T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

COPYRIGHT PROTECTION BY ROBUST DIGITAL IMAGE WATERMARKING IN UNSECURED COMMUNICATION CHANNELS

Layth Alasafi

Danışman
Assist. Prof. Dr. Tuna GÖKSU

YÜKSEK LİSANS TEZİ
ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ ANABİLİM DALI
ISPARTA - 2016

© 2016 [Layth Alasafi]

TAAHHÜTNAME

Bu tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin referans gösterilerek tezde yer aldığını beyan ederim.

Layth Alasafi

CONTENTS

ÖZET

Yüksek Lisans Tezi

Güvensiz Haberleşme Ortamlarında Telif Hakkı Koruma Amaçlı

Dayanıklı İmge Damgalama

Layth Alasafi

Süleyman Demirel Üniversitesi

Fen Bilimleri Enstitüsü

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. TUNA GÖKSU

Analog teknolojilerden dijital teknolojilere geçiş dijital içerik ve verilerin korunması ve özdeşliğe duyulan sürekli ilgiyi artırmıştır. Her türlü dijital içerik sahipleri, telif haklı multimedya içeriğinin korunması için yeni teknolojiler aramakta ve keşfetmektedir. Multimedya koruması son yıllarda gündeme gelmiş ve bu konuyla ilgilenmek için araştırmacılar, sürekli olarak yeni, verimli ve etkin teknolojiler araştırmakta ve keşfetmektedirler. Bu tez çalışması, dijital içerik güvenli olmayan bir kanalda yol alırken özdeşlik ve telif hakkı koruma amacıyla, frekans düzlemindeki çok katmanlı ayrık dalgacık dönüşümü (DWT) kullanılarak, iki damgayı bir imgeye gömerek, görünmez damgalamanın görünmezliğini ve dayanıklılığını artırmak için hazırlanmıştır. Özgün bir damgalama algoritması, beş etken konum ve iki damganın kullanımı üzerine dayandırılarak önerilmiştir. Özütleme sürecine ilave olarak, damgalama imgeleri bir dizi atak testine tabi tutulmuştur. Değerlendirme kriterinin temeli, damgalama imgeleri için ataklardan önce ve sonra ölçülen SNR, PNSR, MAE ve RMSE değerleridir. Yine damgalamanın görünmezliği atak öncesi ve sonrası test edilmiştir. SNR ve PNSR değerlerinden elde eden edilen laboratuvar sonuçlarımız, imgelerin yüksek dayanıklılıkta olduğunu ve damgalamanın imge kalitesine olumsuz etkisinin olmadığını göstermiştir.

Anahtar Kelimeler: Ayrık dalgacık dönüşümü (DWT), Görünmez damgalama, telif hakkı koruması, dijital imge damgalama

2016, 63 Sayfa

ABSTRACT

M.Sc. Thesis

COPYRIGHT PROTECTION BY ROBUST DIGITAL IMAGE WATERMARKING IN UNSECURED COMMUNICATION CHANNELS

Layth Alasafi

Süleyman Demirel University

Graduate School of Applied and Natural Sciences

Department of Electronics and Communications Engineering

Supervisor: Assist. Prof. Dr. Tuna GÖKSU

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 (DWT), Invisible watermarking, Copyright protection, Digital image watermarking

2016, 63 pages

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to assist. Prof. Dr. Tuna GÖKSU for his supervision, special guidance, suggestions, and encouragement through the development of this thesis.

I dedicate this work to the spirit of my father and my mother, and I pleasure to express my special thanks to my wife (Shahd Alattar) for their valuable support and also to my children (Hassan , Nabaa , Hiba) .

LIST OF FIGURES

Page

LIST OF TABLES

Page

LIST OF ABBREVIATIONS

BER	Bit Error Rate
CDF	Cohen-Daubechies-Favreau
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DFT	Discrete Fourier Transform
FPGA	Field-Programmable Gate Array
HTML	Hyper Text Markup Language
ICT	Information and Communications Technology
LSB	Least Significant Bits
LAN	Local Area Network
LU	Lower and Upper
PAN	Personal Area Network
SVD	Singular Value Decomposition
WAN	Wide Area Network
XML	Extensible Markup Language

CHAPTER 1

INTRODUCTION

1.1 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:

1. Perceptual transparency;
2. Durability;
3. High capacity; and
4. 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. As the coefficients are at a high frequency, areas will disappear after the various sign processing methods are applied and changes to the coefficients at lower frequency areas will be perceived easily, marking the sign generally added in coefficients at medium frequency areas (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).

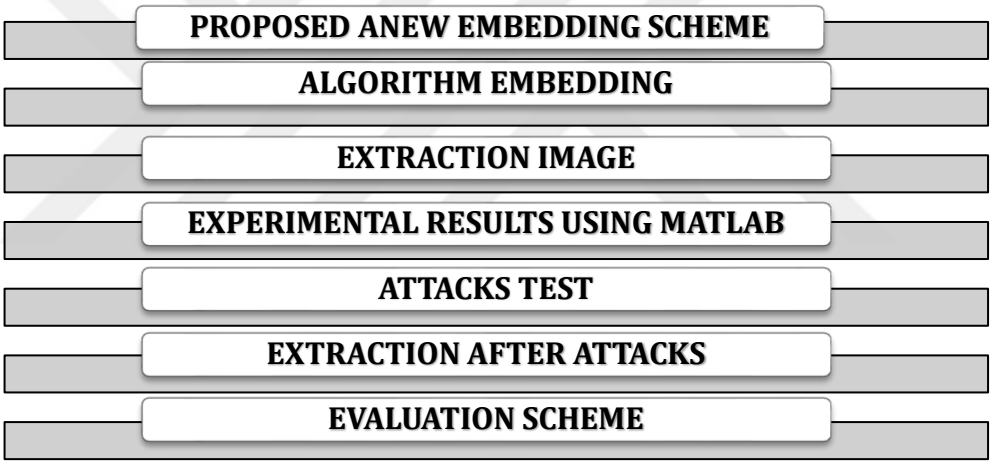
1.2 Contribution of the Thesis

Many media organizations and other organizations scattered around the world require a means to transmit their own digital content through any type of communication channel, including through PAN, LAN and WAN networks. To achieve this, they continuously need to develop complicated mechanics and algorithms to ensure the ownership of their media. Watermark technology is

one of the most important of these techniques being used to prove intellectual property rights. In order to accomplish a novel softness and robustness-watermarking algorithm, we proposed the use of a 5-level DWT algorithm based on a fixed cover image location; we drive into it two marks/logos at different DWT levels. The proposed algorithm will help to keep the images traveling through unsecured environments to be transmitted more securely than classical methods. In addition, it improves copyright protection and authenticity.

1.3 Aim and Scope

Our Study will focus on using a multilayer Discrete Wavelet Transform (DWT) in the frequency domain and embedding two marks or logos into the cover image for the purpose of authentication and copyright. Our study plan will cover the following:



1.4 Thesis Structure

Our research is divided into five chapters, the first three of which are dedicated to a discussion of the theoretical literature related to the research, while the last two chapters discuss the practical applications of the proposed algorithm and their results. This thesis is structured as follows:

Chapter 1 includes the thesis introduction, the aim of the study and its subject and scope.

Chapter 2 includes the most important theoretical aspects on the subject of the research, which meets with the theories used in this field.

Chapter 3 includes a literature review and the approaches that have been used in previous research related to our subject. In addition, the research challenges and any possible benefits of our proposed algorithm will be presented.

Chapter 4 is a discussion of the proposed algorithm processes, modulated process and extraction process in addition to a discussion of the test results and operations.

Chapter 5 presents some recommendations along with our conclusions.

CHAPTER 2

BACKGROUND

2.1 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). Figure 2.1 shows the general watermarking system.

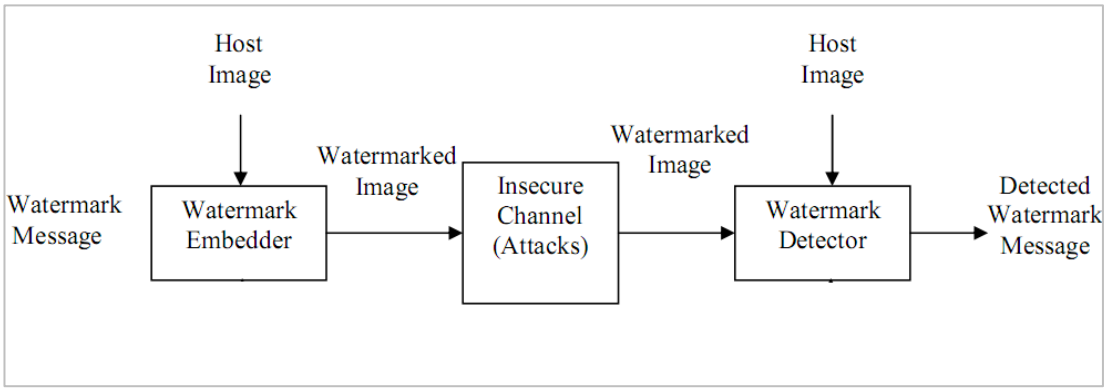


Figure 2.1 General watermarking system

2.2 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:

- *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.
- *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.
- *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.
- *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.

Figure 2.2 shows the relation between quality, capacity and robustness in the watermark still image requirement.

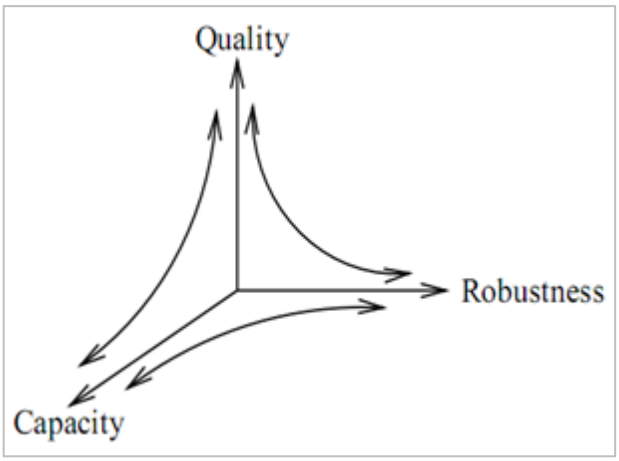


Figure 2.2 The relation between quality, capacity and robustness

2.3 Watermarking Applications

Watermarking is aimed at copyright protection; however, there are a number of other applications that make the watermarking an unrestricted phenomenon. The watermarking area of application is not limited; rather, there are a number of areas where watermarking techniques or schemes can be applied. These include (Linlin Tang and Yu Tian, 2015):

- Copyright protection used to improve intellectual property rights;
- Broadcast monitoring used in commercials and advertisements;
- Authentication used in improved ownership issues;
- Fingerprinting used in tracing the source of illegal reproductions;
- Covert communication used for purposes of transmission of secure information between two parties; and
- Date hiding of information behind other objects for non-secure applications.

Watermarking can be used for:

- Medical safety used in medical applications, such as embedding patient information within medical images; and
- Indexing used in indexing in many areas, such as the indexing of movies and news items or any multimedia object.

2.4 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). Figure 2.3 shows watermarking technique classifications according to information hiding and Figure 2.4 shows watermarking technique classifications.

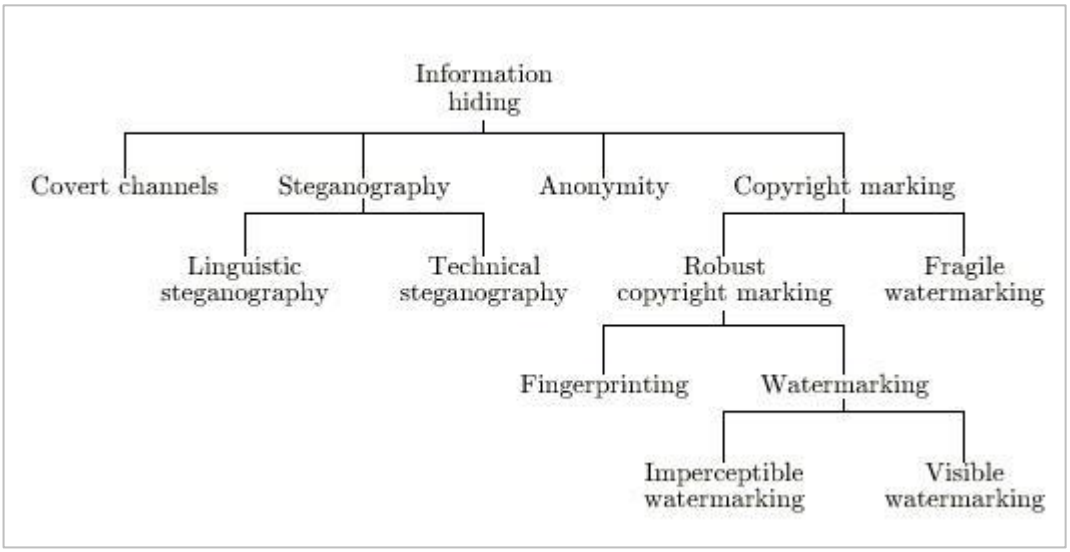


Figure 2.3 Watermarking techniques classifications in information hiding.

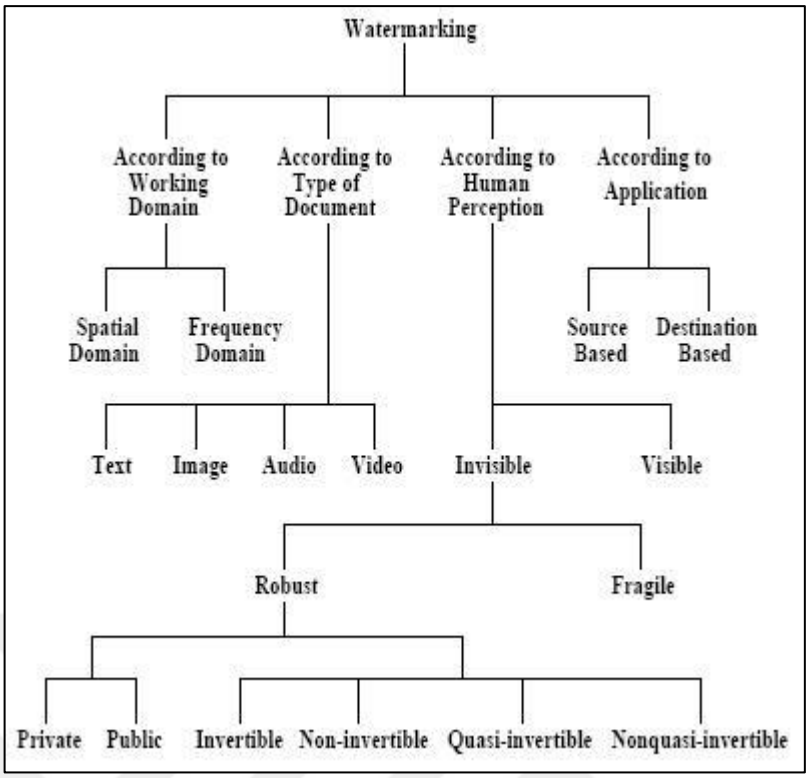


Figure 2.4 Watermarking techniques classifications

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 watermarkings, the invisible watermarking will be used as backup for the visible watermarking (Amit Kumar, 2015).

Figure 2.5 shows visible watermarking techniques, while Figure 2.6 shows invisible watermarking techniques.

Figure 2.5 Visible watermarking

Figure 2.6 Invisible watermarking techniques

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

1- 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.
2- 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).

Table 2.1 shows the main differences between the DFT, DCT and DWT algorithms.

Moreover, watermarking techniques can also be classified depending on the type of object being used for embedding, i.e. the host object type, such as the following:

1- Text watermarking
2- Video watermarking
3- Audio watermarking
4- Image watermarking

Algorithms	Pros	Cons
DFT	DFT is replacement or rotation, translation and scaling invariant. Hence, it can be cast off to recover from geometric distortions	A difficult operation and cost of computing may be complex.
DCT	The mark is embedded into the coefficients of the middle frequency, so the visibility of the image will not be exaggerated and the mark will be difficult to remove by any kind of attack.	Block intelligent DCT destroys the invariance properties of the system. Convinced higher frequency components tend to be repressed throughout the quantization stage.
DWT	Localization both in interval and spatial frequency domains. Advanced compression ratio which is applicable to human perception.	Cost per computing may be higher. Time-consuming; compression time may be higher. Blur/Noise near edges of images or video frames.

Table 2.1 The main differences between DFT, DCT and DWT algorithms

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

1- 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.

2- 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.
3- 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.

The theoretical framework of this research is based on the theory of DWT/Frequency Domain Techniques and the previous theories about predictive transforms and sub band coding. This framework covers the theories presented by Mallat, Clarke and K.R. Rao as well as the mathematical proofs given from various theories by A. Cohen et al.

2.5 Predictive, Transform and Sub Band Coding

Predictive coding refers to the process where data elements pre-existing the current data elements are used to ascertain the current elements. The pre-existing elements may differ along the spatial horizontal, vertical or temporal directions. The magnitudes of the differential signals will be calculated by

Actual values – values of the predictions

They will then be encoded and transmitted (R.J. Clarke, 1985). The procedure is known as *Signal Transformation*, which refers to a procedure where a signal is mapped from one domain (e.g. the original pixel on another domain such as a frequency domain) (K.R. Rao and J.J. Hwang, 1996). Such a transformation from one domain to another will make the signal far more stationary in every frequency band used; therefore, the signal will be far easier to code. (N. Ahmed, T. Natarajan et al., 1974; I. Daubechies, 1990; M. Vetterli and C. Herley, 1992; R.J. Clarke, 1995). The traditional frequency transform will be used for two things in this regard, as given below (R.J. Clarke, 1985):

1. Energy packing
2. De-correlation

When the transformation procedure is completed, the coefficient energy is distributed across a number of varying sub bands. The sub band which is the average version of the signal before its transformation is called the low

frequency sub band. This is also called the DC sub band in various studies; however, this is only a difference of nomenclature.

This will contain a far more focused energy that will surpass the energy contained in its counterpart's, i.e. the high frequency sub bands which are also called AC sub bands in various studies.

However the AC sub bands will have a higher level of variance or detailed information. The transformation procedure will also destroy the interrelation of the pixels, and will do so along multiple directions. When only still images are being used, the procedure will change them spatially along the Y-axis and the X-axis. If the procedure is being applied to video signals, it may change them both spatially and temporally. Although this research does not discuss audio signals, it is worth mentioning that the transformation of audio signals is carried out along temporal lines.

2.6 Discrete Wavelet Transform (DWT)

Wavelets are special functions that have been created from the original function denoted by ψ. The DWT is usually generated from the primary function by using various translation procedures and dilations. If an examination of the continuous form of the wavelets is required, it can be done through the following equation:

$$\psi^{a,b}(t) = |a|^{-1/2}\psi\left(\frac{t-b}{a}\right) \quad \text{.....(2.1)}$$

The mother wavelet or the primary wavelet is represented by ψ in this equation, and as has been described in the introduction above, the primary wavelet function must also fulfill the following condition:

$$\int |\Psi(\omega)|^2 \, |\omega|^{-1} d\omega < \propto \quad \text{.....(2.2)}$$

Ψ denotes the Fourier transform of ψ in the aforementioned equation. However this condition will have to be loosened. The following is a description of it being loosened:

If $\psi(t)$ *decays* $> t^{-1}$

And $t \to \infty$

Then

$$\int \psi(x)dx = 0$$

The idea behind the DWT is to create a representation of an undetermined signal or function by superimposing certain wavelets. This idea carries through to all applications of the DWT and its various uses. The following shows how we can represent this in actual situations:

$$a = a_0^m, b = nb_0a_0^m$$

when

$$a_0 > 1, b_0 > 0$$

However, in the abovementioned representation, both *m* and *n* are required to be integers which are then bound by the integer groups definition thereby making them fall within (–∞, ∞).

Now when this wavelet is represented in another form, we have the following representation:

$$f = \sum c_{m,n}(f)\psi_{m,n} \quad (2.3)$$

However, the following condition will need to be satisfied for this discrete form representation of work:

$$\psi_{m,n}(t) = \psi_{0\ 0\ 0}^{am,nbam}(t) = a_0^{-\frac{m}{2}}\psi(a_0^{-m}t - nb_0) \quad \ldots\ldots(2.4)$$

Although there have been various decomposition schemes which have been presented from time to time, it is often Mallat who has been credited with presenting a decomposition scheme that can accommodate far more than one resolution. This was presented in 1989 in his landmark study (S.G. Mallat, 1989). Mallat's scheme uses two different styles of functions:

1. The wavelet function used is represented by ψ
2. The scaling function that is being used is represented by ϕ

When the scaling function has been translated and dilated, then it will be represented by the following algorithm:

$$\phi_{m,n}(x) = 2^{-\frac{m}{2}}\phi(2^{-m}x - n) \quad \ldots\ldots(2.5)$$

This will have the following description:

$\varphi_{m,n}(x)$ will be the function that will fill the space of the original function at 2M.

$\psi_{(m,n)}(x)$ will span the orthogonal complement in V_{m-1} of V_m.

This is better explained by saying that $\langle \psi_{m,n}, f \rangle$ is actually the diversity of detail between the resolutions 2^{m-1} and 2^m. That is, the transform coefficients *f, m, n*, ψ describe the difference of the information between resolution 2^{m-1} and 2^m. For an algorithm of projection, we consider the spatial norm to be V_{m-1}–V_m and V_m. Therefore, the signals will be projected according to the following algorithm:

$$c_{m,n}(f) = \langle \psi_{m,n}, f \rangle = \sum_k g_{2n-k}\, a_{m-1,k}(f) \quad \text{.....(2.6)}$$

$$a_{m,n}(f) = \langle \phi_{m,n}, f \rangle = \sum_k h_{2n-k}\, a_{m-1,k}(f) \quad \text{.....(2.7)}$$

Here g = the high pass filter used in the transform and h = the low pass filter used in the transform.

Also, this requires that

$$g_l = (-1)^l h_{-l+1} \quad \text{.....(2.8)}$$

and

$$h_n = 2^{\frac{1}{2}} \int \phi\,(x-n)\phi(2x)dx \quad \text{.....(2.9)}$$

The convolution operator is represented by <.>

When we consider the implementation of (*f*) over the special co-ordinates represented by V_m, we have the following function:

$$a_{m,n}(f)$$

This was first theorized by Antonini et al. in 1992 (Antonini, M., Barlaud, P. Mathieu et al, 1992).

During the transform, the forward process will follow the algorithm:

$$a_{m-1}, i(f) = \sum_n^1 (\tilde{h}_{2n-1} a_{m,n}(f) + \tilde{g}_{2n-l} c_{m,n}(f)) \quad \text{.....(2.10)}$$

If we require the resulting transform to be 100% similar, then the algorithm requires that h~ and g~ be the orthogonal/biorthogonal complements of h and g. Both h and g are considered to be the filters, so they should not have infinite taps as it is not suitable when this is being applied in real-life scenarios. This has

been concluded by Vetterli et al. (M. Vetterli, 1985; M.J. Smith and D.P. Barnwell, 1986; I. Daubechies, 1988).

The following are the requirements of the wavelet filter.

1. In order to increase the processing and transforming speed, they must have a very short length. The length is inversely proportional to the speed and performance wherein the larger the length, the higher the risk of it having a detrimental effect on speed. The lower the length, the higher the speed.
2. The length of the filter is also directly proportional to the smoothness. Therefore, the longer and larger the filter, the more smoothness there is. Thus, a balance must be achieved between filter length and the need for performance.
3. If phase compensation is to be removed, then the linear phase will be required (M. Vetterli and J. Kovacevic, 1995).

The analysis and synthesis for the biorthogonal filters are also represented by the above mentioned algorithms. It is worth noting that such filters are used only for the linear phase and as has been described by M. Vetterli, they are sufficiently different from the orthogonal filters. The following are some of the differences between the two:

Orthogonal filters, when they use synthesis filters, are always created by the transposition of the analysis filters. This means that according to the algorithms given above, it will fulfill the condition that

$$h\sim = h' \text{ and } g\sim = g'$$

When biorthogonal filters are being utilized, they will follow the inverse of this condition. Therefore, the synthesis filters will follow the condition:

$$h\sim \neq h' \text{ and } g\sim \neq g'$$

(M. Vetterli and J. Kovacevic, 1995).

Figure 2.7 shows the DWT mechanism.

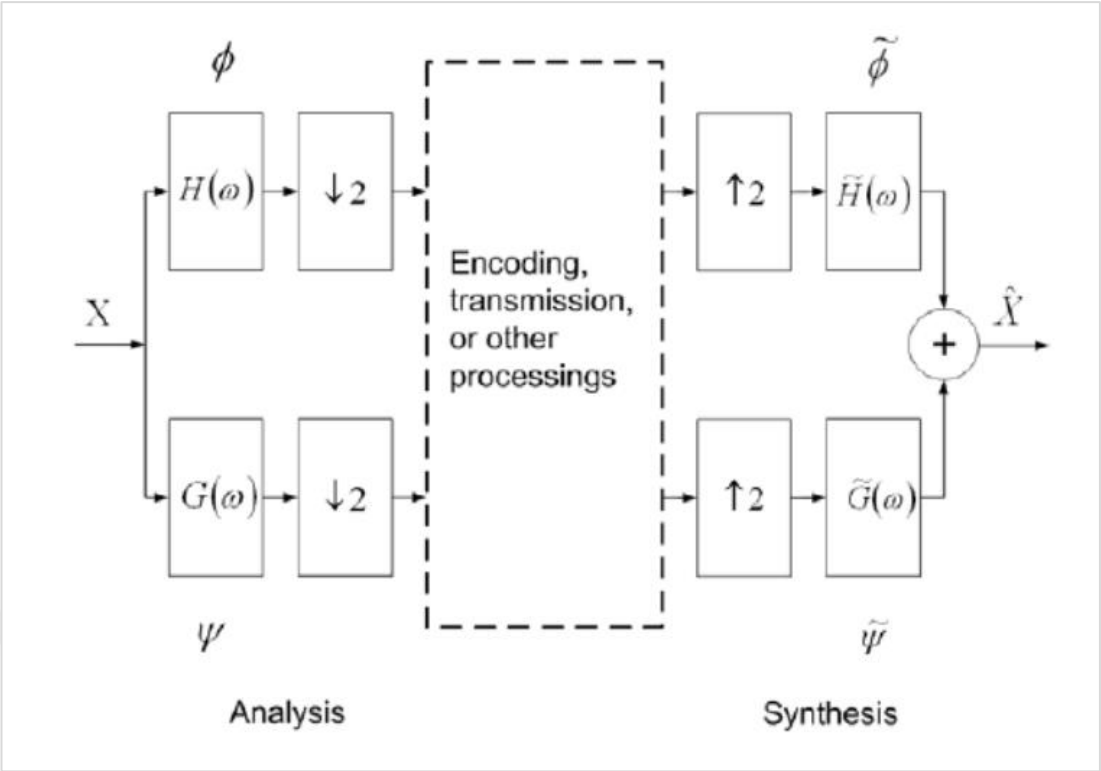


Figure 2.7 DWT mechanism (M. Vetterli and J. Kovacevic, 1995)

When we consider the synthesis filter, we see that this can also be said to be φ ~ and ψ ~. A. Cohen et al. were the first to prove this through algorithms, and to this day, their theoretical and mathematical proof remains the benchmark (A. Cohen, I. Daubechies et al. 1992; M. Antonini, M. Barlaud, P. Mathieu et al. 1992).

A significant job of the DWT process is centered on down sampling. This is the process where the transform signals which have already been acquired are then decimated by a factor of 2:1 during the analysis stage (M. Vetterli and J. Kovacevic, 1995). Figures 2.8, 2.9 and 2.10 show image sub bands used in the DWT.

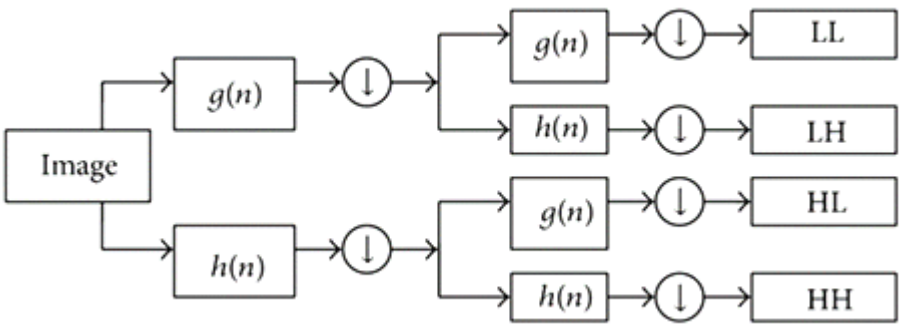


Figure 2.8 Image sub bands in the DWT (M. Vetterli and J. Kovacevic, 1995)

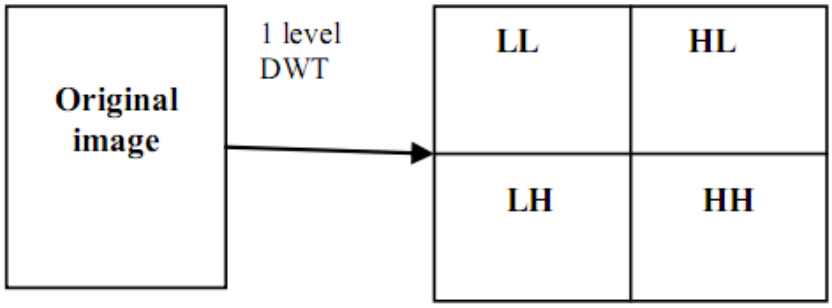


Figure 2.9 First level in the DWT

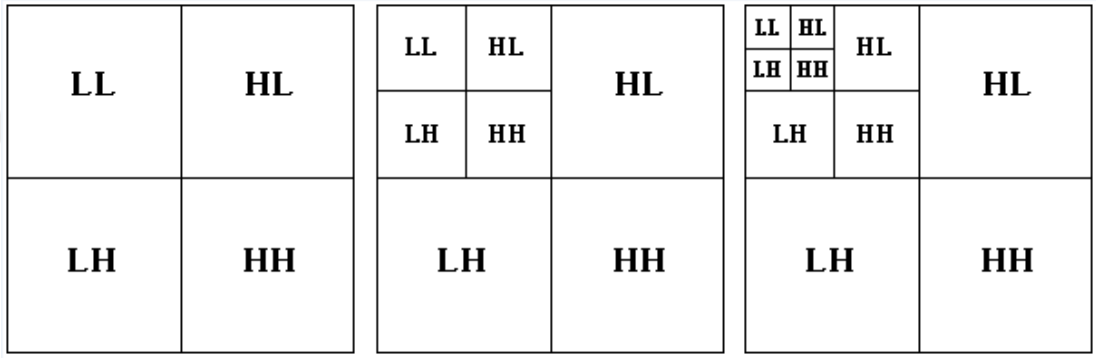


Figure 2.10 Three levels in the DWT

The ratio and the subsequent use of this decimation have been in vogue since their development as QMF in 1977, which has been enlarged upon and refined later on. (D. Esteban and C. Galand, 1977). When the synthesis is about to begin, the signals are processed by using a reverse process called UN sampling. This process uses a 1:2 ratio. Under ideal conditions and if there is no loss of information during either the down sampling or the up sampling processes, the input signal (represented by X) and the reconstructed signal (represented by X^) share the following relation:

$$\hat{X}(z) = z^{-k}X(z),\ K \in N \quad \text{.....(2.11)}$$

In the multiresolution decomposition which was proposed in 1989 by Mallat, the transform will occur by utilizing multiple low-pass sub bands with each axis going through the transform and losing ½ of the primary. For images, this will mean that after each pass, the resolution is reduced to ¼ as there are two dimensions (S.G. Mallat, 1989).

2.7 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 (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 2.11 shows traditional data communications when a message travels through it.

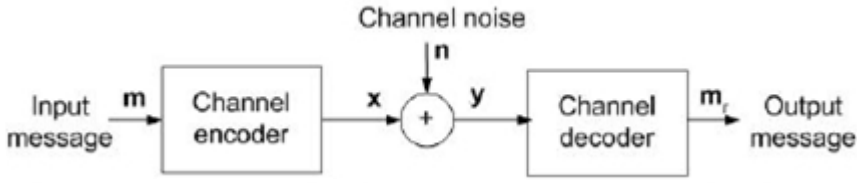


Figure 2.11 Message traveling through traditional data communications

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.

2.7.1 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)

1- 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.
2- 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.
3- 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.
4- 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.
5- 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.
6- Protocol attacks: This kind of attack attempts to whole concept of the watermarking algorithms. Examples include invertibility attacks, where the attcker attempts to take ownership of watermark image itself.

CHAPTER 3

ASSOCIATED PREVIOUS WORKS

3.1 Literature Review

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.

3.1.1 Investigations Studies

Cox et al (1997) have argued that a secure algorithm for watermarking images and other multimedia, such as audio, text and video, should be developed. They have presented an algorithm for watermarking images. The authors have argued that the insertion of a watermark into an independent and identically distributed Gaussian random vector can make the watermark robust. They recommend that the watermark should be placed into the significant components of the image spectrum.

In addition, the common geometric transformations ensure that the original image is accessible and can be listed against the transformed watermarked image. The authors have demonstrated that through this algorithm, the watermark detector clearly recognizes the original owner of the image. The authors further assert that the use of Gaussian noise can ensure security and these arguments are supported by the results and findings of the experiment.

Nikolaidis et al (2001) investigates the scenarios in which digital watermarking is applicable. The research paper also includes the possible situations when digital media can be attacked, and the authors have divided the attacks into categories. These categories include removal attacks, presentation attacks, interpretation attacks and legal attacks. The authors have analyzed these possible categories and scenarios in which attacks are possible; however, they have concluded that the applications may be diverse and that studying and evaluating the scenarios in which these can be implemented must be given proper value.

Tong and Zheng-Ding (2002) describe those authentication techniques for multimedia that are being most widely used for the purpose of authentication

and integrity of content. The authors have divided the authentication techniques into two categories from the perspective of the authenticator. These include digital watermarking based technology and digital signature based technology. However, the main focus of the research paper is based on digital watermarking.

In addition, the paper analyzes the watermarking system, its features, methods of attack, and the circumstances of these attacks along with measures to counter attacks and their after effects. The authors conclude that the developments in digital media lead to an increased importance and significance of digital watermarking with the passage of time and these will be more frequently applied in law and journalism leading to the development of digital watermarking.

According to Motra et al (2003), fast computation of the DWT is necessary for the application of the Discrete Wavelet Transform, such as for audio and video compression. For such an implementation, expensive and fast VLSI devices have been used and an FGPA (a Field-Programmable Gate Array) can also be used for the implementation of the DWT. However, it offers area constrained, but economical, implementation of the DWT. Distributed arithmetic makes way for the implementation of the architecture by a single chip of the Field-Programmable Gate Array (FPGA). The authors have presented FPGA architecture for the implementation of the DWT and IDWT using area-distributed arithmetic, which allows implementing the DWT without consuming area. The FPGA architecture presented by the authors allows for extension without affecting the implementation process or device. The research presents the results that fast implementation of the system can produce high quality signals.

Zhang and Zhang (2004) describe that the wavelet transform has widely been applied in watermarking techniques and results due to the multi-resolution properties of this technique. In this regard, the authors have proposed a watermarking capacity analysis method that can be adapted efficiently in the wavelet domain while they illustrate that previous watermarking capacity analysis methods fall under the spatial domain. Their research paper also includes an analysis of the relation between watermarking capacity and

watermarking detection bit error rate (BER). For the first time, the paper discusses the relation between the limits of BER and the capacity of watermarking.

However, the results of the research show that watermarking capacity and watermarking average energy are the influential factors of the watermarking detection BER (bit error rate). In addition, the results show that with the increase in the watermarking capacity, the BER also increases. The authors have argued that constraints on the power of watermarking are largely a subject of the content of an image, thereby explaining the reason for their having analyzed the watermarking capacity under the wavelet domain. As watermarking research has widely attracted the attention of researchers and scholars, more research has been conducted in the field.

According to Potdar et al (2005), the watermarking is a branch of the information hiding field as it has been used for the protection of content, images and other digital media and manage copyright, tamper detection and authentication of content. On the other hand, Steganography is used for secret communication which is another branch of the information hiding field and both these disciplines are increasingly becoming significant in recent years.

Nonetheless, the authors have conducted a study on the new and existing techniques of both watermarking and steganography. The classification of techniques of both steganography and watermarking is completed with the domains in which data are usually embedded. However, the research is limited to images and not to other types of content.

Steinebach et al (2007) have illustrated that copyright protection has been one of major concerns in today's world. They also state that watermarking is being used in various applications. The transaction of watermarking is one of the great examples of the identification of watermarking, which is the most appropriate approach to digital rights management. However, a number of new challenges for applied algorithms in efficient transaction watermarking have arisen in recent years. A very fast embedding strategy is necessary in order to make the download of marked content fast for the user. This feature is more important in watermarking other than transparency and robustness.

The challenge in transaction watermarking can be met by designing algorithms of low complexity or by providing suitable support mechanisms. However, a low-complexity algorithm would fail to provide high robustness and transparency. In this regard, the authors have presented three strategies to support fast watermark embedding, including container watermarking, client-server watermarking and grid watermarking.

According to Xie et al (2007), in most watermarking schemes, the watermarking embedding key must be available at the watermark detector. The availability of the key at the watermark detector can lead to a security threat due to the fact that detectors may be installed in consumer devices. These public digital watermarking schemes, which are also known as public watermarking techniques, are attracting the attention of researchers and scholars. In this process, two keys are generated wherein the public key is only used for the watermarking detection and the private key is used for watermark embedding. The private key is kept private whereas the public key is known to every device. This public key cannot be used to remove the watermark. In this research paper, the authors have reviewed and analyzed watermarking schemes that have been proposed in the literature and introduced recently and they have evaluated the level of their performance.

Lee and Jung (2007) have stated that embedding a pattern using an algorithm to insert a watermark and to protect media from copyright issues is called digital watermarking, which has become significant at present. In past years, several techniques of watermarking have been introduced; however, there has been no sufficient information about the evaluation and analysis of these techniques in the literature. Nevertheless, the authors have evaluated the previous studies and work in the field in order to evaluate and classify the techniques of watermarking. The research is based on various researchers' and scholars' points of view. After completing the research, the authors argue that transfer domain techniques of watermarking are more popular and are considered to be more effective when presently compared to the spatial domain. Among the transform based methods, DCT-based methods are being used the most extensively. Furthermore, the authors have elaborated that wavelet based

watermarking techniques are now increasingly becoming a significant subject for researchers.

Le et al (2010) have reviewed the literature in the field and they have described the watermarking applications that are available currently along with the benchmarking tools as the benchmarking tools are essential in watermarking. The watermarking tools that are available in the studies and the literature include image watermarking tools, audio watermarking tools and video watermarking tools. Additionally, the authors have analyzed the characteristics of each application and have concluded that image watermarking tools are more commonly used than video and audio watermarking tools.

Sujatha and Sathik (2012) proposed a watermarking scheme that utilizes the perceptual information of an image and generates a watermark using the perceptual information. The disparity values between low frequency sub-bands of the wavelet domain and a rescaled version of the image are identified as the watermark and which use the Arnold Transform. These sub-bands and rescaled versions are disordered.

The process of embedding and extraction of an image in watermarking is done in a high frequency domain of the Discrete Wavelet Transform.

The watermarking scheme involves the process of extracting the information about an image without its presence. Here, a blind scheme has been used. Moreover, the authors have analyzed the competency and performance of this technique through common image processing systems and compared this new scheme with the older ones. The results show that this scheme can offer robustness, imperceptibility and security, which are major concerns in any watermarking technique.

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.

3.1.2 Combined Algorithms Studies

Li et al (2007) have stated that with the increased need for copyright protection, various watermarking techniques have been proposed by researchers and scholars, the most commonly used techniques being the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD). In DWT, the host image is decomposed into frequency bands, while SVD is used in image processing. However, authors have proposed a DWT-SVD domain watermarking

technique which keeps human visual properties under consideration. The proposed method of the DWT-SVD technique for watermarking involves the process of decomposing the host image into four frequency bands. After decomposing, the SVD is applied to each sub-band and a singular watermarking value is embedded into each sub-band. For the analysis of the strength of embedding in images, the human visual model has been proposed and improved in the process. Therefore, the strength of the embedding of this proposed model is determined by a human visual model. Li et al (2007) have argued that their proposed model has the quality of robustness as it embeds data into every frequency sub-band and it has the capacity to use SVD. In addition, the authors have demonstrated that their model is unique as the use of the human visual model can guarantee the imperceptibility of the watermark having been embedded into an image.

Deb et al (2012) have proposed a combined DWT and DCT based watermarking technique with a weighted correction. The DWT (Discrete Wavelet Transform) has characteristics which are similar to the human visual system, which are considered to be excellent features in watermarking. DWT based watermarking techniques are adequate when offering scalability, while the DCT watermarking techniques offer compression and the combination of both is built by using the enviable properties of both in watermarking. In this method, the watermark bits are embedded in the low frequency band of each DCT block of a selected DWT sub-band. Weighted correction is used to enhance the level of imperceptibility. The results of this algorithm show that superior image quality and robustness under various attacks can be preserved using this method. The comparison of this algorithm with other approaches of the DWT and DCT has shown the same results.

Copyright protection and the authenticity of digital multimedia are considered to be the most important issues. According to Chaturvedi & Basha (2012), image watermarking is one of the most famous and reliable methods to protect digital multimedia from copyright issues. This procedure is completed with the help of the Discrete Wavelet Transform (DWT), which performs Level 2 decomposition of the original image. In addition, the watermarked image is embedded in the LL

(lowest level) of the cover image. The authors have stated that IDWT is being used to recover the original image from the watermarked image. On the other hand, DCT (Discrete Cosine Transform) is used to convert the image into blocks of M in order to use the IDCT and reconstruct the image. However, the authors have discussed and evaluated the process of watermarking, similarity and te recovered watermark using both DWT and DWT-DCT. The findings show that DWT-DCT is the best method of level 1 embedding in image watermarking.

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 Mehta and Rajpal (2013), imperceptibility and robustness are the main objectives of watermarking for copyright protection. To achieve this, a hybrid image watermarking algorithm has been built by the authors. The algorithm is based on the Discrete Wavelet Transform and the Singular Value Decomposition. Furthermore, the characteristics of the human visual system model have also been used for authenticity and protection of digital media. The proposed algorithm on a level DWT is applied to blocks of the image to obtain four sub-bands of each block and then a U component is obtained after SVD transformation. The SVD transformation is explored using different values for embedding the watermark in the image. However, the results of the algorithm show that the HVS model is based on a hybrid image watermarking method that is robust and imperceptible as compared to other image processing techniques. Digital watermarking is a technique which provides solutions to the copyright issue in digital and multimedia.

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.

3.1.3 Multi-Level DWT Studies

According to Hu and Jong (2013), the DWT-based watermarking is becoming one of the most significant and most widely used techniques for watermarking. Authors have proposed a novel memory efficient multi-level 2D DWT after reviewing and observing that data scanning has good results on the memory efficiency of DWT architecture. With this new approach, a memory efficient, scalable, parallel, pipelined architecture of multi-level 2D DWT has developed. The results show that the architecture can achieve an area delay product and higher throughput as compared to Cohen-Daubechies-Favreau (CDF).

Sharma and Swami (2013) have proposed the digital watermarking technique based on the 3 level Discrete Wavelet Transform (DWT) and compared it with level 1 and 2 DWTs. In this method, a multi-bit watermark is embedded into the low frequency sub-bands of an image and uses the techniques of alpha blending. The watermark image is dispersed during the process of embedding within the original image and it is dispersed on the scale which is used in the scaling factor of the alpha blending technique. The authors have analyzed the performance of the 3 level DWT compared to levels 1 and 2. However, the performance is measured based on the scaling factor of the embedding and the alpha blending technique.

Patil and Bormane (2013) describe that there are two most important aspects of any image-based stenographic system, namely the capacity of the cover image and the quality of the stego-image. Considering the importance of these aspects, a lossless data hiding scheme has been proposed based on quantized coefficients of the Discrete Wavelet Transform in the frequency domain. A quantized DWT based method has been used to embed data into successive zero coefficients of medium- to high-frequency components in each block for a 3 level 2D DWT of the cover image. Furthermore, by using this method, the original data can be recovered lossless after extracting the data inserted into the image during the process of embedding.

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.

Al-Azwi et al (2014) have introduced an efficient low-complexity multidimensional DWT architecture which is based on a lifting scheme for the CDF DWT filter. This new architecture consists of low-complexity control units and identical computation which are easily implementable on 2D and 3D DWT architectures. The results show that the architecture can operate at a 198 MHz operating frequency, which results in reducing the time for first level DWT decomposition.

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.

CHAPTER 4

PROPOSED ALGORITHM AND EVALUATION

4.1 Proposed Algorithms

In this chapter, 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).

In addition to the discussion of the extraction process, the watermarking images will be subjected to a set of attack tests. The evaluation criteria have been the bases for the assessment of the value of the SNR, PNSR, MAE and RMSE for both the watermarking images and the watermarking images after the attacks. Our proposed algorithm has been implemented and tested using MATLAB code. The steps of our proposed algorithm are as follows:

1. Fix the cover image to the size of 512×512, and reading the two watermark logos each with the size of 512×512.
2. Accomplishment of a fifth level DWT using the Haar wavelets and selecting the LL1, LL2, LL3, LL4 and LL5 sub-bands.
3. Fulfillment of the fourth level DWT for the first watermark logos.
4. Completing the fifth level DWT for the second watermark logos.
5. Start with the embedding processing using the DWT such that the first watermarked (W1) image is embedded in the LL2 and LL4 sub bands and the watermarked (W2) image is embedded in the LL2, LL3 and LL5 sub bands.
6. Perform the fourth level IDWT to reconstruct the first watermarked image.
7. Perform the fifth level IDWT to reconstitute the second watermarked image.
8. Summation of both watermarked images to obtain our watermarking Image.

For the extraction process, we follow these steps:

9. Read the watermarking image.

10. Read the host/cover image.
11. Complete the fifth level DWT for the watermarking image.
12. Complete the fifth level DWT for the host/cover image.
13. Subtract both sets of sub-bands (LL1, LL2, LL3, LL4 and LL5).
14. Show our watermark image.

Figure 4.1 shows our proposed algorithm.

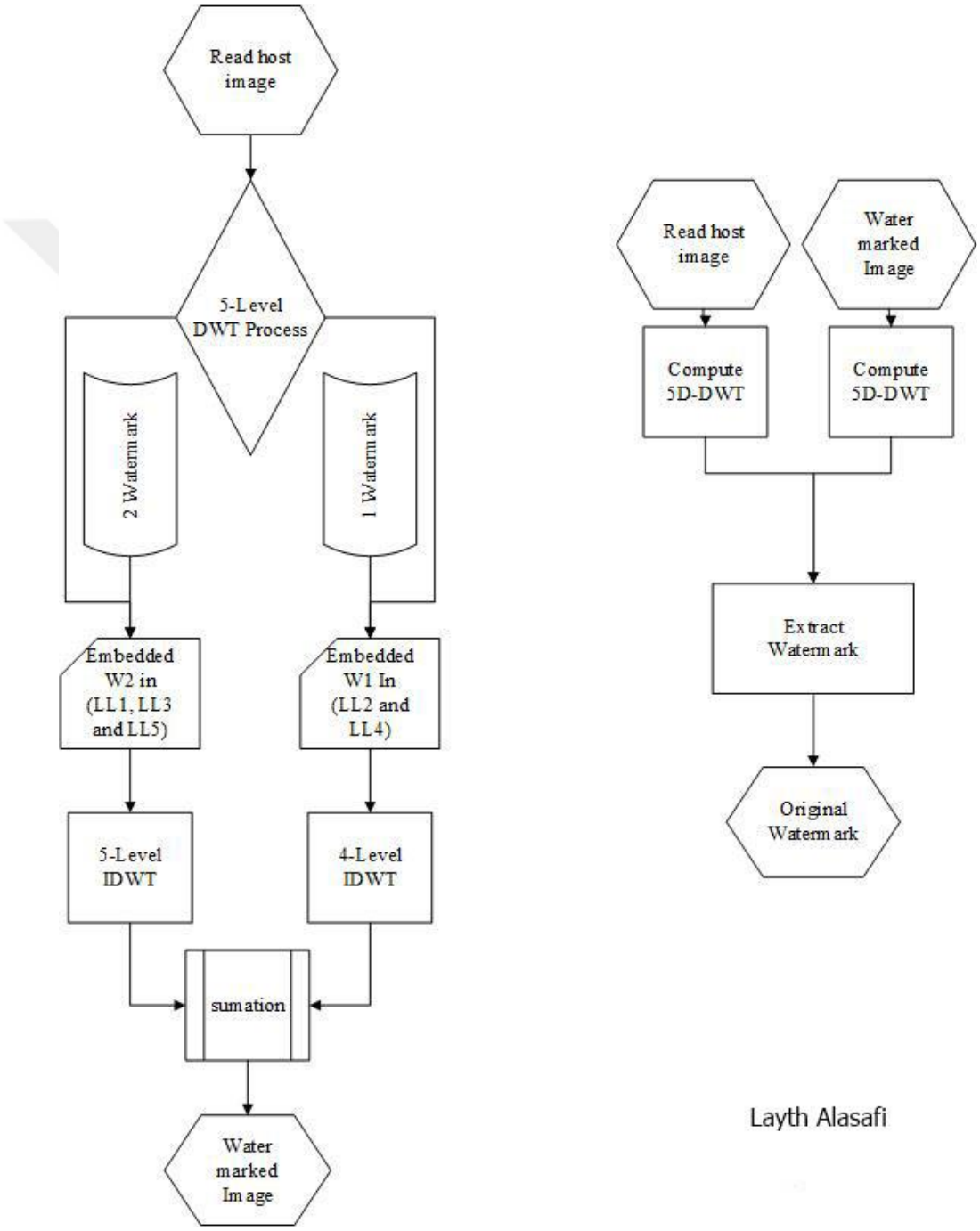


Figure 4.1 Proposed algorithm

4.1.1 Embedding Process

If we assume that we have an image IM(i,j) (512×512 in size) considered to be our cover image, and we assume that we have a watermark image W1(i,j) (512×512 in size) being the primary watermark image and W2(i,j) (512×512 in size) considered to be the second watermark image, and we assume that we obtain the image LW1(i,j) (512×512 in size) as a result of watermarking processer, this will be the first watermarked image, and LW2(i,j) (512×512 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:

$$LW1(i,j) = IM(i,j) + W1(i,j) \quad (4.1)$$

$$LW2(i,j) = IM(i,j) + W2(i,j) \quad (4.2)$$

$$LW(i,j) = (LW1(i,j) + LW2(i,j))/2 \quad (4.3)$$

4.1.2 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:

$$LW1 = IM(i,j) - LW(i,j) \quad (4.4)$$

$$LW2 = IM(i,j) - LW(i,j) \quad (4.5)$$

Figure 4.2 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.

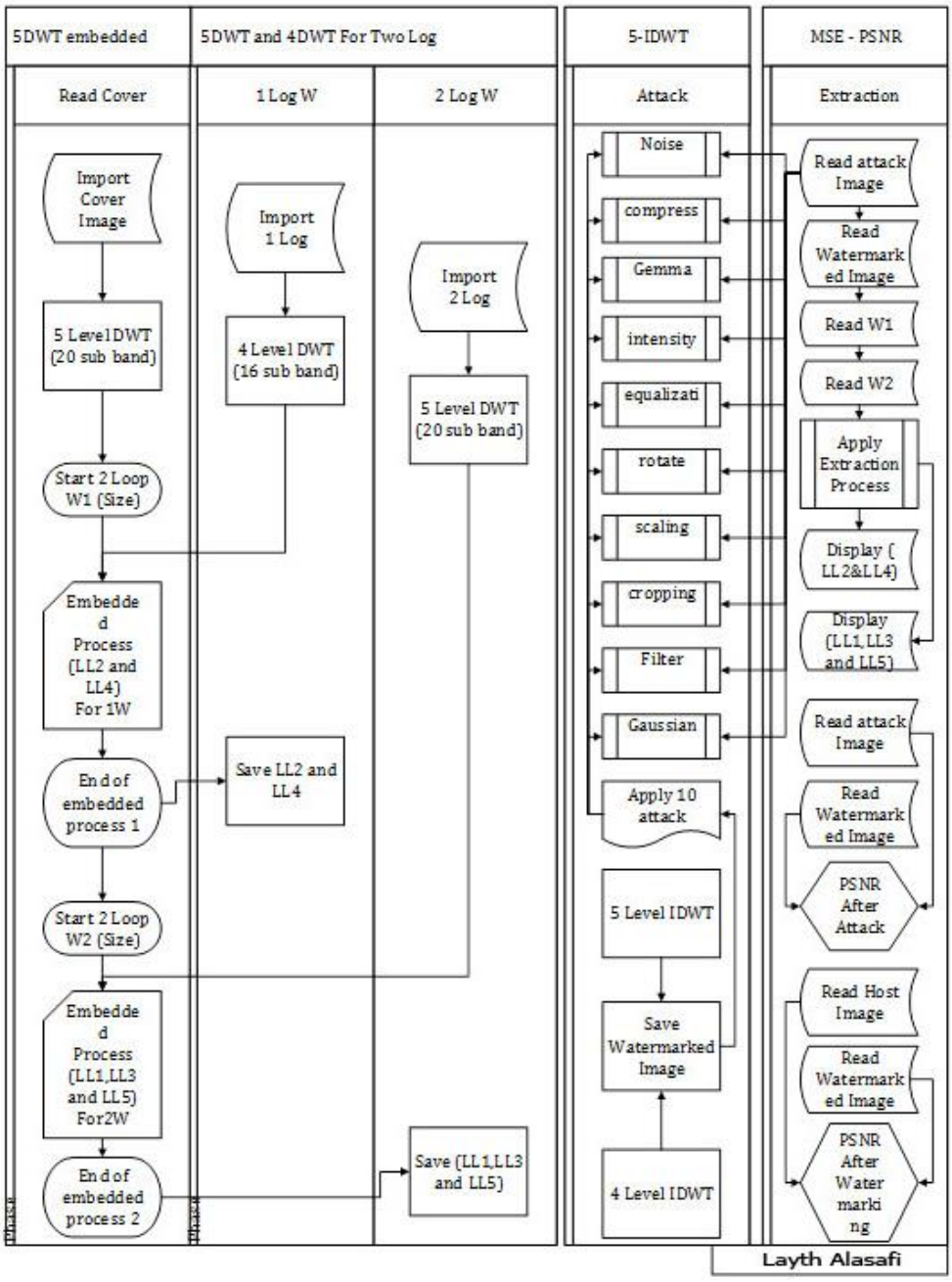


Figure 4.2 Overall proposed algorithms

4.2 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

4.1 shows the five test images along with the watermarked images after the embedding process.

Table 4.1 Test images along with watermarked image after embedded process

Image Name	Cover Image	Watermarked Image
Lena		
Girl face		
Muhammad Ali		

Table 4.1 Cont.

Image Name	Cover Image	Watermarked Image
Zelda		
Sailing boat		

Table 4.2 shows the different gray-scale images of size 512×512 that were used in our lab as the watermark logo.

Table 4.2 Watermark logo used in our lab

Logo Number	Logo Image
1	
2	

Table 4.2 Cont.

3	
4	
5	

4.3 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, Gaussian attack, cropping, noise attack, low pass filtering attack, and a gamma attack. Table 4.3 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 4.4 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 4.3 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 = 3×3	
4.	Cropping	On both sides	

Table 4.3 Cont.

5.	Scaling	512×256	
6.	Rotation	20°	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8] [b=0 t=1]	

Table 4.3 Cont.

9.	Gamma	1.5	
10.	JPEG Compression	Q = 75	
11.	Noise	0.02	

Table 4.4 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 = 3×3)	
4.	Cropping	On both sides	

Table 4.4 Cont.

5.	Scaling	512×256	
6.	Rotation	20˚	
7.	Equalization	Automatic	
8.	Adjustment	[l=0 h=0.8] [b=0 t=1]	

Table 4.4 Cont.

9.	Gamma	1.5	
10.	Compression	Q = 75	
11.	Noise	(0.02)	

4.4 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:

- Peak signal-to-noise ratio (PSNR)

$$PSNR = 10.\log 10\left[\frac{Max(IM(i,j))^2}{\frac{1}{Ni.Nj}\bullet\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)-T(i,j)]^2}\right] \quad \text{.....(4.6)}$$

- Signal-to-noise ratio (SNR)

$$SNR = 10.\log 10\left[\frac{\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)]^2}{\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)-T(i,j)]^2}\right] \quad \text{.....(4.7)}$$

- Mean absolute error (MAE)

$$MAE = \frac{1}{Ni.Nj}.\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)-T(i,j)] \quad \text{.....(4.8)}$$

- Root mean square error (RMSE)

$$RMSE = \sqrt{\frac{1}{Ni.Nj}.\sum_{0}^{Ni-1}\sum_{0}^{Nj-1}[IM(i,j)-T(i,j)]^2} \quad \text{.....(4.9)}$$

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 4.5 (a) and (b), Tables 4.6 (a) and (b), and Tables 4.7 (a) and (b).

Table 4.5 (a) Lena Cover image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	47.82907559	52.77628772	0.58576820	0.34312439
Gaussia.png	25.22651011	30.17372224	7.90412989	6.26767349
Filter.png	24.06624841	29.01346054	9.03373098	5.51398087
crop.png	5.13903406	10.08624619	79.84134984	35.40832520
Resize.png	24.08718737	29.03439950	9.01197971	5.66981888
Rotate.png	3.35254691	8.29975904	98.07362512	76.23985291
Equal.png	29.39658058	34.34379271	4.89046939	4.15634537
Intensit.png	13.84397549	18.79118762	29.30763670	25.29699707
Gamma.png	14.41038912	19.35760125	27.45744471	24.86824799
Hostr75.jpg	29.67216958	34.61938171	4.73773859	3.57241058
Noise.png	16.80074205	21.74795418	20.85174819	2.86824036

Table 4.5 (b) Lena watermarked image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	25.26598820	30.19573247	7.88412601	6.25088120
Filter.png	24.07408171	29.00382599	9.04375693	5.47851181
crop.png	5.12099814	10.05074242	80.16837112	35.44919586
Resize.png	24.12874021	29.05848449	8.98702513	5.61575699
Rotate.png	3.35791408	8.28765836	98.21035083	76.32825470
Equal.png	30.20442794	35.13417222	4.46510390	3.81538010
Intensit.png	13.94897931	18.87872359	29.01375911	24.95387268
Gamma.png	14.32426730	19.25401158	27.78686824	25.20635223
Hostr75.jpg	29.75464581	34.68439009	4.70241199	3.52939606
Noise.png	16.82225123	21.75199551	20.84204863	2.53207397

Table 4.6 (a) Girl face Cover Image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	44.47991684	50.95081526	0.58671823	0.34423828
Gaussia.png	21.97382975	28.44472817	7.82949835	6.15766525
Filter.png	24.85652947	31.32742789	5.61822271	2.93664932
crop.png	4.85621928	11.32711770	56.18423351	26.92266464
Resize.png	25.39995098	31.87084940	5.27749555	2.96701813
Rotate.png	5.75075750	12.22165592	50.68594520	44.16291046
Equal.png	11.87286664	18.34376506	25.04852126	21.39670181
Intensit.png	10.13551488	16.60641330	30.59494524	27.97736359
Gamma.png	30.13382618	36.60472460	3.06008941	2.14155960
Hostr75.jpg	13.70091760	20.17181602	20.29455553	2.86085129
Noise.png	44.47991684	50.95081526	0.58671823	0.34423828

Table 4.6 (b) Girl face watermarked image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	22.03663819	28.47827954	7.79931333	6.13988113
Filter.png	24.87187162	31.31351298	5.62723039	2.86005020
crop.png	4.82891379	11.27055514	56.55129941	26.96273422
Resize.png	25.49747200	31.93911335	5.23618133	2.86148071
Rotate.png	3.40632366	9.84796502	66.61500958	47.24612427
Equal.png	5.83840907	12.28005043	50.34633069	43.81867218
Intensit.png	12.02000946	18.46165082	24.71085684	21.05246353
Gamma.png	10.06665381	16.50829517	30.94251335	28.32160187
Hostr75.jpg	30.32766935	36.76931070	3.00265068	2.06389999
Noise.png	13.73775095	20.17939230	20.27686129	2.52335739

Table 4.7 (a) Muhammad Ali Cover Image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Wimage.png	49.38390966	52.76182697	0.58674424	0.34426880
Gaussia.png	26.58975149	29.96766880	8.09387961	6.44962311
Filter.png	25.20439179	28.58230910	9.49346438	4.02235794
crop.png	5.57218265	8.95009996	90.99869882	43.35406876
Resize.png	25.80960324	29.18752055	8.85450226	4.16621017
Rotate.png	5.56165645	8.93957376	91.10904459	62.26588821
Equal.png	11.71319380	15.09111111	44.87295035	39.23724365
Intensit.png	13.03213091	16.41004821	38.55118834	36.25600433
Gamma.png	16.41674907	19.79466638	26.10999937	24.96641159
Hostr75.jpg	46.99189351	50.36981082	0.77276891	0.48598862
Noise.png	18.45420456	21.83212187	20.65066716	2.90584183

Table 4.7 (b) Muhammad Ali watermarked image used as a reference image

Test Image	SNR	PSNR	RMSE	MAE
Gaussia.png	26.62830653	29.99149453	8.07170821	6.43125153
Filter.png	25.19810688	28.56129488	9.51646021	3.94215775
crop.png	5.55367372	8.91686173	91.34759004	43.39382553
Resize.png	25.84879599	29.21198399	8.82959901	4.07315445
Rotate.png	5.55882695	8.92201495	91.29341082	62.36033249
Equal.png	11.66577508	15.02896309	45.19517019	39.51578522
Intensit.png	13.11704168	16.48022969	38.24095206	35.91173553
Gamma.png	16.31765479	19.68084279	26.45440761	25.31054306
Hostr75.jpg	50.41159471	53.77478271	0.52215693	0.23861313
Noise.png	18.46966265	21.83285065	20.64893455	2.56837845

4.5 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 4.8 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 4.8 Extraction of the watermark logo before and after attack

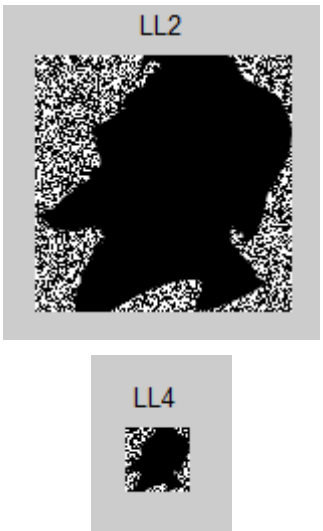
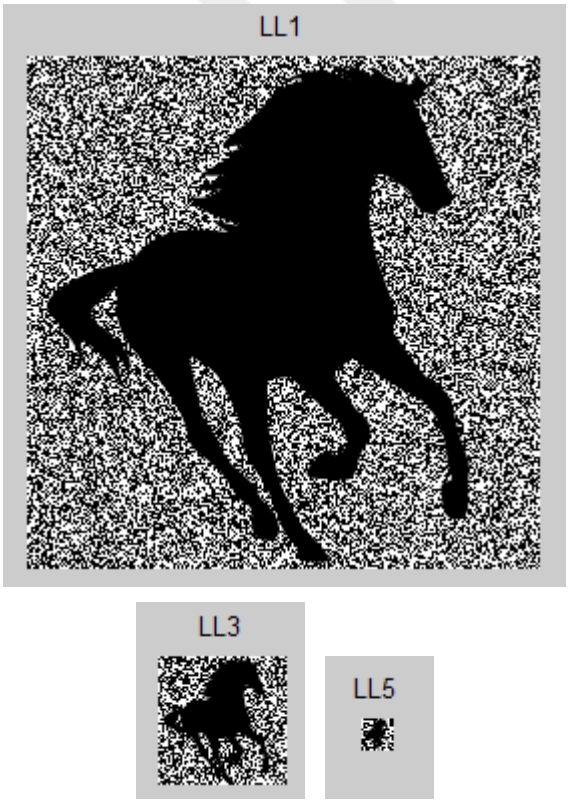
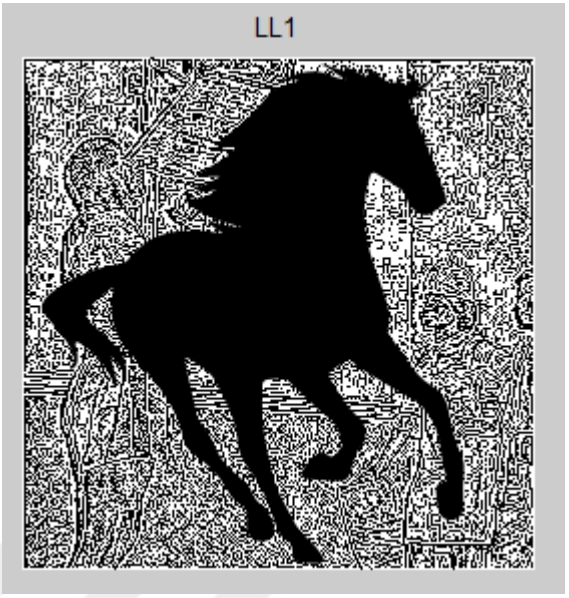
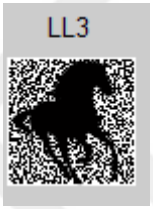
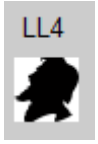
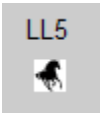
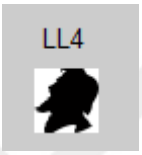
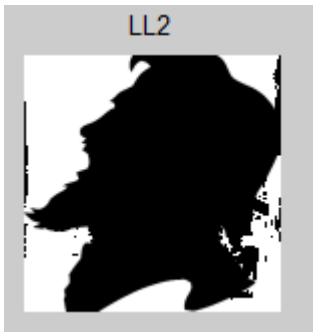
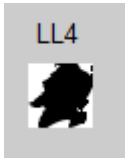
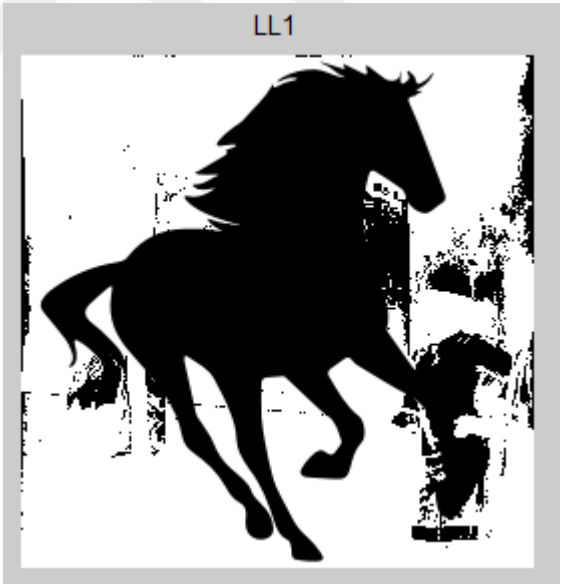
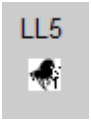
Test Image	First Watermark Logo	Second Watermark Logo
Extraction from watermarked image		
Gaussian (mean = 0, variance = 0.001)		

Table 4.8 Cont.

Filter (0.02)	 	  
Gamma –1.5	 	  

Cropped both sides	 	  
Equalization	 	  

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

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.

5.2 Recommendations

Science and technology related to image processing are an accelerated form of evolution. Due to the heavy reliance on the use of modern technology and the need for transferring of digital objects through multiple types of communication channels, some such channels can be unsafe in a variety of ways, in addition to the wide range of applications that involve watermarking techniques as tools to support the work in copyright protection and the improvement of ownership. The following are some recommendations for future work:

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

REFERENCES

[1] Graps, "An introduction to wavelets," Computational Science & Engineering, IEEE, vol. 2, pp. 50-61, 1995.

[2] Al-Azawi, S., Abbas, Y.A. & Jidin, R., (2014), Low Complexity Multidimensional CDF 5/3 DWT Architecture, *9th International Symposium on Communication Systems, Networks and Digital Sign,* pp. 804-808.

[3] Amit Kumar Singh, 2015, "Robust and Imperceptible Dual Watermarking for Telemedicine Applications," Wireless Personal Communications, Volume 80, Issue 4, pp 1415-1433

[4] 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, Vol. 78. No. 2 – 2015.

[5] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., "Digital Watermarking for Copyright Protection: A Communications Perspective." IEEE Communications Magazine. Vol. 39, No. 8, (August 2001): pp. 90-133.

[6] Chaturvedi, N., & Basha, S.J, (2012), Comparison of Digital Image Watermarking Methods DWT & DWT-DCT on the Basis of PSNR, *International Journal of Innovative Research, Engineering and Technology,* Vol. 01, Issue 02, pp. 147-153.

[7] Cox, I.J.; Miller, M.L.; McKellips, A.L.; "Watermarking as communications with side information," Proceedings of the IEEE, Volume: 87 Issue: 7, July 1999, pp. 1127-1141.

[8] Cox, I.J., Kilian, J., Leighton, T. & Shamoon, T., (1997), Secure spread spectrum watermarking for multimedia, *IEEE transactions on image processing,* Vol. 06, No. 12, pp. 1673-1687.

[9] Deb, K., Al-Seraj, S., Hoque, M., & Sarkar, I.H., (2012), Combined DWT-DCT based digital image watermarking technique for copyright protection, *7th International Conference on Electrical and Computer Engineering, IEEE,* pp. 458-461.

[10] Gitanjali Verma, 2015, “Comparative Study of Imperceptible digital Watermarking Techniques,” Journal of Current Computer Science and Technology, Vol. 5, No 6 (2015).

[11] Gunjal, B.L. & Mali, S.N., (2014), Comparative Performance Analysis of Digital Image Watermarking Scheme in DWT and DWT-FWHT-SVD domains, *Annual IEEE India Conference.*

[12] Hu, Y & Jong, C.C., (2013), A memory efficient High-Throughput Architecture for Lifting-Based Multi-Level 2D DWT, *IEEE Transactions on Signal Processing,* Vol. 61, No. 20, pp. 4975-4987.

[13] 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/

[14] J. Cox, M.L. Miller, and J.A. Bloom, “Digital Watermarking,” Morgan Kaufmann, 2001.

[15] J.Y. Stein, Digital signal processing: a computer science perspective, New York: Wiley, 2000.

[16] Jane, O & Elbaşı, E, (2014), A new approach of non-blind watermarking methods based on DWT and SVD via Lu decomposition, *Turkish Journal of Electrical Engineering & Computer Science,* doi: 10.3906/elk-1212-75.

[17] K. Magai, H. Ito ; H. Mishima; M. Suzuki; K. Asai, 2004, “Watermarking robust against analog VCR recording,” Image Processing, 2004. ICIP ’04. 2004 International Conference on, Volume: 5)

[18] Kaur, R. & Jindal, S. (2014), Robust Digital Image Watermarking in High Frequency Band using Median Filter Function Based on DWT-SVD, *Fourth International Conference on Advanced Computing and Communication Technologies,* pp. 47-52.

[19] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R.L., “Watermarking Digital Image and Video Data: A State-of-the-Art Overview” IEEE Signal Processing Magazine. Vol. 17, No. 5, (September 2000): pp. 20-47.

[20] Le, T., Nguyen, K.H. & Le, H.B., (2010), Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking tools, *second international Conferences on Advances in Multimedia, IEEE,* pp. 67-73.

[21] Lee, S., & Jung, S., (2001), A survey of watermarking techniques applied to multimedia, ISIE, pp. 272-277.

[22] Li, Q, Yuan, C & Zhong, Yu-Zhuo, (2007), Adaptive DWT-SVD domain image watermarking using Human visual Model, *ISBN,* pp. 1947-1951.

[23] Linlin Tang, Yu Tian, Jengshyang Pan, 2015, "Applications of Cloud Model in Digital Watermarking," Chapter Intelligent Data Analysis and Applications Volume 370 of the Series Advances in Intelligent Systems and Computing, pp. 371-379.

[24] Malakooti, M.V., Panah, Z.F. & Hashemi, S.M., (2013), Image Recognition Method based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD), *SDIWC,* pp. 42-47.

[25] Mehta, R. & Rajpal, N., (2013), A Hybrid Semi-blind gray-scale image watermarking algorithm based on DWT-SVD using human Visual System Model, *IEEE,* pp. 163-168.

[26] Motra, A.S., Bora, P.K., & Chakrabarti, I., (2003), AN efficient hardware Implementation of DWT and IDWT, *IEEE,* pp. 95-99.

[27] Nikolaidis, A., Tsekeridou, S., Tefas, A. & Solachidis, V., (2001), A survey on watermarking application scenarios and related attacks, *IEEE,* pp. 991-994.

[28] Panchal, U. H & Srivastava, R (2015), A comprehensive Survey on Digital Image Watermarking techniques, *Fifth International Conference on Communication Systems and Network Technologies,* pp. 591-595.

[29] Patil, P. & Bormane, D.S., (2013), DWT Based Invisible Watermarking Technique for Digital Images, *International Journal of Engineering and Advanced Technology (IJEAT),* Vol. 02, Issue. 04, pp. 603-605.

[30] Petitcolas, F., Anderson, R., and Kuhn, M., "Information Hiding – a Survey." Proc. of the IEEE. Vol. 87, No. 7, (July 1999): pp. 1062-1078.

[31] Podar, V.M., Han, S. & Chang, E., (2005), A Survey of Digital Image Watermarking Techniques, *3rd IEEE International Conference on Iindustrial Informatics,* pp. 709-716.

[32] 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): pp. 690-695.

[33] R. Sugihara et al., 2001, "Practical capacity of digital watermark as constrained by reliability," Information Technology: Coding and Computing, 2001. Proceedings. International IEEE Conference, pp. 85-89.

[34] R. C. Gonzalez and R.E. Woods, "Digital Image Processing," 3rd ed., Prentice Hall, 2008.

[35] Saini, S, (2015), A survey on watermarking web contents for protecting copyright, *IEEE Sponsored 2nd International conference on Innovations in Information Embedded and Communication Systems.*

[36] Sathik, M.M. & Sujatha, S.S., (2012), A Novel DWT Based Invisible Watermarking Technique for Digital images, *International Arab Journal of e-Technology,* Vol. 02, No. 03, pp. 167-173.

[37] Sharma, P. & Jain, T., (2014), Robust Digital Watermarking for Colored Images Using SVD and DWT Techniques, *IEEE,* pp. 1024-1027.

[38] Sharma, P. & Swami, S., (2013), Digital Image Watermarking Using 3 Level Discrete Wavelet Transform, *Conference on Advances in communication and control systems,* 2013, pp. 129-133.

[39] Steinebach, M., Hauer, E. & Wolf, P., (2007), Efficient Watermarking Strategies, *Third International Conference on Automated production of Cross Media Content for Multi-Channel Distribution,* IEEE, pp. 65-71.

[40] Swanson, M.D., Kobayashi, M., and Tewfik, A.H., "Multimedia Data-Embedding and Watermarking Technologies." Proc. of the IEEE. Vol. 86, No. 6, (June 1998): pp. 1064-1087.

[41] T.H.N. Le, K.H. Nguyen; H.B. Le, 2010, "Literature Survey on Image Watermarking Tools, Watermark Attacks and Benchmarking Tools," Advances in Multimedia (MMEDIA), 2010, Second International Conferences, pp. 67-73.

[42] Tao, P. & Eskicioğlu, A.M., (2015), A robust multiple watermark scheme in the Discrete Wavelet Transform domain.

[43] Tong, L. & Zheng-Ding, Q., (2002), The survey of digital watermarking-based image authentication, *IEEE,* pp. 1556-1559.

[44] Voloshynovskiy S. et al., "Attacks on Digital Watermarks: Classification, Estimation Based Attacks, and Benchmarks." IEEE Communication Magazine. Vol. 39. No. 8, (August 2001): pp. 118-126.

[45] Xie, R., Wu, K., Duand, J. & Li, C., (2007), Survey of Public Key Digital Watermarking Systems, *ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and parallel/Distributed Computing,* pp. 439-443.

[46] Zhang, W., Zhu, W., and Fu, Y., "An Adaptive Digital Watermarking Approach." Proc. of IEEE Int. Conference on Mechatronics and Automation, Chengdu, China. (August 2004): pp. 690-695.

[47] Zhang, F. & Zhang, H., (2004), Image Digital Watermarking Capacity and Reliability Analysis in Wavelet Domain, *IEEE 47th International Midwest,* pp. 101-104.

CURRICULUM VITA

Personal Information:

Name : Layth Alasafi

Place of Birth : Kirkuk-Iraq

Date of Birth : 05.05.1972

Marital Status : Married

Nationality : Iraqi

Education:

Undergraduate Education: Ministry of Higher Education & Scientific Research / foundation of technical Education / Electronic And Control Engineering / Republic Of Iraq

ÖZGEÇMİŞ

Kişisel Bilgiler:

Adı ve Soyadı : Layth Alasafi

Doğum Yeri ve Yılı : Kerkük-Irak- 05.05.1972

Medeni Hali : Evli

Milliyet : Irak

Yabanc Dili : İngilizce

Eğitim Durumu:

Lisans Öğrenimi : Yükseköğretim ve Bilmsel Araştırma Bakanlığı / Teknik Eğitim Kurumu / Elektronik ve Kontrol Teknikleri Mühendisliği / IRAK CUMHURİYETİ