

# Copyright Protection by Robust Digital Image Watermarking in Unsecured Communication Channels

Layth Alasafi<sup>\*1</sup>, Tuna Göksu<sup>2</sup>, Ammar Albayati<sup>3</sup>

<sup>1,2</sup>Süleyman Demirel University, ECE Department, Süleyman Demirel, Turkey

<sup>3</sup>Çankaya University, CENG Department, Ankara, Turkey

\*Corresponding author, e-mail: e-mail: laythtalat@gmail.com, ammar.jameel.ict@gmail.com

## Abstract

The transition from analog technologies to digital technologies has increased the ever-growing concern for protection and authentication of digital content and data. Owners of digital content of any type are seeking and exploring new technologies for the protection of copyrighted multimedia content. Multimedia protection has become an issue in recent years, and to deal with this issue, researchers are continuously searching for and exploring new effective and efficient technologies. This thesis study has been prepared in order to increase the invisibility and durability of invisible watermarking by using the multilayer Discrete Wavelet Transform (DWT) in the frequency plane and embedding two marks into an image for the purpose of authentication and copyright when digital content travels through an unsecured channel. A novel watermarking algorithm has been proposed based on five active positions and on using two marks. In addition to the extraction process, watermarking images will be subjected to a set of attack tests. The evaluation criteria have been the bases of assessing the value of SNR, PNSR, MAE and RMSE for both the watermarking images and the watermarking images after attacks, followed by the invisibility of the watermarking being measured before and after the attacks. Our lab results show high robustness and high quality images obtaining value for both SNR and PNSR.

**Keywords:** Discrete Wavelet Transform, invisible watermarking, copyright protection, digital image watermarking

Copyright © 2017 Institute of Advanced Engineering and Science. All rights reserved.

## 1. Introduction

In our modern lives, reliance on information and communications technology (ICT) is growing steadily and this increasing need for the use of information technologies can influence our lives in either positive or negative ways in many aspects. Therefore, the transmission of digital media through unsecured media, such as the Internet, or private networks, such as Local Area Networks (LAN), Personal Area Networks (PAN) and Wide Area Networks (WAN), is not a simple mission. Proving the ownership of transmitted digital multimedia introduces the requirement of having a robust watermarking scheme in order to improve copyright protection and the rights of ownership (Gitanjali Verma, 2015). There have been number of techniques proposed and introduced by various scholars, but the most prominent and famous technique is watermarking. Watermarking embeds data directly into multimedia content and this process generally involves a key that determines the location of the watermark. There are several schemes and methods of watermarking explored by researchers in order to deal with this issue (Tao & Eskicioğlu, 2015). These involve the following main characteristics: Perceptual transparency; Durability; High capacity; and Robustness. Perceptual transparency can be defined as the perceptual similarity between original data and marked data. When a mark or logo is added so as to meet this requirement, the quality of the original data will not be influenced (Tao & Eskicioğlu, 2015). Durability is the term used to indicate the level to which the authenticity of a mark can be determined after the marked data have passed through certain mark processing applications. A durable marking method depends on the application given. For example, while the durability of an image against transmitting from a channel is required for a publication control application, it is not required for a reproduction inhibition application (K. Magai, 2005). Capacity is defined as the amount of information which can be stored in the original data. Capacity depends on an application for durability. For example, a mark of one bit

is generally sufficient for the inhibition of reproduction. However, capacity is required to be approximately 60-70 bits for other applications, such as a fingerprint. In many studies in the literature, it has been demonstrated that frequency space watermarking methods are more successful than other methods. For this reason, only frequency space methods will be studied in this thesis. Watermarking in a frequency space is done by changing the proper transformation coefficients (R. Sugihara et al, 2001). Subsequently, the inverse transformation is applied to the marked image. As marks are applied, the frequency space will expand to the entire image in the pixel space. After the inverse transformation is applied, it is more durable than the marks applied in the pixel space. DFT, DCT, DWT and CWT are the commonly used frequency spaces. There exist fast algorithms in order for the Discrete Wavelet Transform (DWT) to be carried out. In addition, the DWT has the feature of good energy compression. Because of these two features, the DWT has been used to solve many image-processing problems. In brief, wavelet transformation divides an image into multiple parts at special frequencies (Sathik & Sujatha, 2012).

### 1.1. Digital Watermarking

The development in digital multimedia technologies in the past decades has been considerable due to faster and easier use of these technologies on the Internet. Greater growth and successful techniques in multimedia technologies have brought significant changes while creating a number of issues for users with regard to securing their content. The threats to using multimedia technology include copyright protection, the general security of multimedia and verification of multimedia content. However, copyright protection is one of the most important problems that pose a threat to multimedia content (Barni, M., 2001). Digital watermarking is one of the techniques that are being utilized by operators in order to secure their data and avoid copyright issues. Watermarking is a technique such that a secret code or signal is embedded into the data so as to protect it from copyright and authentication infringements (Langelaar and Gerhard C., 2000). The code is embedded in a manner such that it does not affect the quality of the content while making the content secure. Digital watermarks are composed of copyright or authentication digital code embedded into the data. This code remains unseen in the digital content until the content passes through a particular detector to detect the code (Zhang, W. et al., 2004).

### 1.2. Watermarking Requirements in Still Images

A number of watermarking techniques or applications exist based on the nature and security level of the digital content. Each watermarking technique or application has its own requirements that are based on which the design is developed. Every watermarking technique and application cannot be studied; nevertheless, the diversity cannot be ignored. There are, however, a number of requirements which must be fulfilled by the watermarking technique (Pu, Y., et al., 2004). These are as follows:

- a. **Robustness:** A watermarking algorithm process should be robust against different types of attacks, i.e. the mark inside a cover image should not be able to be removed easily. Alternatively, the loss of the mark should be obtainable only at the expense of distortion of the cover images.
- b. **Fragile watermarking:** The watermarking algorithm process should consider a fragile hidden data inside the cover image such that a mark or logo or any hidden data do not efface any of the cover image properties. This can help such that when modification is applied to the cover image, a part of the mark or logo will be lost thereby improving the robustness of the watermarking algorithm.
- c. **Imperceptibility:** A watermark embedding is actually imperceptible, i.e. humans cannot distinguish the original data from the data with the injected watermark. Alternatively, a watermarking algorithm process is required to embed a mark that does not affect the visualization of cover images.
- d. **Capacity:** Capacity is the amount of data that image can carrier to included, higher ability of available capacity increased strength of the algorithm; however, this should not lead to a loss of quality or a loss of robustness of these algorithms.

### 1.3. Classification of Watermarking Techniques

A watermarking technique is the procedure that embeds data or an image (called a mark or logo) into a digital object such as a multimedia file. This mark or logo can be later extracted or detected by reversing the same watermarking technique used in the embedding process. The host image is used to carry out this mark or logo called cover image or original images. A watermarking technique is merely a process used to put a mark or logo inside a cover image in order to protect the copyright ownership of the image.

One of the most important requirements that have watermarking techniques considered robust is that either a mark or logo cannot be detected or extracted by attackers easily or the mark or logo inside a cover image is affected less by external attacks. Watermarking techniques are classified according to the different methods used to process modulated or modulated nature of this embedded process, such as the working domain, the type of mark or logo and cover image used; Moreover, they can be classified according human perception and according to any applications used (T.H.N. Le, et al., 2010). In addition, Imperceptible watermarking, or invisible watermarking, includes every type of watermarking technique such that a mark or logo cannot be sensed visually. Without using special software, the mark or logo cannot be extracted, such as watermarking by using DCT and DWT techniques. In addition, invisible watermarking can be either robust or fragile. Robust watermarking means the embedded mark or logo makes alterations to the pixel bits and it cannot be observed. Moreover, the extraction process should be done using proper decoding machinery only (Petit Colas, F, 1999). Fragile watermarking means a mark or logo is embedded in the cover image in a technique such that any modification or any attacker operation occurring on the host/cover image causes the mark or logo to be destroyed (J.Y. Stein, 1995). While visible watermarking techniques include every type of technique where a mark or logo is visible to the eye, this technique is widely used in media channels nowadays, such as media channel logos (Swanson, M.D, 1998). Some new studies have suggested that by using both visible and invisible watermarks, the invisible watermarking will be used as backup for the visible watermarking (Amit Kumar, 2015).

Other watermarking techniques can also be classified depending on the working domain:

- a. Spatial domain techniques, where watermark techniques are used to embed a mark or logo into the cover image by changing the pixels' characteristics inside the image itself, such as changed bits in the pixels or changing the weight of a number of these pixels (T.H.N. Le et al., 2010). Many techniques were used in this aspect, such as the Least Significant Bits (LSB) techniques and SSM modulation based techniques. This type is one of the most powerful techniques used to hide a mark; however, it may adversely affect the general visualization of the image.
- b. Frequency domain techniques are used to insert the mark or logo into the spectral coefficients of the cover image. Many techniques have been used in these groups; however, the most used techniques have been the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD). Moreover, there are some new techniques that are based on combining two or more of these techniques, such as DCT and DWT, or DWT and SVD (T.H.N. Le, 2010). Linking spatial domain techniques and frequency domain techniques are applied more nowadays since they use the spectral coefficients of the cover image instance of changing the pixel bit. This makes it difficult to detect any embedded mark or logo with the naked eye without the use of special tools for detecting or extracting the mark or logo (Linlin Tang and Yu Tian, 2015).

In addition, some studies classify the watermarking according to the detection process (T.H.N. Le et al., 2010), such as the following:

- a. Blind watermarking: In this type of watermarking technique, the detection process does not need original data to extract the mark or logo. It has a wide application field, but requires a higher watermark technology and cost over time and money.
- b. Non blind watermarking: In this type of watermarking technique, the detection process needs both an original image and the mark or logo to complete the detection process.
- c. Semi-blind watermarking: In this type of watermarking technique, the detection process needs either an original image or a mark or logo to complete the detection process.

## 2. Watermarking Techniques and Unsecured Communication Problem

Watermarking technologies are usually used on a digital object when the owner wants to send this object through an unsecured communication channel (Mohammed ALSULTAN., Et al. 2017) and (I.J. Cox et al., 2001). In order to understand the nature of the transfer of this, we need to understand the mechanism of this carrier and its relationship to the concept of watermark technologies. Figure 1 shows traditional data communications when a message travels through it.

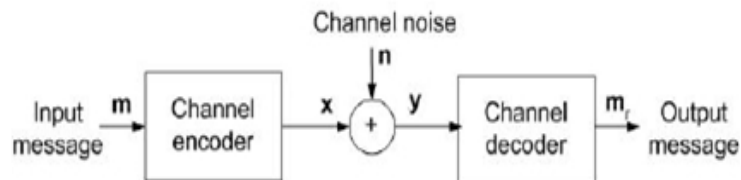


Figure 1. Message traveling through traditional data communications

The figure above shows message ( $m$ ) when travelling through an unsecured communication channel. After the channel encoder, we get signal ( $x$ ). There may be a set of noise ( $n$ ) or attaches that are applied to the message ( $m$ ), so the signal( $x$ ) transforms to become signal ( $y$ ) (i.e. ( $x$ ) signal plus noise ( $n$ )). On the other side of the communications channel, there is a receiver or decoder that attempts to decode the ( $y$ ) signal and acquire the original message ( $m$ ). The essential procedure in each watermarking technique can be modeled as a form of a communication signal in which a message is transferred from the embedder to the receiver/decoder [Cox J.; Miller, M.L., 1999].

This problem affects the quality of the watermark, which may lead to loss of the watermark completely, and consequently, the loss of intellectual property rights. There are also many forms of attack that may affect a message as it travels in unsafe intermedia, and these risks are constantly evolving. It is important to improve robust watermark algorithms to save over the watermark that travels in an unsecured channel. The next section will provide more information and discussion about perspective attacks.

**Attacks Classifications:** There are many types of attacks possible that impact on images transmitted in unsafe intermedia. These attacks can be classified as follows (Voloshynovskiy, S. et al., 2001)

- a. Malicious attacks: These attacks normally aim to remove or make the watermark in cover images unrecoverable by manipulating information of the particular algorithm. Examples include rescanning, re-printing and re-watermarking.
- b. Non-malicious attacks: Any kind of attack can be considered as if they are not non-malicious attacks if they do not target the basic host image or watermark information while the attacker is attempting to manipulate the other properties of the image to influence the watermark. Examples include compression attacks and Common Signal Processing Operations such as A/D conversion, D/A conversion, re-quantization and re-sampling.
- c. Removal attacks: This kind of attack is exactly as the malicious attacks. An attacker here attempts to remove the watermarking completely without manipulating the information of any particular algorithm. Examples include de-noising, quantization, collusion attacks and re-modulation.
- d. Geometric attacks: This type of attack does not attempt to remove the embedded watermark itself; it attempts to distort the watermark extraction process so that it becomes difficult to extract the watermark after this type of attack. Examples include the transform invariant domain, local shifts and affine modifications.
- e. Cryptographic attacks: This type of attack attempts to crack the security approaches in watermarking algorithms and embed malicious information or remove the watermarking. Examples include brute force search for information.
- f. Protocol attacks: This kind of attack attempts to whole concept of the watermarking algorithms. Examples include inevitability attacks, where the attacker attempts to take ownership of watermark image itself.

### 3. Associated Previous Works

Previous studies are divided into three main sections: investigations studies, combine algorithms studies, and multi-level DWT studies, which are discussed in the following sub sections.

#### 3.1. Investigations Studies

According to Saini (2015), copyright protection and authentication have become issues due to the growth of Internet systems. In order to protect digital content from copyright issues, digital watermarking has been utilized for a long time. The author has analyzed various techniques of watermarking for web content and evaluated the HTML and XML techniques in order to assess their advantages and disadvantages.

New and robust techniques for watermarking must be introduced and implemented. These will be based on syntactic and semantic rules. These techniques will secure the watermark with a strong cryptographic method along with the use of SALT. In addition, it will also make the watermark invisible. The role of the CA is to determine the authorized author of any digital content as the original author is registered in the CA, and in the case of unauthorized access or attack, the CA will determine the author of the content. However, this technique can be applied to any web language, such as HTML and XML and other similar services.

Panchal and Srivastava (2015) have stated that image watermarking has become popular in the recent years due to the increased use of the Internet and multimedia through the Web. In addition, image watermarking is about adding information to a host image in the form of a logo or text. Image watermarking is mainly aimed at protecting copyright, authenticating content, maintaining the integrity of data and identifying the ownership of images. However, watermarking not only aims at protecting copyright, it equally focuses on authentication and identification of the owner.

The authors have pointed out that watermarking requires robustness, capacity, high imperceptibility and security in order to be efficient. Watermarking techniques that are built using spatial domains are simpler and can embed greater number of bits and have a lower level of complexity. On the other hand, watermarking techniques that are built under a frequency transform domain are resistant to attacks and cannot be embedded in a large number of bits due to the decreased level of quality. For this reason, the authors suggest that these techniques ought to be used with spatial domain techniques at high capacity.

#### 3.2. Combined Algorithms Studies

Jane and Elbaşı (2013) have demonstrated that the literature in the field has emphasized the embedding techniques that are commonly being used for copyright protection and security. The Discrete Wavelet Transform is commonly used in most watermarking techniques due to the separation of the frequency components. Furthermore, the Singular Value Decomposition (SVD) and Lower and Upper (LU) decomposition are also prominent in the field of watermarking. Therefore, the authors have proposed a new combination of the DWT and SVD via the LU decomposition for the watermark algorithm that requires the cover work to detect a watermark. The results show that this algorithm is robust and reliable against attacks. Moreover, the algorithm prevents attacks by embedding a binary watermark on the low-low band.

According to Malakooti et al (2013), the search for a digital image from a vast quantity of images is quite difficult when it is based on image content rather than metadata. Moreover, search results of most methods are satisfactory; however, there are a number of images other than the target image. The authors have proposed a new method for image recognition based on the Wavelet Transform and Singular Value Decomposition (SVD) that can retrieve most of the images that are similar to the target image. In this method, the DWT has been used to transfer images from the spatial domain to the frequency domain in which the image is divided into four sub-bands. Three levels of 2D DWT have been applied to concentrate the image components into a third level sub band. The SVD is then applied in order to extract its singular values.

Kaur and Jindal (2014) have proposed a robust digital image watermarking technique which is based on the DWT and SVD using the median filter function. In this method, the original image is passed through the median filter function in order to make the image smooth, after which a first level DWT is applied. The high frequency band is used in embedding and

modifying the singular value of the watermark and the original image. Although there are a number of other techniques that can be used for watermarking, this method can ensure the robustness of watermarking against attacks as compared to other techniques.

According to Gunjal and Mali (2014), secured, robust and high embedding capacity along with invisible digital image watermarking techniques are the most important requirements for copyright protection. To achieve these objectives, the authors have presented a non-blind digital image watermarking technique. The authors have analyzed the performance of this technique using the DWT, DWT Fast Walse-Hadamard Transform and the Singular Value Decomposition domains. After the implementation of this technique, the authors argue that the DWT-FWHT-SVD domain can achieve the objective of perceptual quality which is better in comparison to the DWT domain. Consequently, the results of the DWT-FWHT-SVD domain reveal that this architecture can achieve robustness against various attacks in comparison to other DWT and DWT-SVD based techniques.

### 3.3. Multi-Level DWT Studies

Sharma and Jain (2014) have argued that copyright protection through watermarking has to be tested and checked for robustness and imperceptibility after a certain period of time to resolve the issue of copyright in actuality. Robustness and imperceptibility are the main objectives of any DWT watermarking technique and these objectives must be achieved to ensure security of digital media. The authors have proposed the technique of using a hybrid transform which involves the process of transforming the cover image and modifying it in singular values rather than DWT sub-bands. This way, the watermark makes itself susceptible to different types of attacks. In addition, the results of this study demonstrate that the technique of hybrid transformation can improve imperceptibility and robustness in order to avoid attacks. The protection of data has been a constant issue of concern for researchers.

Tao and Eskioğlu (2015) have generalized the idea of embedding a binary pattern in the form of a binary image in the LL and HH bands at the second level of the DWT decomposition. They have included all four bands and compared the embedding of the watermark at the first and second level decomposition. The proposed algorithm is robust against a number of attacks due to embedding the watermark in lower frequencies. Embedding the watermark in higher frequencies protects the digital content from another set of attacks. However, the experiment of the authors demonstrates that the first level decomposition is more advantageous because the area for the watermark embedding is maximized and extracted watermarks are textures and have better visual quality.

Ammar Jameel Hussein et al (2015) produced a novel algorithm by using a 4-level DWT algorithm based on a dynamic binary cover image location selected and. They embedded two watermark logos using different DWT levels and proposed these algorithms for authenticity and copyright protection. In the proposed watermarking algorithm, they applied a 5-level DWT to the cover image to obtain the fifth low frequency sub band (LL5) binary value, and an examination of the dynamic binary location value of selected location for embedding purposes in five different locations in the host image using the same algorithm process. The experimental results demonstrate that this algorithm scheme is imperceptible and robust against several image processing attacks. The watermarked image quality is evaluated by calculation of the PSNR and SNR.

## 4. Proposed Algorithm and Evaluation

In this section, we will discuss the watermarking algorithm that has been proposed based on five positions in the cover image by using two marking images as the watermarking. The first log is suggested to be embedded in two locations (LL2 and LL4), while the second watermark is embedded in three locations (LL1, LL3, and LL5).

**4.1. Embedding Process:** If we assume that we have an image  $IM(i,j)$  (512x512 in size) considered to be our cover image, and we assume that we have a watermark image  $W1(i,j)$  (512x512 in size) being the primary watermark image and  $W2(i,j)$  (512x512 in size) considered to be the second watermark image, and we assume that we obtain the image  $LW1(i,j)$  (512x512 in size) as a result of watermarking processor, this will be the first watermarked image, and  $LW2(i,j)$  (512x512 in size) will be the second watermarked image. Consequently, the summation

of them gives us the watermarked image  $LW(i,j)$  as our watermarked images by using the following mathematic equations:

$$LW1(i,j)=IM(i,j)+W1(i,j) \quad (1)$$

$$LW2(i,j)=IM(i,j)+W2(i,j) \quad (2)$$

$$LW(i,j)=(LW1(i,j)+LW2(i,j))/2 \quad (3)$$

**4.2. Extraction Process:** If we assume that we have an image  $IM(i,j)$  (512×512 in size) considered to be our cover images, and we assume that we have a watermarking image  $LW(i,j)$ , then performing a subtraction between cover image and the watermarking image sub-bands will give us the first watermark image  $LW1$  and second watermark image  $LW2$ , by using the following mathematical equations:

$$LW1=IM(i,j)-LW(i,j) \quad (4)$$

$$LW2=IM(i,j)-LW(i,j) \quad (5)$$

Figure 2 shows the overall work process of the proposed algorithms, including the embedding process, extraction process, application of the set of attacks, and the evaluation process.

**4.3. Laboratory Experiments:** Our laboratory carried out by using MATLAB code, and our proposed algorithms shown in figure 13 performed using one piece of program code to ensure the quality and efficiency of the implementations. We tested our proposed algorithms using different gray-scale images of size 512×512 of the standard image processing test images, such as Lena, Muhammad Ali, Girl face, Zelda, Sailing boat, Lighthouse, Cameraman, Gold hill, Barbara, etc. In addition, we used different gray scale images of size 512×512 as the watermark logo. Table 1 shows the five test images along with the watermarked images after the embedding process. While Table 2 shows or log used:

Table 1. Test Images Along with Watermarked Image after Embedded Process










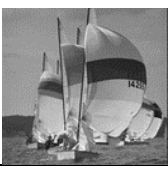



Image Name	Cover Image	Watermarked
Lena		
Girl face		
Muhammad Ali		
Zelda		
Sailing boat		

Table 2. Watermark Logo Used in Our Lab

Logo Number	Logo Images
1	
2	
3	



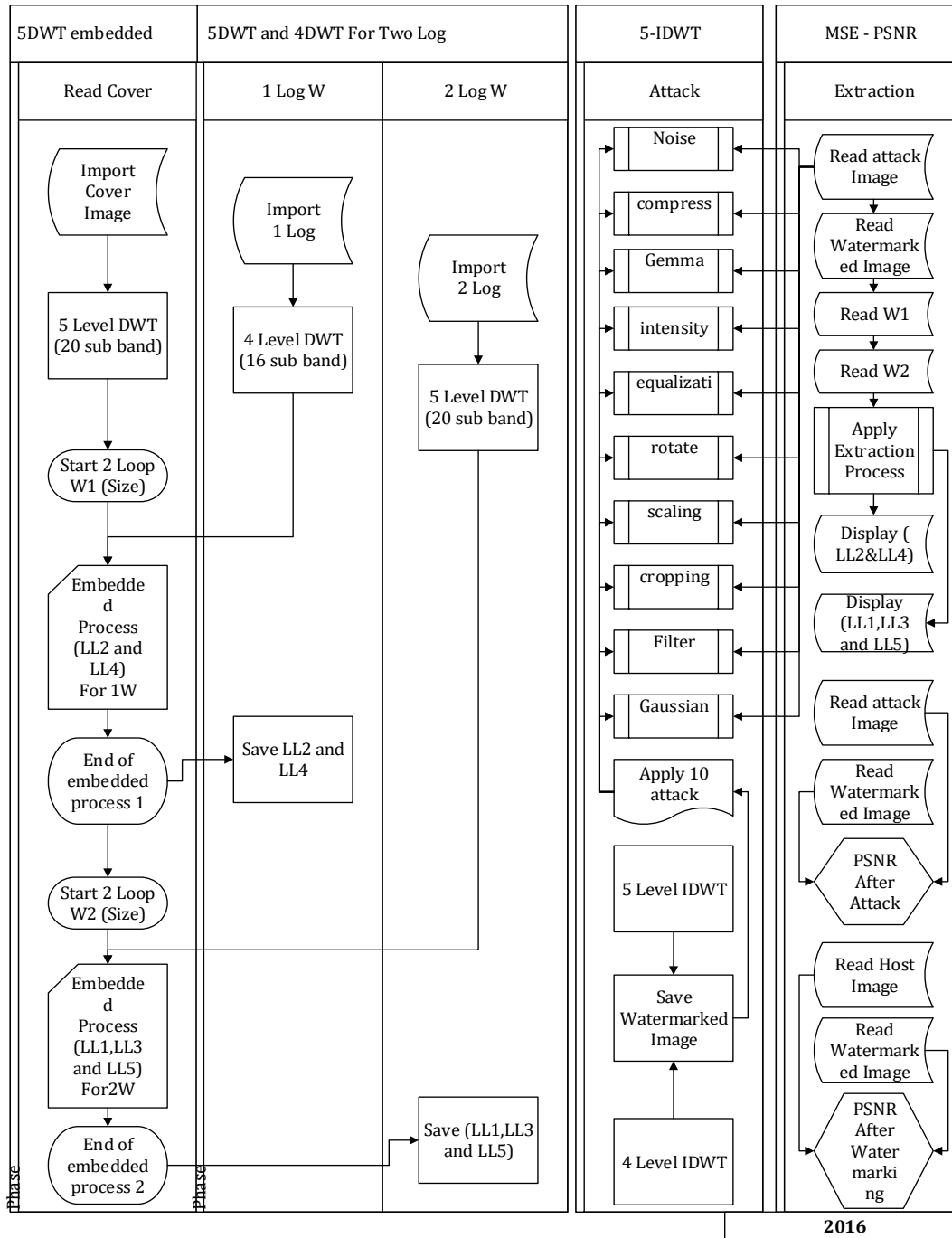


Figure 2. Overall proposed algorithm

**5. Attacks Test**

In order to test our proposed algorithm’s robustness in our lab, we applied different types of attacks to the watermarked image using the MATLAB platform. The attacks included the following: a resizing attack, rotation attack, compression attack, equalization attack, contrast adjustment attack, Gamma attack, Gaussian attack, cropping, noise attack, low pass filtering attack, and a gamma attack. Table 3 shows the attack parameters used in our lab along with the watermark image after the attacks where the Lana image was used as a test image, while Table.4 shows the attack parameters used in our lab along with the watermark image after the attacks where the Girl face image was used as the test image.

Table 3. Watermark Image after Attacks (Lana)























No.	Name	Parameters	Result Image
1.	Watermarked Image	2 Logo	
2.	Gaussian noise	Mean=0 Variance=0.001	
3.	Low Pass Filtering	Window Size=3x3	
4.	Cropping	On both sides	
5.	Scaling	512x256	
6.	Rotation	20°	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8] [b=0 t=1]	
9.	Gamma	1.5	
10.	JPEG Compression	Q=75	
11.	Noise	0.02	

Table 4. Watermark Image after Attacks (Girl Face)

No.	Name	Parameters	Result Image
1.	Watermarked Image		
2.	Gaussian noise	Mean=0 Variance=0.001	
3.	Low Pass Filtering	(Window Size=3x3)	
4.	Cropping	On both sides	
5.	Scaling	512x256	
6.	Rotation	20°	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8] [b=0 t=1]	
9.	Gamma	1.5	
10.	Compression	Q=75	
11.	Noise	(0.02)	

## 6. Evaluation Process

In our lab, we evaluated the proposed watermark algorithms by measuring the PSNR, SNR, MAE and RMSE. J's plugin (2016) was used for the evaluation process. This program calculates the PSNR, SNR, MAE and RMSE of the tested images being contingent with the definitions produced by Gonzalez and Woods (2008). The plugin compared a reference image  $IM(i,j)$  with a target test image  $T(i,j)$ . The two images should have the same size of  $[ni,nj]$ . The PSNR, SNR, MAE and RMSE are calculated with the given equations:

1. Peak signal-to-noise ratio (PSNR)

$$PSNR = 10 \cdot \log_{10} \left[ \frac{\text{Max}(IM(i,j))^2}{\frac{1}{Ni \cdot Nj} \cdot \sum_0^{Ni-1} \sum_0^{Nj-1} [IM(i,j) - T(i,j)]^2} \right]$$

2. Signal-to-noise ratio (SNR)

$$SNR = 10 \cdot \log_{10} \left[ \frac{\sum_0^{Ni-1} \sum_0^{Nj-1} [IM(i,j)]^2}{\sum_0^{Ni-1} \sum_0^{Nj-1} [IM(i,j) - T(i,j)]^2} \right]$$

3. Mean absolute error (MAE)

$$MAE = \frac{1}{Ni \cdot Nj} \cdot \sum_0^{Ni-1} \sum_0^{Nj-1} [IM(i,j) - T(i,j)]$$

4. Root mean square error (RMSE)

$$RMSE = \sqrt{\frac{1}{Ni \cdot Nj} \cdot \sum_0^{Ni-1} \sum_0^{Nj-1} [IM(i,j) - T(i,j)]^2}$$

In our lab, we tested many standard image process test images. Afterwards, we applied our proposed algorithms and a set of attacks. Every test process was applied two times: first, we took the cover image as a reference image; then, we took the watermark image as a reference image. The PSNR, SNR, MAE and RMSE obtained the values shown in Tables 5(a) and (b), Tables 6 (a) and (b), and Tables 7 (a) and (b).

Table 5(a). Lena Cover Image Used As a Reference Image

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	47.83	52.78	0.59	0.34
Gaussia.png	25.23	30.17	7.90	6.27
Filter.png	24.07	29.01	9.03	5.51
crop.png	5.14	10.09	79.84	35.41
Resize.png	24.09	29.03	9.01	5.67
Rotate.png	3.35	8.30	98.07	76.24
Equal.png	29.40	34.34	4.89	4.16
Intensit.png	13.84	18.79	29.31	25.30
Gamma.png	14.41	19.36	27.46	24.87
Hostr75.jpg	29.67	34.62	4.74	3.57
Noise.png	16.80	21.75	20.85	2.87

Table 5(b). Lena watermarked image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	22.04	28.48	7.80	6.14
Filter.png	24.87	31.31	5.63	2.86
crop.png	4.83	11.27	56.55	26.96
Resize.png	25.50	31.94	5.24	2.86
Rotate.png	3.41	9.85	66.62	47.25
Equal.png	5.84	12.28	50.35	43.82
Intensit.png	12.02	18.46	24.71	21.05
Gamma.png	10.07	16.51	30.94	28.32
Hostr75.jpg	30.33	36.77	3.00	2.06
Noise.png	13.74	20.18	20.28	2.52

Table 6(a). Girl Face Cover Image Used As a Reference Image

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	44.48	50.95	0.59	0.34
Gaussia.png	21.97	28.44	7.83	6.16
Filter.png	24.86	31.33	5.62	2.94
crop.png	4.86	11.33	56.18	26.92
Resize.png	25.40	31.87	5.28	2.97
Rotate.png	5.75	12.22	50.69	44.16
Equal.png	11.87	18.34	25.05	21.40
Intensit.png	10.14	16.61	30.59	27.98
Gamma.png	30.13	36.60	3.06	2.14
Hostr75.jpg	13.70	20.17	20.29	2.86
Noise.png	44.48	50.95	0.59	0.34

Table 6(b). Girl Face Watermarked Image Used As a Reference Image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	22.04	28.48	7.80	6.14
Filter.png	24.87	31.31	5.63	2.86
crop.png	4.83	11.27	56.55	26.96
Resize.png	25.50	31.94	5.24	2.86
Rotate.png	3.41	9.85	66.62	47.25
Equal.png	5.84	12.28	50.35	43.82
Intensit.png	12.02	18.46	24.71	21.05
Gamma.png	10.07	16.51	30.94	28.32
Hostr75.jpg	30.33	36.77	3.00	2.06
Noise.png	13.74	20.18	20.28	2.52

Table 7(a). Muhammad Ali Cover Image Used As a Reference Image


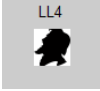



















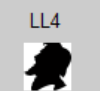








Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	49.38	52.76	0.59	0.34
Gaussia.png	26.59	29.97	8.09	6.45
Filter.png	25.20	28.58	9.49	4.02
crop.png	5.57	8.95	91.00	43.35
Resize.png	25.81	29.19	8.85	4.17
Rotate.png	5.56	8.94	91.11	62.27
Equal.png	11.71	15.09	44.87	39.24
Intensit.png	13.03	16.41	38.55	36.26
Gamma.png	16.42	19.79	26.11	24.97
Hostr75.jpg	46.99	50.37	0.77	0.49

Table 7(b). Muhammad Ali Watermarked Image Used As a Reference Image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	26.63	29.99	8.07	6.43
Filter.png	25.20	28.56	9.52	3.94
crop.png	5.55	8.92	91.35	43.39
Resize.png	25.85	29.21	8.83	4.07
Rotate.png	5.56	8.92	91.29	62.36
Equal.png	11.67	15.03	45.20	39.52
Intensit.png	13.12	16.48	38.24	35.91
Gamma.png	16.32	19.68	26.45	25.31
Hostr75.jpg	50.41	53.77	0.52	0.24
Noise.png	18.47	21.83	20.65	2.57

Extraction after Attack: In our lab, we also tested our proposed algorithms by visually evaluating the watermark logo before and after an attack using the MATLAB platform. Table.8 demonstrates the extraction of the watermark logo before and after an attack (for the original watermarked image, Gaussian, filter, Gamma, Cropping and Equalization) using the Muhammad Ali watermarked image, and Logos number 3 and 4 in Table 3.

Table 8. Extraction of the Watermark Logo Before and After Attack

Test Image	First Watermark Logo	Second Watermark Logo
Extraction from watermarked image	 	  
Gaussian (mean=0, variance=0.001)	 	  
Filter (0.02)	 	  
Gamma -1.5	 	  
Cropped both sides	 	  
Equalization	 	  

## 7. Conclusion

Throughout this research, we discussed the importance of digital watermarking, watermarking requirements in still images and the most important applications area of watermarking techniques. In addition, we discussed the classifications of watermarking techniques and the relationships between watermarking techniques and the unsecured communication problem along with watermarking techniques attacks classifications. Additionally, we went through the related work and discussed the previous studies made by many researchers relating to our topic and we classified them into three groups, namely investigations studies, combined algorithms studies and multi-level DWT studies.

In addition, we proposed algorithms based on five positions in a cover image by using two marked images as the watermarking. The first log suggested that it be embedded in two locations (LL2 and LL4), while the second watermark be embedded in three locations (LL1, LL3 and LL5). We also discussed the implementation of the extraction process wherein the watermarked images were subjected to a set of attack tests. The evaluation criteria were based on assessing the values of SNR, PNSR, MAE and RMSE for the watermarked images before the attacks and the watermarking images after the attacks. Our results show that high quality images obtained by the application of our algorithms were represented by higher values obtained in SNR and PNSR competing with previous studies made by Ammar Jameel et al (2015). Moreover, our proposed algorithms show high robustness against different types of attacks, such as Compression, Gaussian, Filter, Gamma, Cropping, Resize, Noise Equalization, and Rotate attacks. These attacks had very little effect on our watermark logo embedded in the attacked images. We can therefore conclude that our proposed algorithm can contribute effectively to protecting intellectual property rights and improving the ownership of digital objects when traveling through unsecured intermedia. The following are some recommendations for future work:

- a. Increasing the amount of information that can be embedded in a host image through the suggestion of new watermark techniques;
- b. Maintaining more transparency that does not affect the visibility of host images when embedding more information;
- c. Proposing new watermark techniques that give better value in terms of image quality by obtaining higher values of SNR and PNSR;
- d. Increasing the robustness of algorithms by inserting additional elements to the current ones, such as image scramble techniques;
- e. Suggestion for new combinations of algorithms, such as 5 level DWT and DCT or 5 Level DWT and SVD; and
- f. Suggest a new dynamic location within a host image for embedding more information.

## Acknowledgment

The authors L. A. and A. J. thank the Iraqi Board of Supreme Audit Iraq/Baghdad and Iraqi Ministry of Electricity, which contributed effectively to give us this opportunity for publication.

## References

- [1] Amit Kumar Singh. Robust and Imperceptible Dual Watermarking for Telemedicine Applications. *Wireless Personal Communications*. 2015; 80(4): 1415-1433.
- [2] Ammar Jameel, Seda Yüksel, Ersin Elbaşı. Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT" (Improved). *Journal of Theoretical and Applied Information Technology* 20th, 2015; 78(2).
- [3] Barni M, Bartolini F, Cox IJ, Hernandez J, Perez-Gonzalez F. Digital Watermarking for Copyright Protection: A Communications Perspective. *IEEE Communications Magazine*. August 2001; 39(8): 90-133.
- [4] Cox IJ; Miller ML; McKellips AL. *Watermarking as Communications with side Information*. Proceedings of the IEEE. July 1999; 87(7): 1127-1141.
- [5] Cox IJ, Kilian J, Leighton T & Shamoon T. Secure Spread Spectrum Watermarking for Multimedia. *IEEE transactions on image processing*. 1997; 6(12): 1673-1687.
- [6] Gitanjali Verma., "Comparative Study of Imperceptible digital Watermarking Techniques. *Journal of Current Computer Science and Technology*. 2015; 5(6).

- [7] Gunjal BL & Mali SN. Comparative Performance Analysis of Digital Image Watermarking Scheme in DWT and DWT-FWHT-SVD domains. *Annual IEEE India Conference*. 2014.
- [8] Hu Y & Jong CC. (), A memory efficient High-Throughput Architecture for Lifting-Based Multi-Level 2D DWT, *IEEE Transactions on Signal Processing*. 2013; 61(20): 4975-4987.
- [9] Image plugin to assess the quality of images, Written by Daniel Sage at the Biomedical Image Group, EPFL, Switzerland. Available at: <http://bigwww.epfl.ch/>
- [10] J Cox, ML Miller, JA Bloom. *Digital Watermarking*. Morgan Kaufmann, 2001.
- [11] JY Stein, *Digital Signal Processing: a Computer Science Perspective*. New York: Wiley. 2000.
- [12] K Magai, H Ito, H Mishima, M Suzuki, K Asai. *Watermarking Robust Against Analog VCR Recording*. Image Processing, 2004. ICIP '04. 2004 International Conference on 2004; 5
- [13] Linlin Tang, Yu Tian, Jengshyang Pan, 2015. Applications of Cloud Model in Digital Watermarking. *Chapter Intelligent Data Analysis and Applications volume 370 Series Advances in Intelligent Systems and Computing*. 2015; 370: 371-379.
- [14] Malakooti MV, Panah ZF & Hashemi SM. Image Recognition Method based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD), SDIWC. 2013: 42-47.
- [15] Mohammed Alsultan, Thaer Alramli, Ammar Albayati, Ersin Elbasi. Hough Transform Based Watermark Embedding Algorithm in dct Frequency Domain. *Journal of Theoretical & Applied Information Technology*. 2017; 95(8).
- [16] Panchal UH & Srivastava R. A Comprehensive Survey on Digital Image Watermarking techniques. *Fifth International Conference on Communication Systems and Network Technologies*. 2015: 591-595.
- [17] Petitcolas F, Anderson R, Kuhn M. *Information Hiding—a Survey*. Proc. of the IEEE. July 1999; 87(7): 1062-1078.
- [18] Podar VM, Han S & Chang E. *A Survey of Digital Image Watermarking Techniques*. 3rd IEEE International Conference on Industrial Informatics. 2005: 709-716.
- [19] Pu Y, et al. *A Public Adaptive Watermark Algorithm for Color Images Based on Principal Component Analysis of Generalized Hebb*. Proc. of IEEE Int. Conference on Information Acquisition. 2004: 690-695.
- [20] R Sugihara et al. *Practical Capacity of Digital Watermark as Constrained by Reliability*. Information Technology: Coding and Computing, 2001. Proceedings. International IEEE Conference. 2001: 85-89.
- [21] RC Gonzalez, RE Woods. *Digital Image Processing*. 3rd ed., Prentice Hall, 2008.
- [22] Saini S. *A Survey on Watermarking Web Contents for Protecting Copyright*. IEEE Sponsored 2nd International conference on Innovations in Information Embedded and Communication Systems. 2015
- [23] Sathik MM & Sujatha SS. A Novel DWT Based Invisible Watermarking Technique for Digital Images. *International Arab Journal of e-Technology*. 2012; 02(03): 167-173.
- [24] Sharma P & Jain T. Robust Digital Watermarking for Colored Images Using SVD and DWT Techniques. *IEEE*. 2014: 1024-1027.
- [25] Swanson MD, Kobayashi M, Tewfik AH. *Multimedia Data-Embedding and Watermarking Technologies*. Proc. of the IEEE. June 1998; 86(6): 1064-1087.
- [26] THN Le, KH Nguyen; HB Le. *Literature Survey on Image Watermarking Tools, Watermark Attacks and Benchmarking Tools*. Advances in Multimedia (MMEDIA), 2010, Second International Conferences. 2010: 67-73.
- [27] Tao P & Eskicioğlu AM. A robust multiple watermark scheme in the Discrete Wavelet Transform Domain. 2015.
- [28] Voloshynovskiy S. et al., Attacks on Digital Watermarks: Classification, Estimation Based Attacks, and Benchmarks. *IEEE Communication Magazine*. August 2001; 39(8): 118-126.
- [29] Zhang W, Zhu W, Fu Y. *An Adaptive Digital Watermarking Approach*. Proc. of IEEE Int. Conference on Mechatronics and Automation, Chengdu, China. August 2004: pp. 690-695.
- [30] Zhang F & Zhang H. Image Digital Watermarking Capacity and Reliability Analysis in Wavelet Domain. *IEEE 47th International Midwest*. 2004: 101-104.