. To understand how the Haar Wavelets Transform works, let us consider the following simple example; suppose we have one dimension we have image with a resolution of

Table 1: Decomposition to lower resolution

Resolution	Averages	Detail coefficients
4	[8 6 3 7]	
2	[7 5]	[1-2]
1	[6]	[1]

four pixels having values [8, 6, 3, 7]. Haar wavelet basis can be used to represent this image by computing a wavelet transform. To do this, we find the average of two pixels together, results the pixel values [7, 5]. Clearly, some information is lost in this averaging process. We need to store some detail coefficients to recover the original four pixel values from the two averaged values. In our example, 1 chosen for the first detail coefficient, since the average computed is 1 less than 8 and I more than and 1 more than 6. This single number is used to recover the first two pixels of our original four-pixel image. Similarly, the second detail coefficient is-2, since 5+ (-2) = 3 and 5-(-2) = 7. Thus, the original image is decomposed into a lower resolution (two-pixel) version and a pair of detail coefficients.

Regarding this process recursively on the averages gives the full decomposition shown in Table 1.

Thus, for the one-dimensional Haar basis, the wavelet transform of the original four-pixel image is given by [6, 1, 1 and -2]. We call the way used to compute the wavelet transform by recursively averaging and differencing coefficients, filter bank.

We can reconstruct the image to any resolution by recursively adding and subtracting the detail coefficients from the lower resolution version.

Compression of 2-D image with haar wavelet technique: It has been shown in the previous section how 1-D image can be treated as sequences of coefficients. Alternatively, we can think of images as piecewise constant functions on the half-open interval [0, 1]. To do so, the concept of a vector space is used. A one-pixel image is just a function that is constant over the entire interval [0, 1]. Let V^0 be the vector space of all these functions. A two pixel image has two constant pieces over the intervals [0, 1/2] and [1/2, 1]. We call the space containing all these functions V^1. If we continue in this manner, the space V^j will include all piecewise-constant functions defined on the interval [0, 1] with constant pieces over each of 2^j subintervals. Note that because these vectors are all functions defined on the unit interval, every vector in V^j is also contained in V^{j+1}. For example, we can always describe a piecewise constant function with two intervals as a piecewise-constant function with four intervals, with each interval in the first function corresponding to a pair of intervals in the second. Thus, the spaces V^j are nested; that is, $V^0 \subset V^1 \subset V^2$ this nested set of spaces V^j is α necessary ingredient for the mathematical theory of multiresolution analysis. It guarantees that every member of V^0 can be represented exactly as a member of higher resolution space V^1. The converse, however, is not true: not every function G (x) in V^1 can be represented exactly in lower resolution space V^0.

Now we define a basis for each vector space V^j. The basis functions for the spaces V^1 are called scaling functions and are usually denoted by the symbol **ϕ**. A simple basis for V^j is given by the set of scaled and translated box functions as shown in Eq. 3:

$$\Phi_i^j(x) := \Phi(2^j x - i) \qquad i = 0, 1, 2 \ldots 2^j - 1$$

Where:

$$\Phi(x) := \begin{cases} 1 & \text{for } 0 \le x < 1 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

The wavelets corresponding to the box basis are known as the Haar wavelets, given by Eq. 4:

$$\Psi_i^j(x) := \Psi(2^j x - i) \qquad i = 0, 1, 2 \ldots 2^j - 1$$

Where:

$$\Psi(x) := \begin{cases} 1 & \text{for } 0 \le x < 1/2 \\ -1 & \text{for } 1/2 \le x < 1 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Thus, the DWT for an image as a 2-D signal will be obtained from 1-D DWT. we get the scaling function and wavelet function for 2-D by multiplying two 1-D scaling functions: Ø (x-y) = Ø (x) Ø (y). The wavelet functions are obtained by multiplying two wavelet functions for wavelet and scaling function for 1-D. For the 2-D case, three exist there wavelet functions that scan details in horizontal **Ψ**(1) (xy)) = Ø (x) **Ψ**(y), vertical **Ψ**(2) (x.y) = **Ψ**(x) Ø (y) and diagonal directions; **Ψ**(3) (x.y) = Ø(x) **Ψ**(y). This may be represented as a four channel perfect reconstruction filter bank. Now; each filter is 2-D with the subscript indicating the type of filter high pixels frequency (HPF) low pixels frequency (LPF) for separable horizontal and vertical components. By using these filters in one stage, an image is decomposed into resolution: horizontal (HL), vertical (LH) and diagonal (HH). The operations can be repeated on the low (LL) band using the second stage of identical filter bank.

Thus, a typical 2-D Hear transform, used in image compression and can be represented as a four channel perfect reconstructions as shown in Fig. 3.

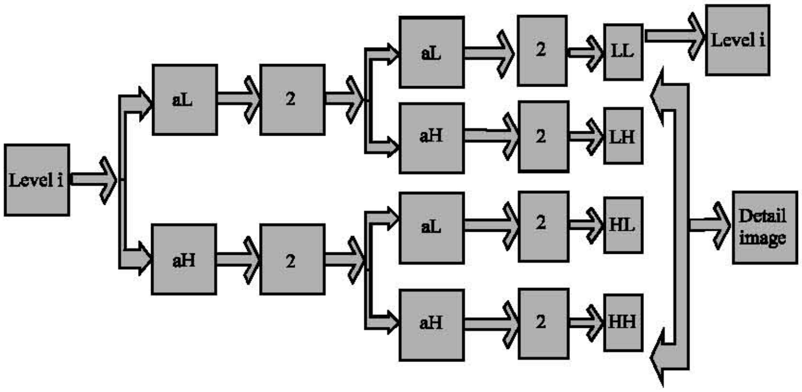


Fig. 3: Structure of 2D haar wavelet proposed systems

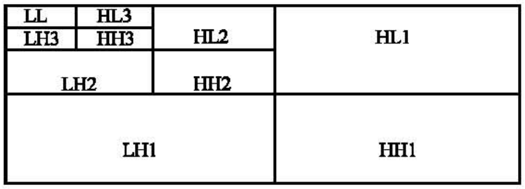


Fig. 4: Structure of wavelet decomposition

The WT (Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple scale wavelet decomposition, as in the three scales WT shown in Fig. 4.

The transformation of the 2-D image is a 2-D generalization of the 1-D wavelet transformed already discussed. This operation provides us with an average value and detail coefficients for each row. Next, these transformed rows are treated as if they were themselves an image and apply the 1-D transform to each column. The resulting values are all detail coefficients except a single overall average coefficient. In order to complete the transformation, this process is repeated recursively only on the quadrant containing averages.

Now let us see how the 2-D Harr Wavelet Transformation is performed. The image is comprised of pixels represented by numbers consider the 8x8 image taken from a specific portion of a typical image shown in Fig. 5. The matrix (a 2D array) representing this image is shown in Fig. 6.

Now we perform the operation of averaging and differencing to arrive at a new matrix representing the same image in a more concise manner. Let us look how the operation is done.

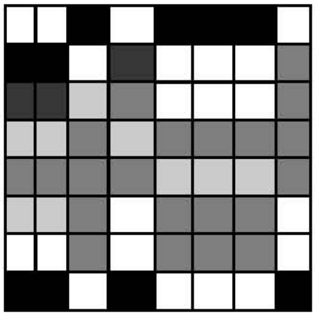


Fig. 5: 8×8 image

$$\begin{pmatrix} 56 & 10 & 1 & 63 & 58 & 8 & 10 & 54 \\ 11 & 53 & 52 & 14 & 14 & 50 & 51 & 16 \\ 20 & 44 & 46 & 37 & 22 & 42 & 40 & 24 \\ 39 & 27 & 26 & 38 & 34 & 32 & 31 & 34 \\ 31 & 35 & 34 & 30 & 30 & 36 & 40 & 24 \end{pmatrix}$$

Fig. 6: 2D arrays that representing Fig. 5

- **Averaging:** (56+10)/2 = 33, (1+63)/2 = 32, (58+8)/2 = 33, (10+54)/2 = 32
- **Differencing:** 56-33 = 23, 1-32 =-31, 58-33 = 25 and 10-32 =-22

So, the transformed now becomes (33 32 33 32 23-31 25-22). Now the same operation on the average values i.e., (32.5 32.5 0.5 0.5 23-31 25-22) is performed. Then we perform the same operation on the averages i.e. first two elements of the new transformed row. Thus the final transformed row becomes (32.5 0 0.5 0.5 32-31 25-22). The new matrix we get after applying this operation on each row of the entire matrix of Fig, 6 is shown in Fig. 7.

We get the final transformed matrix as shown in Fig. 8. This operation on rows followed by columns of the matrix is performed recursively depending on the level of transformation meaning the more iteration provides more transformations. Knowing that the left-top element of the Fig. 8 i.e., 32.5 is the only averaging element which is the overall average of all elements of the original matrix and all the remaining elements are details coefficients.

The point of the wavelet transform is that regions of little variation in the original image manifest themselves as small or zero elements in the wavelet transformed version. A matrix with a high proportion of zero entries is said to be sparse for most of the image matrices. Their corresponding wavelet transformed versions are much sparser than the original. Sparse matrices are easier to store and transmit than ordinary matrices of the same size.

This is because the sparse matrices can be specified in the data file solely in terms of locations and values of their non-zero entries.

It can be seen that in the final transformed matrix, we find a lot of zero entries. From this transformed matrix, the original matrix can be easily calculated just by the reverse operation of averaging and differencing, i.e., the original image can be reconstructed from the transformed image without loss of information. Thus, it yields a lossless compression of the image. However, to achieve more degree of compression, we have to think of the lossy compression.

$$\begin{pmatrix} 32.5 & 0 & 0.5 & 0.5 & 23 & 25 & -22 \\ 32.5 & 0 & -0.5 & -0.5 & -21 & -18 & 18 \\ 32.5 & 0 & -0.5 & -0.5 & -12 & -10 & 7 \\ 32.5 & 0 & 0.5 & 0.5 & 6 & 1 & -2 \\ 32.5 & 0 & 0.5 & 0.5 & -2 & -3 & 8 \end{pmatrix}$$

Fig. 7: Transformed array after operation

$$\begin{pmatrix} 32.5 & 0 & 0 & 0 & -0.5 & -3.75 & -0.375 & 0.375 \\ 0 & 0 & 0 & 0 & -0.5 & -3.75 & -0.125 & -0.125 \\ 0 & 0 & 0 & 0 & -2 & 0.5 & 4 & -2.25 \\ 0 & 0 & 0 & 0 & 3 & -4 & 4.75 & -3.5 \\ 0 & 0 & 0.5 & 0.5 & 22 & -25 & 21.5 & -20 \end{pmatrix}$$

Fig. 8: Final transformed matrix after one step

Namely by using a suitable threshold, that is replacing by zeros all entries with small absolute value. But this means that the inverse transformation will not produce the original mage exactly.

The watermarking based on WT uses Eq. 5:

$$\mathrm{Iwx,y} = \begin{cases} \mathrm{Wi} + \alpha|\mathrm{Wi}|\mathrm{xi}, \ldots \mathrm{u,v} \in \mathrm{HL,L} \\ \mathrm{Wi} \ldots \quad \ldots \quad \ldots \quad \mathrm{u,v} \in \mathrm{LL,HH} \end{cases} \tag{5}$$

where, W_i denotes the coefficient of the transformed image into wavelet domain, x_i the bit of the watermarking to be embedded and $\alpha$is a scaling factor. Figure 9 shows the embedding of a watermarking in the wavelet domain.

The following paragraph explains the embedding watermark in wavelet method; input the original image (24-bit), the embedding algorithm is described in the following steps:

Step 1: Input the original image, anther image
Step 2: The size of the image should be same
Step 3: Decompose image by using Haar wavelet transform
Step 4: Load the watermark into the suitable subband of the original image
Step 5: Convert the watermark into a stream of bits (zeroes and ones)
Step 6: The watermark will match the size of the matrix
Step 7: Convert every image from RGB to matrix color format
Step 8: Save watermarked color image
Step 9: Display watermarked image

Discrete wavelet transform subsystems: The second subsystem is the Discrete Wavelet Transform (DWT).

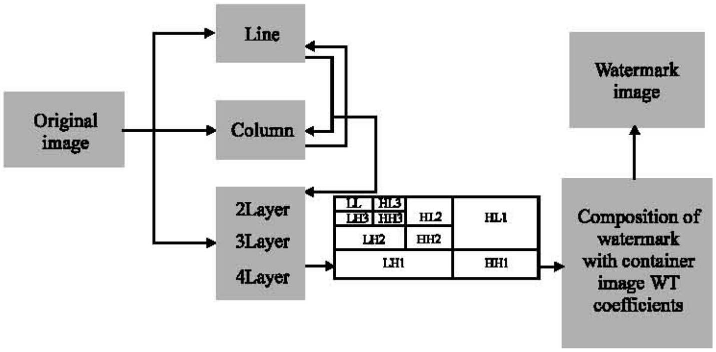


Fig. 9: Embedding of a watermarking in the wavelet domain

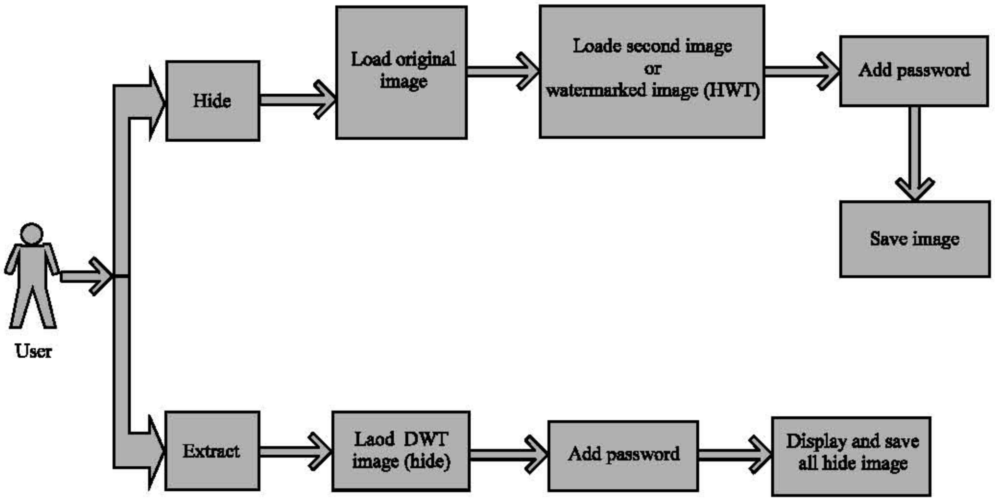


Fig. 10: DWT subsystem

Figure 10 shows the general structure of the DWT and shows its main parts.

This subsystem consists of two parts, which are Hide and Extract.

Hide (embedding) part: To understand the embedding technique we will describe it through the following:

Let I be a color image with M*N pixels which consists of channels R, G and B. The three channels are divided into a set of n*n (n is odd) non-overlapping subblocks. In general, the size of the subblock has an influence on the robustness of the watermark. Each watermark bit can be embedded into one subblock by modifying the values of the subblock's middle pixel and the other pixels. Let us define m as the middle pixel value and u as the mean value of the other pixels. For example, it is supposed that the authors have a 3*3 subblock as shown in Fig. 11. In this case, P5 is the middle pixel value m and the mean value of the other pixels can be computed by μ (P1 + P2 + P3 + P4 + P6 + P7 + P8 + P9)/8. To control the balance between the robustness and image quality, the robustness coefficient value T must be used; different robustness coefficient values for channels R, G and B are used:

TR is the robustness coefficient value of channel R, TG is for channel G and TB is for channel B.

Basically, the visual effect to modify the R, G and B channels is different in terms of the human visual sensitivity. In addition, the B channel has the larger tolerance to be modified than that of other channels. For these reasons, the robustness coefficient value TB used in the scheme is the largest value. TR and TG are the secondly and minimal respectively. The other advantage to adopt varied robustness coefficient is that the whole survival rate of watermark bit can be enhanced.

P_1	P_2	P_3
P_4	P_5	P_6
P_7	P_8	P_9

Fig. 11: Subblock of size 3*3

The Hide part process is described as follows:

- Load the original image which has a size larger than the size of second image (embedded image)
- Load the second image which has size smaller than the original image. The second image may be a watermarked image generated by the first subsystem (HWT)
- Save image
- Add password

This part is giving more security for the watermarked image because it's embedded image, which differ than other techniques. Used in watermarking As well as, adding the password key gives additional security for the watermarked image.

The procedure of the embedding algorithm is as follows:

- Input original image, image watermarking
- Divide channels R, G and B into a set of n*n non-overlapping subblocks, respectively
- Set the robustness coefficient values TR, TG and TB for channels R, G and B respectively. In the next step, T represents TR, TG and TB when channels R, G and B are chosen to hide the watermark, respectively

- Modify m (middle pixel) and μ (other pixels) for watermark embedding in the following:

$$\mathrm{IF}(W_k = 1) \quad \text{and} \quad (m - u \geq T)$$

No Modify
Else

$$(m,u) = (m + \left\lceil \left|(m-u) - \frac{T}{2}\right| \right\rceil, u - \left\lfloor \left|(m-u) - \frac{T}{2}\right| \right\rfloor) \qquad (6)$$

$$\mathrm{IF}(W_k = 0) \quad \text{and} \quad (u - m \geq T)$$

No Modify
Else

$$(u,m) = (u + \left\lceil \left|(u-m) - \frac{T}{2}\right| \right\rceil, m - \left\lfloor \left|(u-m) - \frac{T}{2}\right| \right\rfloor) \qquad (7)$$

- Add the password (owner PRK) to watermarking to hide part
- Save watermarked image

In Eq. 6 and 7, the μ value can be adjusted by subtracting or adding the pixel values P1, P2, P3, P4, P5, P6, P7, P8 and P9, respectively. When the first watermark bit has been embedded on channel R, the same location on channels G and B are also chosen to embed the first watermark bit.

Extract (recover) part: In the method of watermark Extraction in Wavelet, we need to input the watermarking image where the output is the original image. Watermark extraction needs to have some original data (original image). It is performed using Independent Component Analysis (ICA) which is applied to the bands of original and watermarked images and, extracted by the backward embedding formula. The procedures of an extraction after various attacks are realized in purpose to check the watermark robustness against attacks. The quality of the extracted watermark is calculated using the correlation coefficient. The advantages of ICA algorithm approach include storage of less information by the image's owner and better quality of the extracted watermark in the case of attacks.

Independent Component Analysis (ICA) is a statistical and computational technique for revealing hidden factors that underlie sets of random variables, measurements, or signals. ICA defines a generative model for the observed multivariate data, which is typically given as a large database of samples. In the model, the data variables are assumed to be linear mixtures of some unknown latent variables and the mixing system is also unknown. The latent variables are assumed to be not Gaussian and mutually independent and they are called the independent components of the observed data. These independent components, also called sources or factors, can be found by ICA which is superficially related to principal component analysis and factor analysis. ICA is a much more powerful technique, however, capable of finding the underlying factors or sources when these classic methods fail completely.

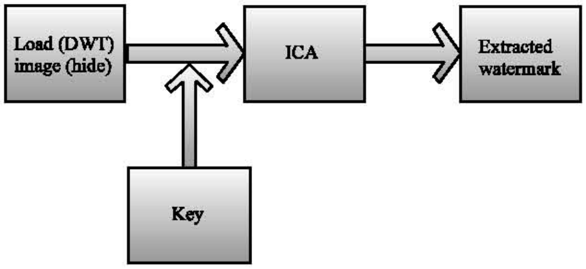


Fig. 12: Extraction scheme using ICA

Following are the steps of Extract part process as shown in Fig. 12:

- Load the DWT image (generated in Hide part)
- Add password (that used in Hide part)
- Display and save all Hided images

The extraction algorithm is described in the following steps:

Step 1: Input watermarked image
Step 2: Add the password (owner PRK) to the watermarked image
Step 3: Divide channels R, G and B into a set of n*n non-overlapping subblocks, respectively
Step 4: Compute the middle pixel value m and the mean value μ of the subblock
Step 5: Recover the watermark bit by comparing m with μ according to the following statements:

If m>μ: The watermark bit 1 is extracted
Else: The watermark bit 0 is extracted

Step 6: Read the next watermarked subblock and repeat Step 4 and 5 until all the watermark bits are extracted
Step 7: Display original image

When the first watermark bit is extracted from channel R, the watermark bit hidden on channels G and B can also be extracted using the proposed extracting algorithm.

EXPERIMENTAL RESULTS

Here, we will demonstrate the steps of using the proposed system. After selecting the watermark image shown in Fig. 13, the user should select the Haar Wavelet Transform subsystem. Figure 14, 15 show the effect of choosing the line transform and the column transform processes.

Figure 16-18 show the effect of 2Layer WT, 3Layer WT and 4 Layer WT on the selected image, respectively.

The processes of HWT can be selected randomly and in any combination. After selecting the desired HWT, the next step is selecting the watermarking option form the main menu and chooses another image (using the same steps of open option) Fig. 19 shows process of watermarking on the original image.

The next step, the user should choose Discrete Wavelet Transform (DWT) process. DWT process consists of two parts Hide and Extract.

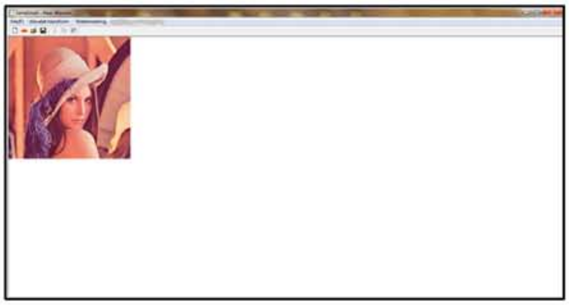


Fig. 13: Watermark image

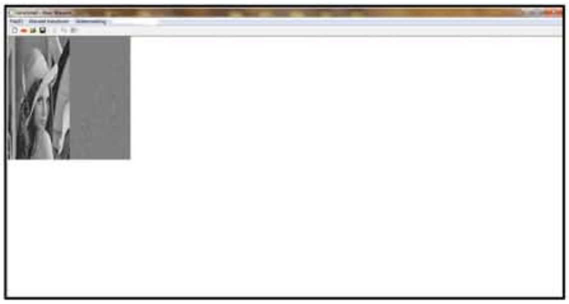


Fig. 14: Line transform

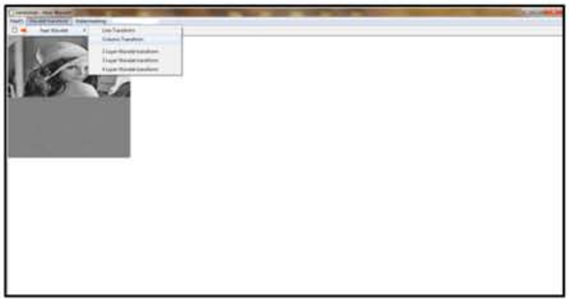


Fig. 15: Column transform

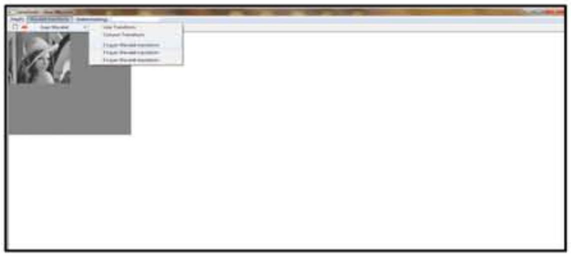


Fig. 16: 2LayerWT

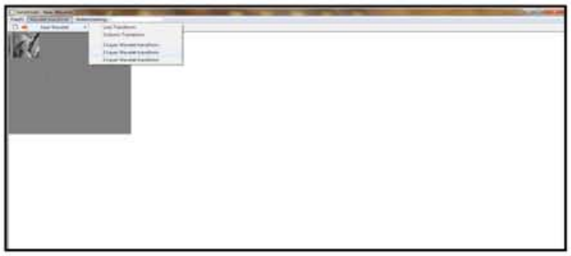


Fig. 17: 3LayerWT

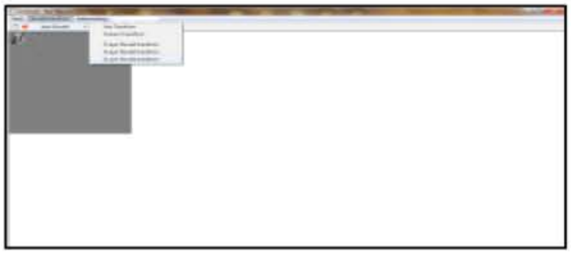


Fig. 18: 4LayerWT

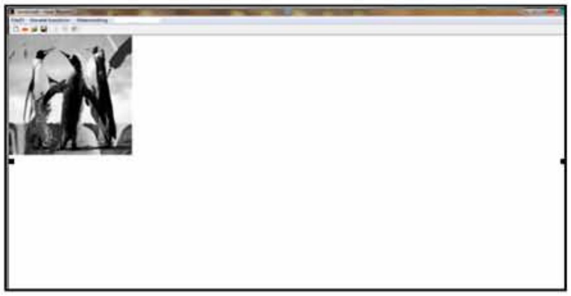


Fig. 19: First watermarking process

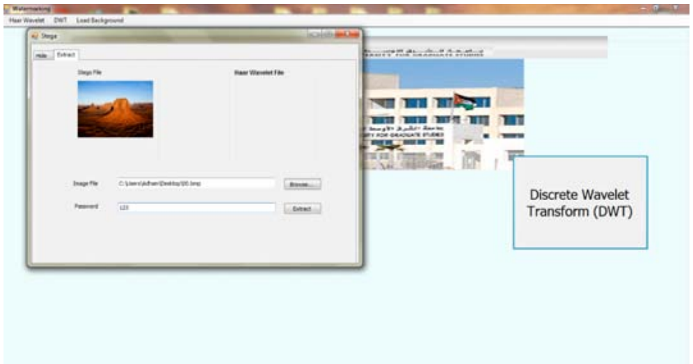


Image File: C:\Users\Adhan\Desktop\00.bmp

Password: 123

Fig. 20: Final result of hide part

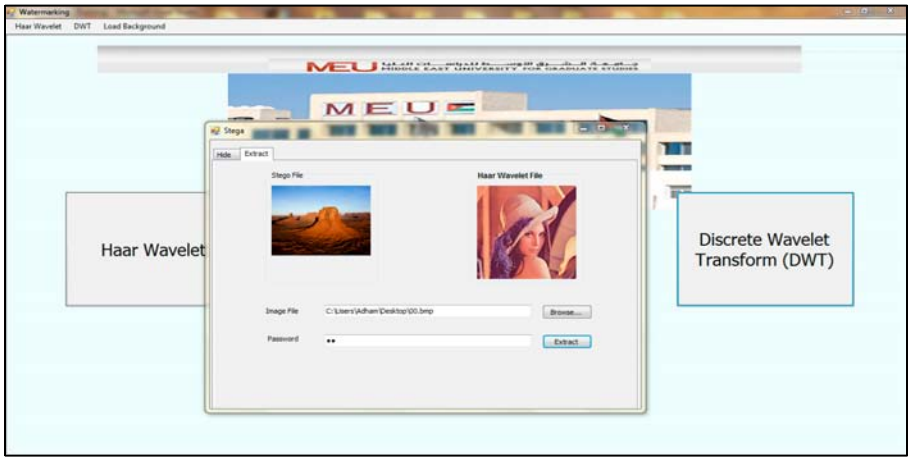


Image File: C:\Users\Adhan\Desktop\00.bmp

Password: ••

Fig. 21: The extracted watermarked image

The hide (embedding) part: This part is to hide/embed an image (or HWT) inside original image. It consists of the following steps:

- Load the original image
- Load HWT image
- Save resulted image
- Add password
- Hide button

Figure 20 shows the result of the hide (embedding) part.

The Extract (recover) part: The task of this part is to extract/recover the images that embedded in the Hide part. It consists of the following steps:

- Load the DWT image
- Put the password
- Extract the watermarked image

Figure 21 shows the extracted watermarked image.

DISCUSSION

The robustness of the generated images based on the proposed system is tested using different types of attacks (Invert, Rotate, Crop and Scale). We create a program calls Image Attack that will be used to attack the watermarking image resulted from the proposed system. Figure 22 shows the general structure for our Image program attacks.

Figure 23-26 show the 4 different types of attacks (Invert, Rotate, Crop and Scale) applied to the watermarking image, respectively.

After attacking the above image, we can extract the original image using the Extract part of the DWT process. Figure 27-30 show and proves that the watermarked image is extracted without any effects of these attacks.

The proposed digital image watermarking algorithm is constructed by cascading two different but complementary techniques: the Discrete Wavelet Transform and Haar Wavelet Transform to provide robustness image to all attacking. The algorithm is proofs

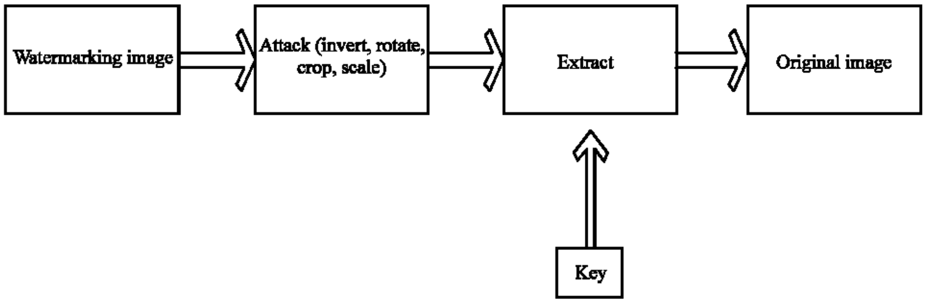


Fig. 22: Image attack structure

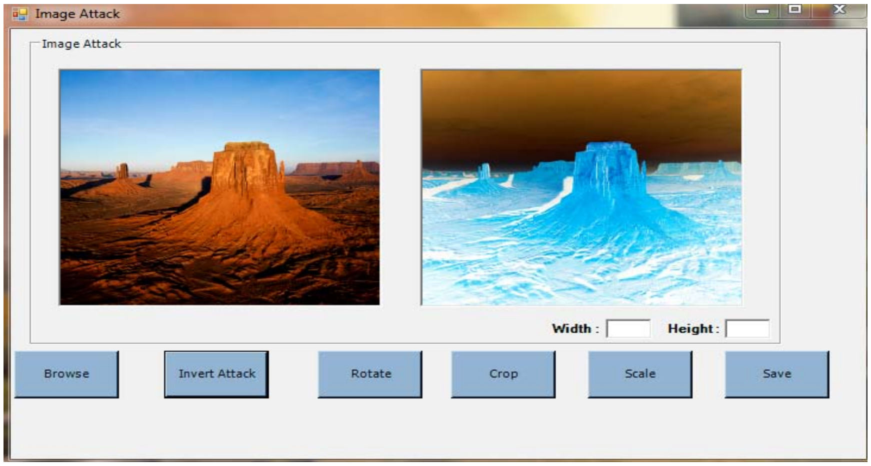


Fig. 23: Invert attack

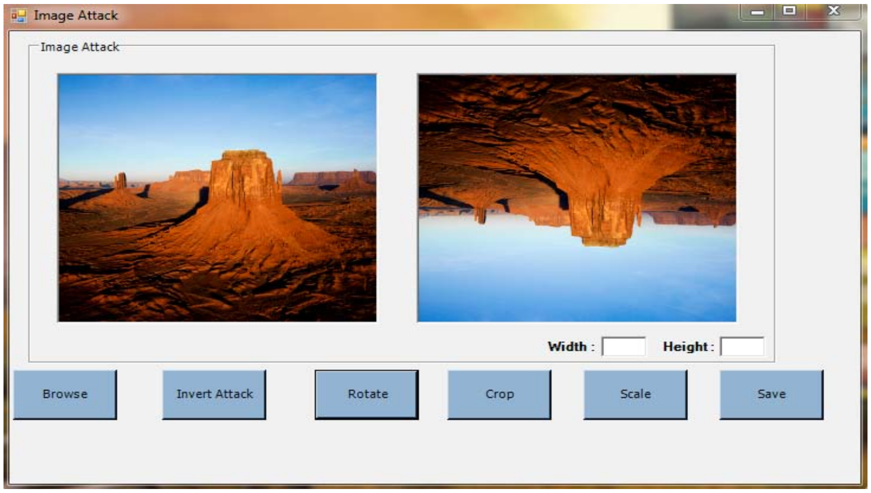


Fig. 24: Rotate attack

resist against numerous image manipulations. Furthermore, the method is easy to implement and suitable for real time applications. Adding a private key to the new technique gives more robustness and security to the watermarked image against attacks.

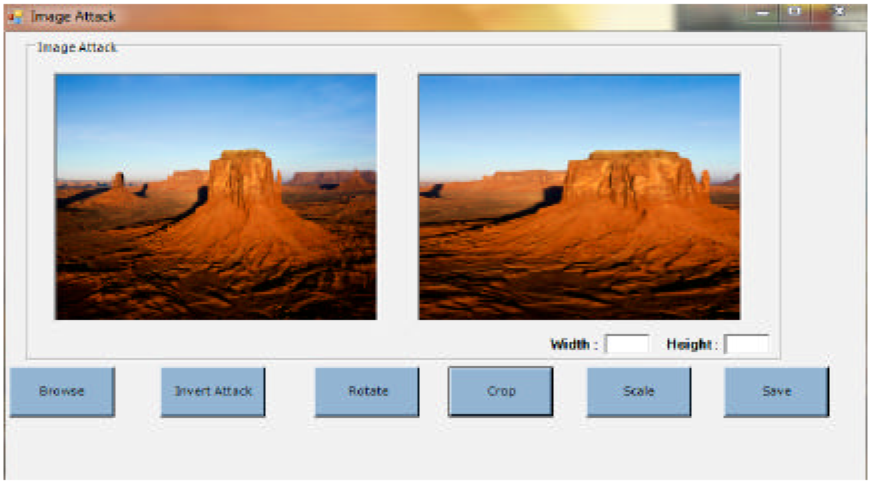
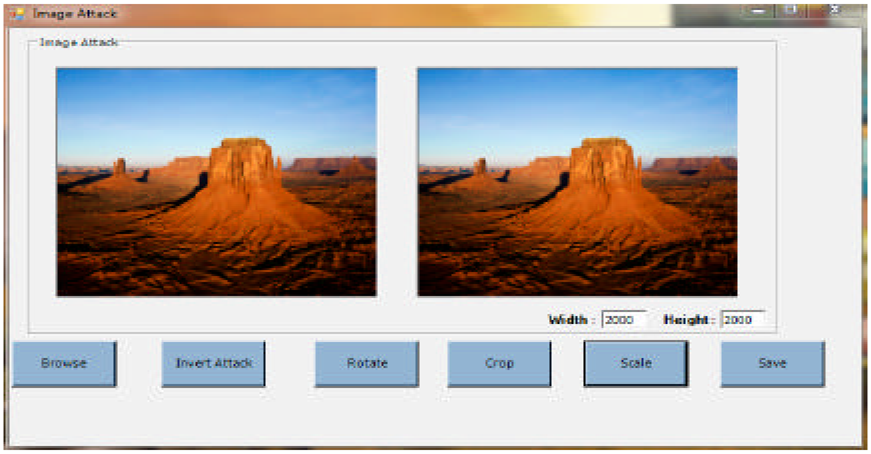


Fig. 25: Crop attack



Width : 2000 Height : 2000

Fig. 26: Scale attack

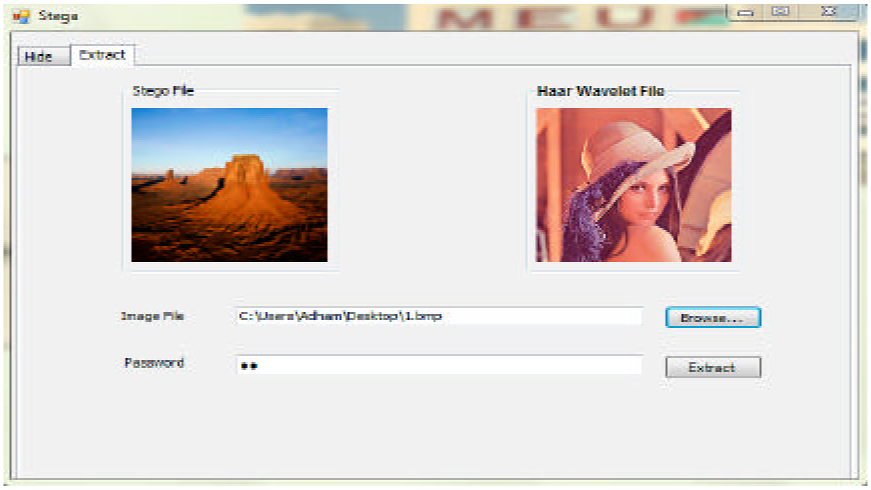


Image File C:\Users\Adham\Desktop\1.bmp

Password ●●

Fig. 27: Extacted watermarked image as a result of the scale attack

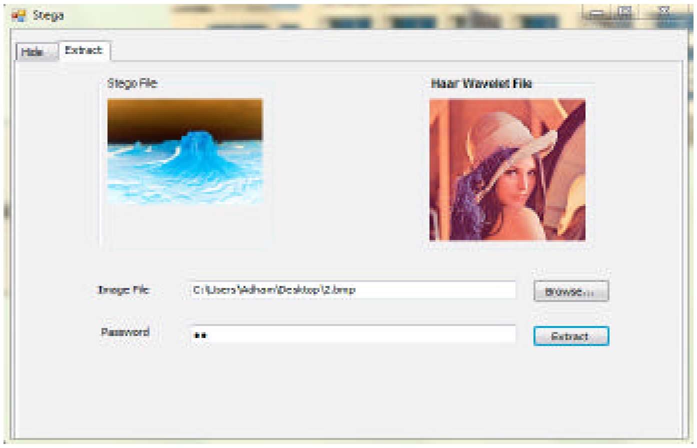


Image File C:\Users\Adham\Desktop\2.bmp

Password ••

Fig. 28: Extacted watermarked image as a result of the invert attack

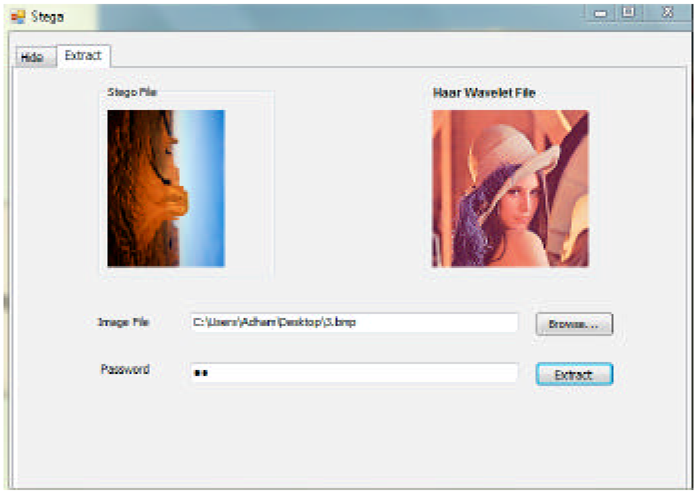


Image File C:\Users\Adham\Desktop\3.bmp

Password ••

Fig. 29: Extacted watermarked image as a result of the rotate attack

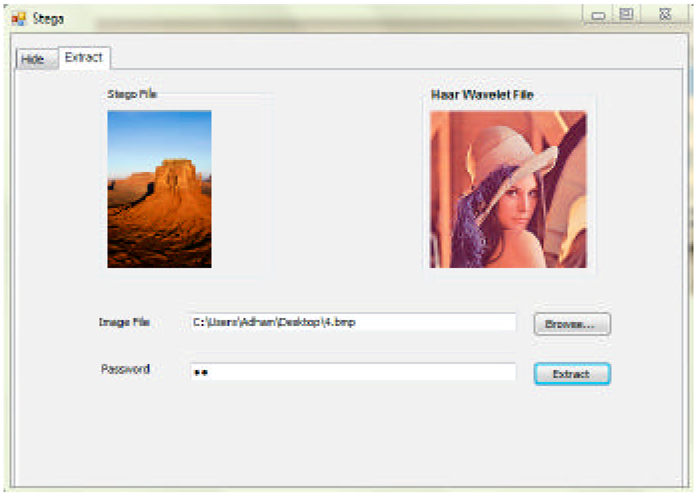


Image File C:\Users\Adham\Desktop\4.bmp

Password ••

Fig. 30: Extacted watermarked image as a result of the crop attack

The robustness of the proposed system has been improved by using two powerful techniques HWT and DWT. The robustness of both techniques alone has been evaluated and tested by many researchers. For the sake of performance and comparison, we also evaluated the watermarking when DWT-only and HWT-only were used. The evaluated result shows better performance using the cascaded HWT and DWT. However, in comparison with other techniques, the wavelet transformation used frequently by many researchers due to its excellent spatial localization and multi resolution characteristics, which is very close to theoretical models of the human visual system.

The based embedding in the second algorithm allows watermark image to be hidden in this image that gives a clear superiority of the algorithm. This technology has been proposed to solve the problem of illegal manipulation and distribution of digital image. Therefore, DWT and HWT technique is used in our proposed system and because it is more robust against transmission and decoding errors, it is computationally efficient and can be implemented by using simple filter convolution.

DWT-HWT are compared with HWT, both methods are the digital watermarking techniques coming from Transform Domain category; therefore, they have some features in common. However, they have some variant characteristics. Performance comparison between DWT-HWT and HWT is summarized in the next paragraphs. Moreover, we used in this comparison the PSNR (Peak Signal-to-Noise Ratio), to show the effects of the attacked images and how it robustness against different types

Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. We evaluated imperceptibility of the cascaded HWT-DWT algorithm by measuring PSNR. The PSNR in decibels (dB) is given below in Eq. 8:

$$\begin{aligned} \text{PSNR} &= 10 \cdot \log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right) \\ &= 20 \cdot \log_{20}\left(\frac{\text{MAX}_I}{\sqrt{\text{MSE}}}\right) \end{aligned} \qquad (8)$$

Here, MAX1 is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear with B bits per sample, MAX1 is 2B-1. It is most easily defined via the Mean Squared Error (MSE) which for two m*n monochrome images I and K where, one of the images is considered a noisy approximation of the other. The MSE is given in Eq. 9:

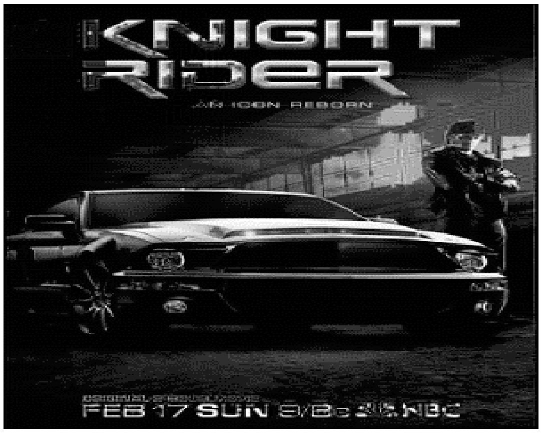


Fig. 31: HWT image without attack. PSNR value = 16.7838 db

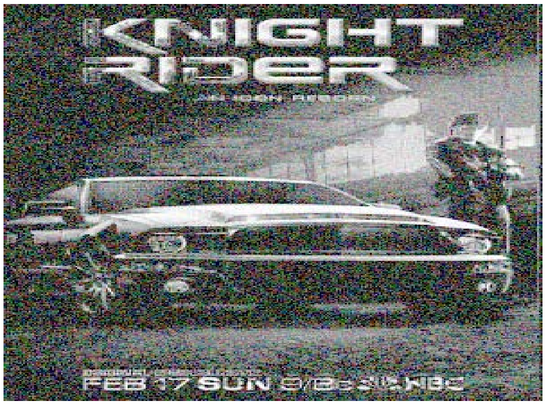


Fig. 32: HWT image after Invert and Noise attack. PSNR value = 12.5846 db

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2 \qquad (9)$$

Figure 31-37 show the effect of different types of attacks on the images that watermarked using HWT-DWT and HWT. The results are generated by using the PORCUPINE software, Version 1.2.2

Therefore, from the above examples we can show that the imperceptibility of the proposed system has been improved by using two powerful techniques HWT and DWT. For the sake of performance and comparison, we also evaluated the watermarking when HWT-only were used. The evaluated results show better performance using the cascaded HWT and DWT.

Furthermore, comparing our proposed method (HWT-DWT) with (DWT-DCT) (Al-Haj, 2007) exploits strength of two common frequency domains method;

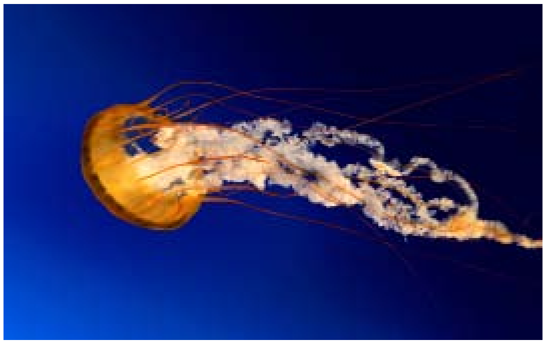


Fig. 33: HWT-DWT image without attack PSNR value = 37.52231 db. PSNR value = 28.3914 db

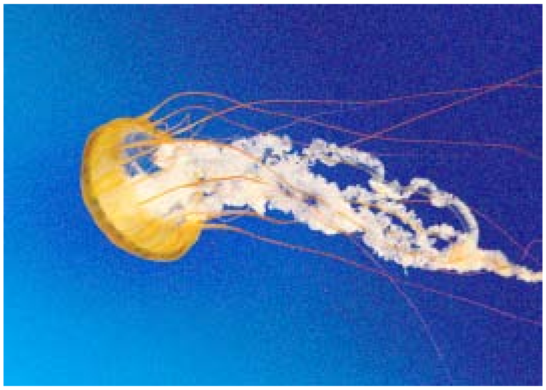


Fig. 34: HWT-DWT images After Invert and Noise attack

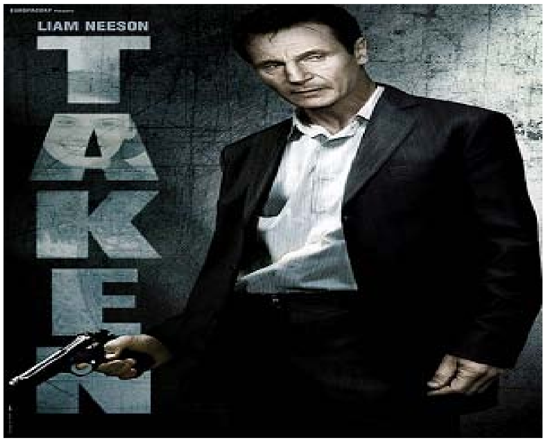


Fig. 35: HWT-DWT image without attack. PSNR value = 49.3914 db

HWT and DWT, to obtain higher efficiency and performance. The quality of each watermarks, which is extracted by exploiting the proposed method, is superior

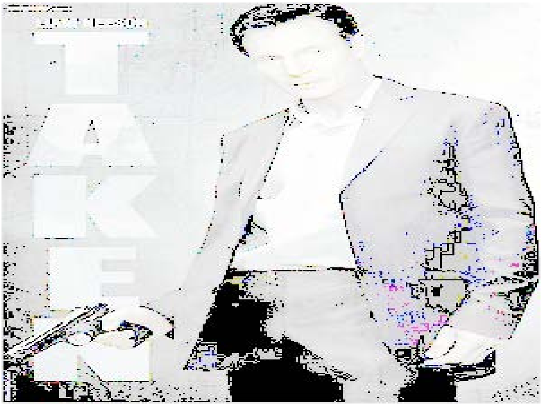


Fig. 36: HWT-DWT images After Invert. PSNR value = 38.5894 db

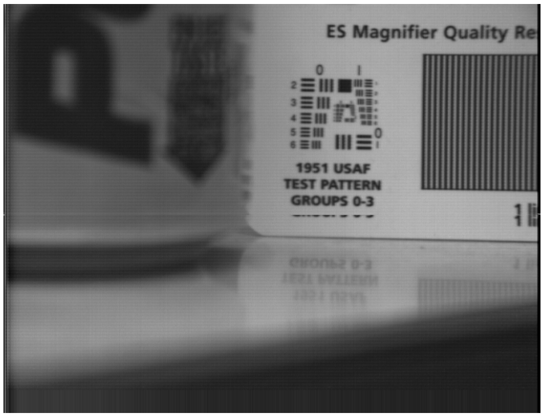


Fig. 37: HWT-DWT image without attack. PSNR value = 50.3914 db

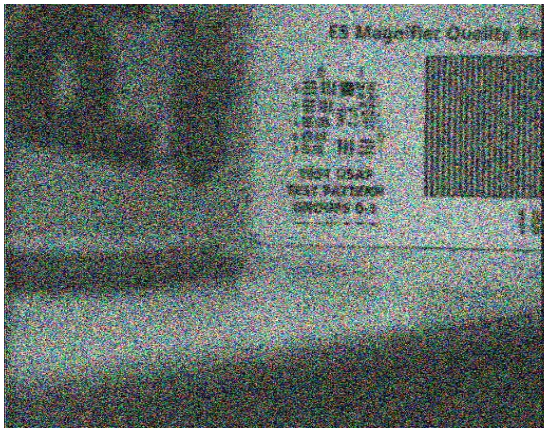


Fig. 38: HWT-DWT images after Noise. PSNR value = 39.2714 db

Table 2: Comparing PSNR of Al-Haj's with the proposed method

	PSNR (db)	
Figure No.	Al-Haj's	Proposed method
Figure 38 HWT-DWT images after noise	37.88	39.2714
Figure 36 HWT-DWT images after invert	37.26	38.5894

to that of why DWT-DCT method. In the following several watermarking attacks, including inverting and noising, are simulated to investigate the robustness of our watermarking method. The experimental results for the cases of attacks related to Fig. 36 and 38 are shown it Table 2.

CONCLUSIONS

It is concluded from this study relating the proposed system that represents a new method (HWT-DWT) constructed by cascading two different but complementary techniques for image protection by using watermarking technique. Such technique is considered one of the powerful and robust schemes in protection process. Wavelet transformation (HWT-DWT) provides robust resistance to the protected image against manipulation and forgery attacks. Adding a private key (password) to the watermarking will increase the privacy and security, but by embedding watermark along with adding the private key (password) more protection in wavelet transform will result, leading to more resistance against attacks. A new technique has been proposed to solve the problem of illegal manipulation and distribution of digital image, i.e., HWT and DWT system. By comparing the response of this system with that of the DWT-DCT, it (HWT-DWT) shows the imperceptibility of our proposed method in illustrating through comparing different types of attacks on the images and the relevant generated values (PSNR).

REFERENCES

Al-Haj, A., 2007. Combined DWT-DCT digital image watermarking. J. Comput. Sci., 3: 740-746.

Amin, M.M., M. Salleh, S. Ibrahim and M. Katmin, 2003. Information hiding using steganography. Proceeding of the 4th National Conference on Telecommunication Technology, Jun 25, Concorde Hotel, Shah Alam, Selangor, pp: 21-25.

Bayram, I. and I.W. Selesnick, 2009. Overcomplete discrete wavelet transforms with rational dilation factors. IEEE Trans. Signal Process., 57: 131-145.

Cabir, V. and K. Serap, 2007. Image Normalization and Discrete Wavelet Transform Based Robust Digital Image Watermarking. Vol. 56. Computer Engineering Sakarya University, Turkey.

Cachin, C., 1998. An information-theoretic model for steganography. Comput. Sci., 1525: 306-318.

Cox, I.J., J. Kilian, T. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process., 6: 1673-1687.

Cox, I.J., M.L. Miller and J.A. Bloom, 2000. Watermarking and their properties. Proceedings of the International Conference on Information Technology: Coding and Computing, (ICITCC'00), Las Vegas, NV, pp: 6-6.

Cox, I.J., M.L. Miller and J.A. Bloom, 2002. Digital Watermarking. Morgan Kaufmann Publishers, San Francisco.

Darmstaedter, V., J.F. Delaigle, J.J. Quisquater and B. Macq, 1998. Low cost spatial watermarking. Comput. Graphics, 22: 417-424.

Das, A., A. Hazra and S. Banerjee, 2010. An efficient architecture for 3-D discrete wavelet transform. IEEE Trans. Circuits Syst. Video Technol., 20: 286-296.

Dittmann, J., 2000. Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete. Springer Publisher, Berlin.

Grans, L., 2003. Multiresolution Watermark Based on Wavelet Transform for Digital Images. University of British Columbia, Canada.

Haldar P., 2008. Watermarks. Parallax, 14: 101-113.

Hanjalic, A., C. Langelaar, G. van Roosmalen, J. Biemond and L. Langendijk, 2000. Image and Video Databases: Restauration, Watermarking and Retrieval. Amsterdam, Elsevier Publisher, The Netherlands.

Hartung, F., J.K. Su and B. Girod, 1999. Spread spectrum watermarking: Malicious attacks and counterattacks. Proceedings of the SPIE Electronic Imaging '99, Jan. 25, Security and Watermarking of Multimedia Contents, San Jose, CA, pp: 147-147.

Houng-Jyh, W., S. Po-Chyi and C.C.J. Kuo, 1998. Wavelet-Based Digital Image Watermarking. University of Southern California, Los Angeles.

Hsu, C.T. and J.L. Wu, 1998. DCT-based watermarking for video. IEEE Trans. Consum. Elect., 44: 206-216.

Inoue, H., A. Miyazaki and T. Katsura, 1999. An image watermarking method based on the wavelet-transform. Proc. ICIP, 3: 296-300.

Karzenbeisser, S. and F. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 1580530354, pp: 240.

Kunder, D. and D. Hatzinkos, 2001. A Robust Digital Image Watermarking Method using Wavelet-Based Fusion. University of Toronto, Canada.

Kutter, M. and F. Hartung, 2000. Introduction to Watermarking Techniques. In: Information Hidingtechniques for Steganography and Digital Watermarking, Katzenbeisser, S. and F.A.P. Petitcolas (Eds.). Artech House, Boston.

Lepik, U., 2007. Application of the Haar wavelet transform to solving integral and differential equations. Inst. Applied Mathematics Univ. Tartu, Proc. Estonian Acad. Sci. Phys., 56: 28-46.

Leung, Y., M. Cheng and L. Cheng, 2009. A robust watermarking scheme using selective curvelet coefficients. Dep. Electronic Eng. City Univ. Hong Kong, 7: 163-181.

Lin, T. and J. Delp, 1999. A review of data hiding in digital images. Image Capture Syst. Conf., PICS, 52: 274-278.

Murtag, F., 2007. The haar wavelet transform of a dendrogram. J. Classification, 24: 3-32.

Paquet, A., 2001. Multiresolution Watermark Based on Wavelet Transform for Digital Images. Project Report, University of British Columbia, Canada.

Radomir, S. and J.F. Bogdan, 2003. The Haar Wavelet Transform: Its Status and Achievements. Nanyang Technological University, School of Electrical and Electronic Engineering, Singapore.

Robi, P., 2004. The Wavelet Tutorial. Rowan University, College of Engineering, New Jersey.

Stephan, J., 2005. Image Watermarking Using Wavelet Transform. University System Cyril and Methodius, Faculty of Electrical Engineering, Germany.

Tsai, M.J., 2009. A visible watermarking algorithm based on the content and contrast aware (COCOA) technique. J. Vis. Commun. Image R., 20: 323-338.

Wolfgang, B., C.I. Podilchuk and E.J. Delp, 1999. Perceptual watermarks for images and video. Proc. IEEE., 87: 1108-1126.

Wu, N.I., C.M. Wang, C.S. Tsai and M.S. Hwang, 2008. A Certificate-Based Watermarking Scheme for Colored Images. Vol. 6. Institute of Computer Science and Engineering, National Chung Hsing University, Taiwan.

Yeung, M., B. Teo and M. Holliman, 1998. Digital watermarks: Shedding ligith on the invisible. Intel Corporation, 18: 32-41.