Imperceptibility and Robustness Improvement using segmented DWT Watermarking Technique

تحسين اللادراكية والمتانة باستخدام التقسيم لتقنية التحويل المويجي المتقطع للعلامة المائية

Prepared By
Sura Abdulmunem.M.Al-juboori

Supervisor By
Prof. Dr. Hamza Abbass Al-Sewadi

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

January, 2019

Authorization statement

I, **Sura Abdulmunem AL-Juboori**, authorize the Middle East University to provide hard copies or soft copies of my thesis to libraries, institution or individuals upon their request.

Name: Sura Abdulmunem AL-Juboori

Date: 30/1/2019

Signature: 

اقرار التفويض

انا **سرى عبد المنعم الجبوري** . افوض جامعة الشرق الاوسط بتزويد نسخ من رسالتي ورقيا او الكترونياً للمكتبات، او المنظمات، او الهيئات و المؤسسات المعنية بالابحاث والدراسات العلمية عند طلبها .

الاسم : سرى عبد المنعم محمد الجبوري

التاريخ : 2019/1/30

التوقيع : 

Examination Committee Decision

This is to certify that the thesis entitled **"Imperceptibility and Robustness Improvement using segment DWT watermarking technique"** was successfully defended and approved on 27/1/2019.

Examination Committee Members	***signature***

(Chairman of Examination Committee and Supervisor)

Porf. Hamza Abbass AL-Sewadi

Professor

Middle East University

Hamza A. Al
30/1/2019

(Internal committee Member)

Dr. Mudhfar Al-Jarrah

Associate professor

Middle East University

(External committee Member)

Dr. Mohammad Hatim Hijjawi

Assistant Professor

Applied Science Private University

M. Hijjawi

Acknowledgments

First, thanks to ALLAH HIS ALMIGHTY for enabling me to complete this work in spite of all the difficulties. I would like to sincerely thank Prof. Dr. Hamza Abbass Al-Sewadi, for his guidance, assistance, understanding, patience and most importantly, his Collaborate with me during from Complete of this study at the Middle East University. His mentorship was paramount in providing a well-round experience consistent with my long- term career goals. I want to thank Assistant teacher Ammar.H.Ali, for help me advice and suggestions. Thanks to those whose spirits were supportive to me, But the will of God did not give them chance to share this moment my father and my uncle, may God have mercy on them, My deepest thanks to give My Mother, My husband and my family for their love, support and patience during my study. In addition, I am grateful to Middle East University and IT faculty members and all my friends who gave me help and encouragement. Thanks for all.

The Researcher

Dedication

My dear mother, my husband who carried patience with me and encouraged me and give the best support, my daughters granules, brother, sisters and close friends for their full support, for their great patience, endless love, attention and pray for me.

I dedicate my effort this modest them

Table of Contents

List of Tables

List of Figures

Table of Abbreviations

DW	Digital Watermark
C	Carrier image
W	Watermark
CW	Watermark image
2D-DWT	2 level –discrete wavelet transform
PNSR	Peak signal noise ratio
NCC	Normalized Cross correlation
MES	Mean square error
SSIM	Structural similarity index
QIM	Quantization index modulation
LSB	Less significant bits
SVMs	Support vector machine
SVD	Single Value Decomposition
DCT	Discrete Cosine Transform
DFT	Discrete Fourier transform
DWT	Discrete Wavelet Transform
HVS	Human visual system
SMQT	Successive mean quantization transform
LL	Low-low Sub brand
LH	Low-high Sub brand
HL	High-low Sub brand
HH	High-high Sub brand
IDWT	Inverse discrete wavelet transform
AES	Advance encryption standard
DES	Data encryption standard

H	Host image
K1	Key for encrypted watermark
K2	Key for embedding and extraction
HH2	High–high (level two)
N	Number of segment to original image
Wn	Number of segment to watermark
Enc	Encryption
Dec	Decryption
T.em	Time embedding
T.ex	Time extraction

Imperceptibility and Robustness Improvement using segmented DWT Watermarking Technique

Prepared by
Sura Abdulmunem Mohammed
Supervisor by
Prof.Dr. HamzaAbbass Al-Sewadi

Abstract

A watermark is one of the means of preserving copyright. It is a technique for including information with confidential or personal content within a picture, video or text. This thesis proposes a method of inclusion in which the division is the basic idea; this division is for both carrier image (grayscale), such as (512*512) and the watermark (binary image) of different sizes using two cases such as (2 * 2 & 4 * 4). After dividing the image of the carrier we use a technique (DWT-2 level) that proved high performance in terms of robustness and imperceptibility, which is the core of this study. An algorithm (AES-128) was used to encrypt each of the segments from watermark before embedding, as the first key, and then use another key for embedding inside the carrier image, for more security. The experimental results of the proposed method (with segmentation) have shown high imperceptibility and robustness as compared with the results of the (without segmentation) method it remained unchanged and some are very few for most of the measurements. And it has also proved to be robust against noise (Salt and pepper, Additive, and Gaussian blur) but gave weak results using rotation and loss of watermark embedded by cropping. Hence, this technique would be suitable for applications that involve resistant to attacks, and copyright protection.

Keywords: Segmentation, Copyright, traditional method, proposed method ،Cryptography, Digital watermarking.

تحسين اللادراكية والمتانة باستخدام التقسيم لتقنية التحويل المويجي المتقطع للعلامة المائية

إعداد

سرى عبد المنعم محمد سلطان

إشراف

الأستاذ الدكتور حمزة عباس السوادي

الملخص

العلامة المائية هي واحدة من وسائل الحفاظ على حقوق النشر. فأنها تعتبر تقنية لتضمين معلومات ذات محتوى سري أو شخصي داخل صورة أو فيديو أو نص. تقترح هذه الرسالة طريقة للتضمين يكون فيها التقسيم هو الفكرة الأساسية ؛ هذا التقسيم يكون لكل من صورة الحامل (ذات تدرج الرمادي) بأبعاد (٥١٢ * ٥١٢) والعلامة المائية (الصورة الثنائية) بأحجام مختلفة باستخدام حالتين (٢ * ٢ & ٤ * ٤). بعد تقسيم صورة الناقل ، نستخدم تقنية (مستوى DWT-2) التي أثبتت أدائها العالي من حيث القوة والحساسية ، وهي جوهر هذه الدراسة. تم استخدام خوارزمية (AES-128) لتشفير كل جزء من العلامة المائية قبل التضمين كالمفتاح الأول ، ثم استخدام مفتاح آخر للتضمين داخل صورة الناقل ، لمزيد من الأمان. واظهرت النتائج التجريبية للطريقة المقترحة (مع التجزئة) بأنها لم تغيير وبعضها ذات فارق قليل مقارنة مع نتائج الطريقة التقليدية (بدون تجزئة) لمعظم القياسات المستخدمة ، كما أثبتت أنها قوية ضد الضوضاء (ملح وفلفل، المضاف،والغوسيه) ولكنها أعطت نتائج ضعيفة باستخدام التدوير، مع فقدان للعلامة المائية عند باستخدام الاقتصاص . وبالتالي ، فإن هذه التقنية ستكون مناسبة للتطبيقات التي تنطوي على مقاومة الهجمات وحماية حقوق النشر.

الكلمات المفتاحية: التجزئة ، حقوق النشر ، الطريقة التقليدية ، الطريقة المقترحة ،التشفير ، العلامات المائية الرقمية.

Chapter one

Background and Study Importance

Chapter one

Background and Study Importance

1.1 Introduction

watermarking gained a great international attention by including the digital watermark, for example embedding watermark data into the original information and in other words, a type of a bit stream inserted as digital watermark into multimedia data such as text , video, audio, and image files where this helps to keep the copyright information (for the author).

For more explanation, the watermark is a digital signature or a stamp placed on an image (for example) to determine its ownership.

In general, there are two important properties of a watermark; the first property is that the watermark embedding should not alter the quality and visibility of the host image and it should be invisible and when a "watermark" became visible, it can be considered weak because of the easy of removing it and making a copy of the material (steal it).

The watermark preferred designed is to be completely invisible, hence the data representing the watermark should be scattered throughout the file multimedia in a way that it cannot be identified and manipulated.

The second property is robustness against image distortions. This means that the watermark is hard for an attacker to remove and it should be also robust to common image processing and geometric operations, such as resizing, rotating, filtering, and image compression.

The embedding process used to preserve the original data unchanged especially to the detection of the watermark which should be only removed by the extraction algorithm.

Different types of watermark algorithms are developed with a view to serve different purposes. The significant three types can be identified as follows

1. Robust watermark for robustly carrying ownership information

2. Imperceptibility refers to the perceptual similarity between the watermarked and the original images.

3. Capacity refers to the number of watermark bits embedded into the host image.

The embedding techniques of watermark generally follow either spatial domain analysis or transform domain analysis or both.

This thesis suggests and discusses a watermarking algorithm that adopts a fragmented technique for color image. The effect of segmenting is investigated for improvement of imperceptibility and robustness. The proposed algorithm employs the two dimensional discrete wavelet transform (2D-DWT) as the technique for embedding the watermark in images.

1.2 History of watermarking

The art of papermaking was invented in China over a thousand years ago, however, paper watermarks did not appear until about 1282, in Italy. The marks were made by combine thin wire patterns to the paper molds, the paper would be slightly thinner where the wire was and hence more transparent. (Jonathan M. Bloom, 1999)

For that, meaning and purpose of the earliest watermarks were uncertain. They may have been used for practical functions such as identifying the molds on which sheet of papers was made, or as trademarks to identify the paper maker. On the other hand, they might have represented Signs symbolize something else, or might simply have as decoration.

By eighteenth century, watermarks on paper made in Europe and America had become more clearly and utilitarian. They were used as trademarks, to record the date the paper was manufactured and to indicate the size of original sheets (Jonathan M. Bloom, 1999).

It was also began to be used as anti-counterfeiting measures on money and documents

Komatsu and Tominaga In 1988 were the first researchers who used the term digital watermark. However, this term really came into publicity on the early of 1990 (I. J. Cox, M. L. Miller and J. A. Bloom, 2002).

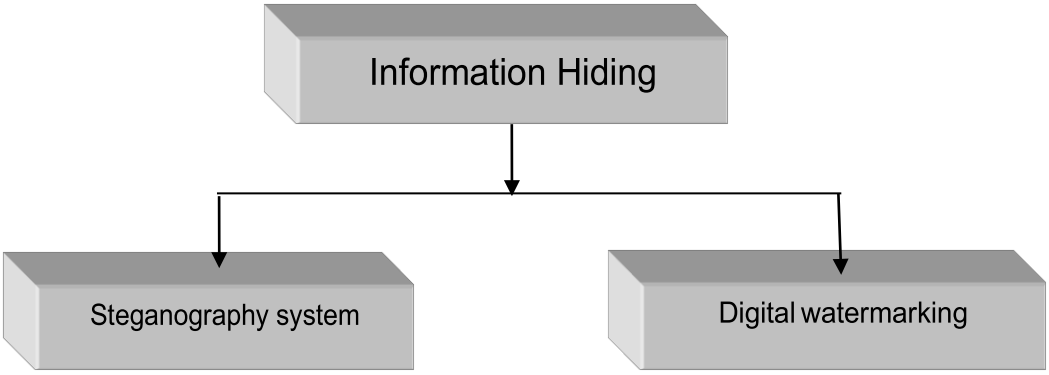
Since 1995 digital watermarking has acquired a lot of attention and has developed very fast and there are a lot of topics open for further research. In the late of 1990s several companies were established to market watermarking product (S. Katzenbeisser and F. A. P. Petitcolas, 2000).

1.3 Information hiding, steganography, and watermarking

Information security has become more necessary and very important, so there is a need for a technique that can maintain the transfer of information without being exposed to theft or vandalism.

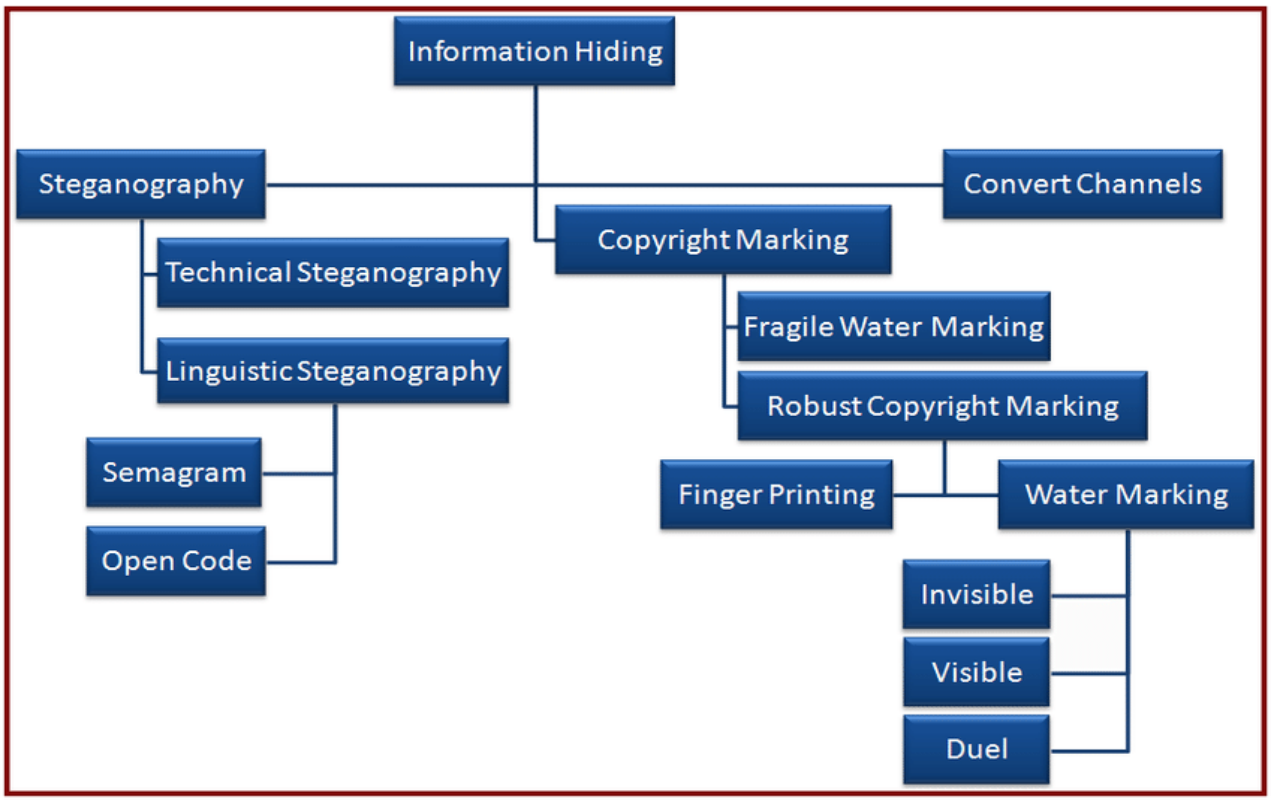
The system of information concealment is mainly classified into two parts:

steganography and digital watermarking, as illustrated in Figure (1.1)



Figurer 1.1 Information Hiding Classification

. The associated digital watermark closely in the field of hiding information by setting a system efficiently hide because of its importance and a crucial role , providing ways to encrypt the data so that it becomes unreadable to any unauthorized user. There are technical skills that have large capacity to conceal information, but because of some philosophical differences each of these types to hide its own technology, Figureure 1.2 shows the classification of hiding of information technology (Indradip et.al 2102)

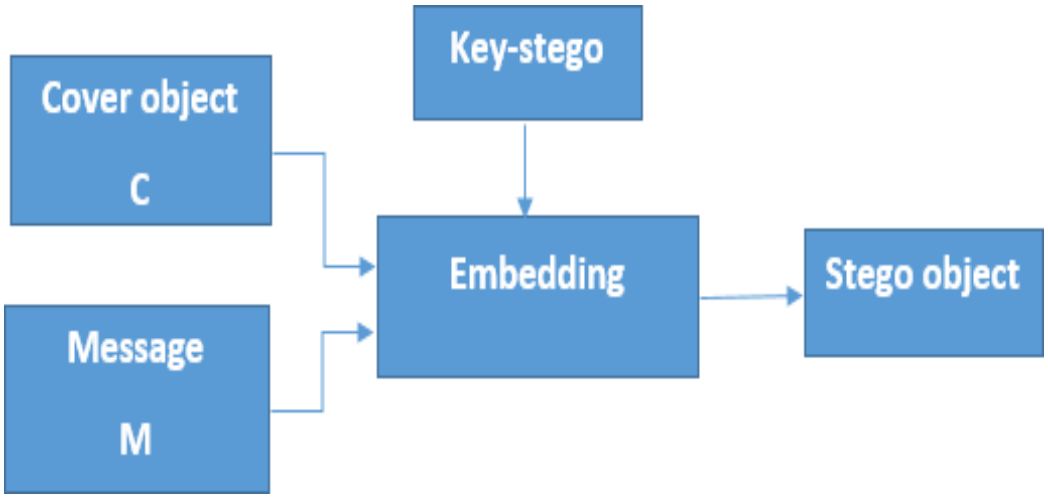


Figurer 1.2 A classification of Information-hiding Techniques (Indradip et.al 2102)

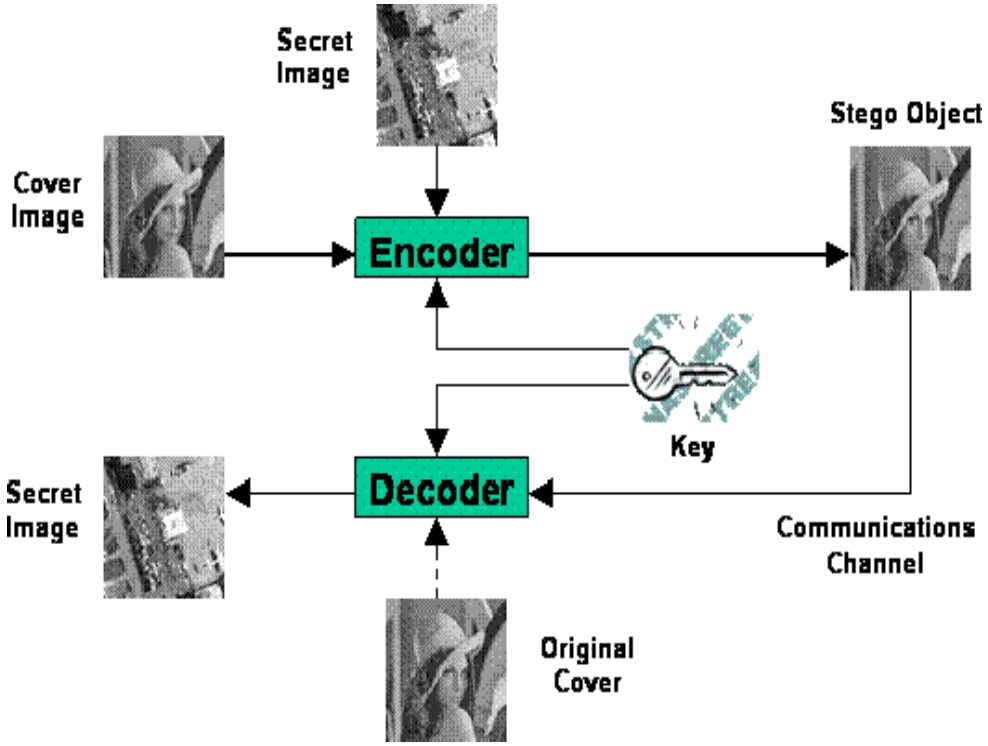
The term Steganography is derived from the Greek words steganos which means "covered" and graphia which means "writing", also it is known as an art the science of communication of hidden information. This concealment is also an evidence of an encrypted message the inclusion of content hidden in media coverage is not noticeable. In a way that does not raise the doubts of the eavesdropper, so people have used this kind of concealment in various forms such as invisible tattoos or invisible ink to transmit content.

Now with the development of computer technology, the use of means of communication and networks as channels of information transmission, it is easy to transfer and store information, including e-mail, voice, video, etc.

In general, the information-hiding process in a stenographic system starts by identifying the cover medium's redundant bits (those that can be modified without causing damage to the intermediary content) (Provos, N., & Honeyman, P.2003). The process of hiding information by a steganography is illustrated simply as in the diagrams Figureures 1.3& 1.4 (Sharma Manoj Kumar & P. C. Gupta.2013).



Figurer 1.3 Steganography embedding process Model



Figurer 1.4 Generic process of encoding and decoding (Awad, Amma 2017)

The digital watermark is widely used to protect copyright in all images, audio recordings, and videos. The rapid growth of the Internet in the easy transport of audio and video has dictated the need to solve the problem of copyright protection. Therefore, the integrity and reliability of the production of information is one of the most important digital factors of the multimedia. From here, the achieved research and studies conducted about the concealment of information to ensure copyright have multiplied in digital watermark technology (Cayre, F., Fontaine, C., & Furon, T.2005)

Figurers 1.5 and 1.6 illustrate the process of watermarking (Sharma Manoj Kumar & P. C. Gupta.2012)

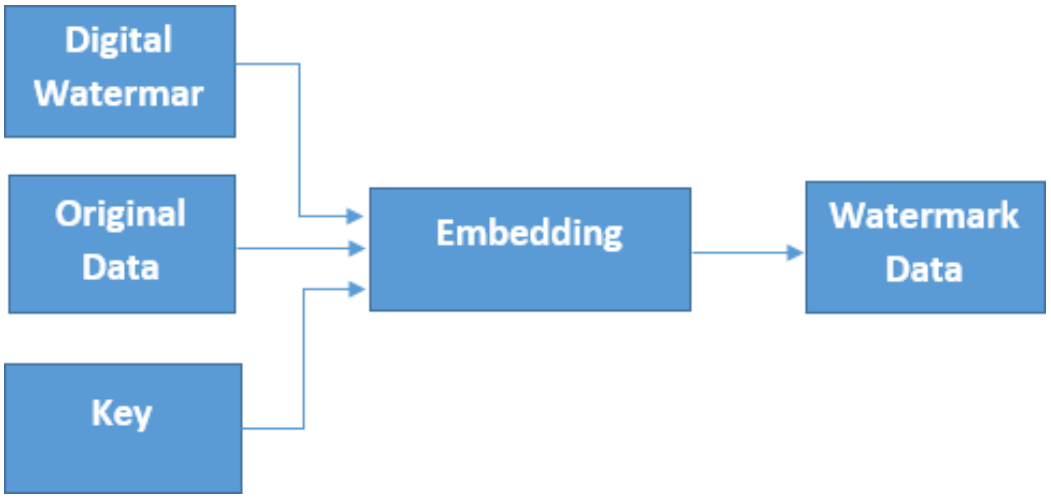
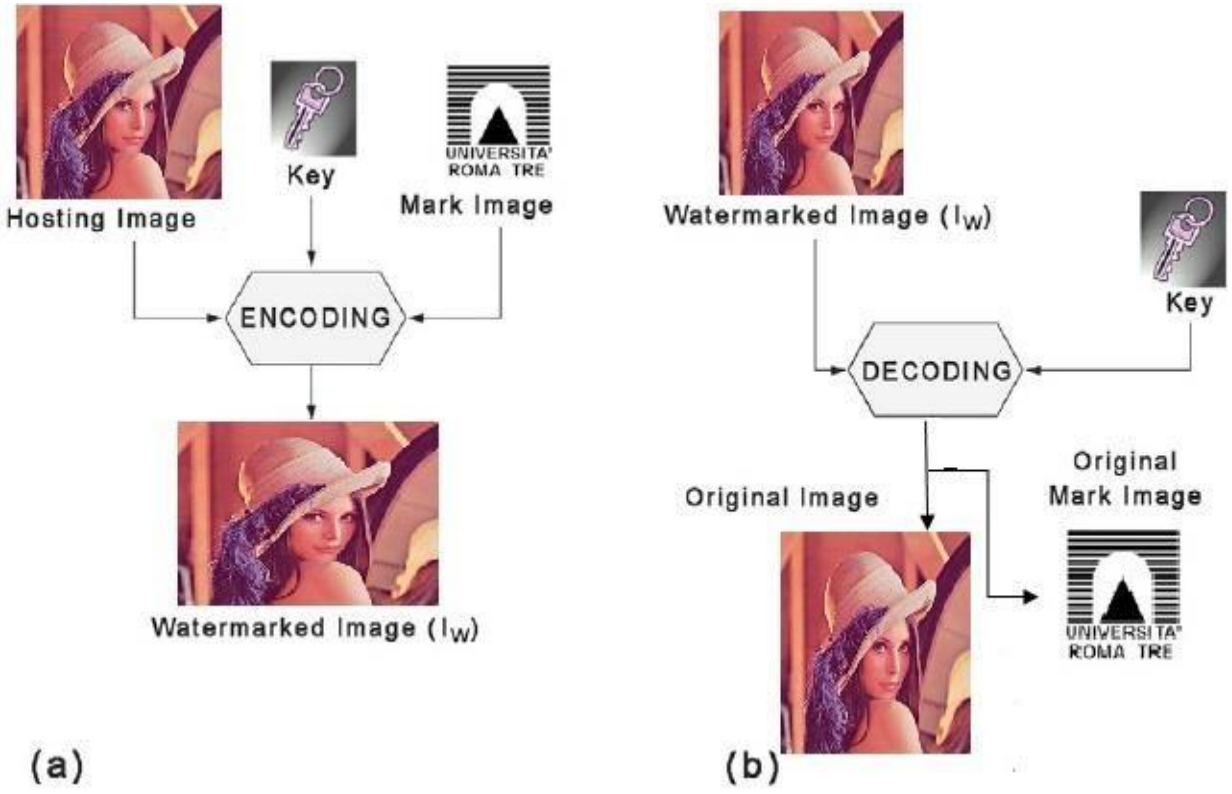


Figure 1.5 Watermarking embedding Process Model (Sharma Manoj Kumar & P. Gupta.2012)

The extraction of the watermark is exactly the inverse process of the embedding**.**



Figurer 1.6 Generic process of encoding and decoding (Spagnolo G. S. et.al 2005).

1.4 : Steganography vs. watermarking

In the following, a detailed comparison of steganography and watermarking techniques for various criteria is listed in Table (Yusof yunsita, khalifa Othman.o 2007) (T. Morkel et.al 2005).

Table (1.1) Comparison between Steganography and Watermarking for various criteria.

Steganography	Digital watermarking
Stenographic communication is usually point-to-point or one to one. The end result of the extracted image is called“ stego-file”.	Watermarking techniques are usually one to many points, The end result of the extracted image is called “watermarked file”.
Steganography tools hide large blocks of information.	Watermarking tools place less information
Steganography conceals a message where hidden message is the target of the communication.	Digital watermarking extends some information that may be considered attributes of the cover such as copyright.
It is invisible to the human eye, and must not be known.	It is not always to be hidden as some system use visible, but most system use invisible.
Steganography system just hides any information in “any media” text file, audio, video etc.	It is associated to the digital object.
Concerned with detection of hiding message, it is not robust against modification.	Concerns potential removal by a pirate, it should be more robust to attacks.

1.5 Statement of the Problem

Many digital watermarking techniques are utilized to hide secret information in the carrier image in order to achieve copyright protection and data authentication. Also development of multimedia transport over the Internet has increased to a wide range of applications such as business, industry, education and other fields. This has raised the problem of protecting the right of ownership of digital images and videos (Kaur .M et.al 2012).

With the emergence of many malicious attacks and actions that would destroy or claim ownership of copyright or attack modify and manipulate with original data , across Internet all data transfers are subject to this, so there is great interest in providing research and studies through which to provide an efficient system that works to give robustness, prevents any theft or modification, as well as provides good imperceptibility to transfer information without arousing the attention of the eavesdropper.

Overcoming these problems through the digital watermark technology involves embedding the watermark in the form of a signature or logo in media that is protected and the data contained either visible or invisible depending on the application used. This research focuses on the invisible watermark of the fixed images and use transformation technique, The transform technique is complex but gives better robustness .The algorithm in this thesis, will present a suitable solution to overcome the problem of attacks after transmitting image through the internet or after performing some image operation like compression, skewing or cropping. Therefore, there is an essential need to propose a new improvement of digital watermarking using Discrete Wavelet Transform (DWT) techniques that is robust against different types of attacks. The extracted watermark is required to be clear and can be easily recognized without any distortion.

To make sure of strength watermarking image, it should be robust against various kinds of attacks such as JPEG compression, filtering, rotation, scaling, cropping, collusion, Gaussian noise, salt and paper and blurring, which will be taken in this study to determine the strength of the image extracted.

1.6 Questions of the study

1. Is it possible to design algorithm scheme that enhances imperceptibility and robustness at the same time?
2 Dose the proposed tools produce an integrated system that produces a robust watermark technique?
3 What would be the effect of the environment on the watermark such as rotation, and cropping?
4 How do the vectorization and inverse phases of the DWT affect the system behaviors?
5 How would our design be compared with traditional discrete wavelet transforms (usual) watermarking techniques?
6 How would the parameter such as Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC), and Structural Similarity Index (SSIM) are effected in the improved robustness?

1.7 Objectives of the study

The main objectives of this study are:

1. Propose a new modification of robust watermarking algorithm based on the concept of segmentation of both the watermark and the carrier image with the employment of a frequency domain technique, such as the discrete wavelet transform (2D-DWT).

2. The new technique aims to achieve a high level of robustness and low image quality degradation.
3. The suggested algorithm is sought to be efficient for both embedding and extraction by implementing a divide and conquer strategy.
4. The performance of the system should be tested against various types of image attacks.

1.8 Motivation

The main importance of the thesis system is the Imperceptibility and Robustness of watermarking technique by using the frequency domain which is most commonly used than other techniques (i.e. discrete wavelet transform). In addition to use segmentation techniques in carrier image and vectoriztion in image logo tool plays the most important part in this study in order to prevent illegal manipulation and distribution of the digital image. Although there are many ways to protect the images, the proposed system in thesis introduces an enhancement approach to protect the image for the purposes of copyright, ownership of intellectual property.

1.9 scope of the study

The digital watermark is a modern means of protecting the copyright ownership of the author. The scope of this research includes the inclusion of logos in the images using segmentation for each of the logo and the carrier image. Also, the work is limited to the use of transform domain technology such as discrete wavelet transforms (2-level DWT), the study the effect on the Robustness and Imperceptibility of the extracted image.

Also quantify the improvement in this study and compare result with the other methods for information embedding and extraction, by measuring PSNR, MSE and NCC. The use of these measures is for the possibility of identifying the strengths and weaknesses that appear on the test to be reported in this study.

1.10 Thesis Organization

The thesis contains four chapters In addition to the first one. It's organized as follows:

Chapter 1 given history of the watermark as well definition of steganography and watermarking techniques and some comparison between them then stated the problem statement, project objectives, motivation and goals.

Chapter 2 Provides the Theoretical Literature and Previous Studies of watermarking techniques along with listing and explaining different related works that is most related to proposed system.

Chapter 3 describes in detail the system methodology architecture and the different models and algorithms for the traditional method and proposed method using segmentation with discrete wavelet transform-2 level technique that are used in all parts of the system.

Chapter 4 The Experimental results of the designed system are presented and discussed in detail.

Chapter 5 Includes conclusions and future work including recommendation.

Chapter Two

Theoretical Background

and Literature Review

Chapter Two

The Theoretical Background and Literature Review

2.1 Introduction

Recently, great interest in the watermark is noticed. The reasons for the increased concern about the copyright protection for the content with the use of the Internet become more need to the development of new ways to improve the protection of these rights. (Khanzode, P et.al 2011).

This chapter presents definition and description of digital watermarking and its importance, theoretical background, literature review classification, applications, various attacks and finally related work for watermarking techniques.

2.2 Digital Watermarking

A watermark is an act of masking data in a host media in such a way that it is inconceivable and can only be separated by an authorized user. It is required to be resistant to many intentional and unintentional intrusions and attacks because these attacks may cause them to deteriorate or damage to host media (Abbate, J.1999).

Watermarking is not a new technique. It is descendent of a technique known as steganography which has been in existence for at least a few hundred years. Steganography is a technique for concealed communication. In contrast to cryptography where the content of a communicated message is secret, in steganography the very existence of the message that is communicated is a secret and its presence is known only by parties involved in the communication. Steganography is a technique where a secret message is hidden within another unrelated media and then communicated to the other party.

Some steganography techniques like the use of invisible ink, word spacing patterns in printed documents, coding messages in music compositions, etc., have been used by military intelligence since the times of ancient Greek civilization (Abou Ella Hassanien 2006).

Watermarking can be considered as a special technique of steganography where one message is embedded in to another and the two messages are related to each other in some way. The watermarking are the presence of specific patterns in currency notes which are visible only when the note is held to light and logos in the background of printed text documents that most common examples. The watermarking techniques prevent forgery and unauthorized replication of physical objects (Abou Ella Hassanien 2006).

The difference between a digital and physical watermark is that digital uses digital content instead of physical objects that was commonly used. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark and it depicts some metadata, but the low-energy signal is called watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format, like security or rights information about the main signal (Preeti Gupta 2012).

The digital watermarking system essentially consists of a watermark embedder and a watermark detector (see Figure 2.1). The watermark embedder dose the watermark insertion into the cover signal and the watermark detector detects the presence of watermark signal in the watermarked cover signal (Preeti Gupta 2012).

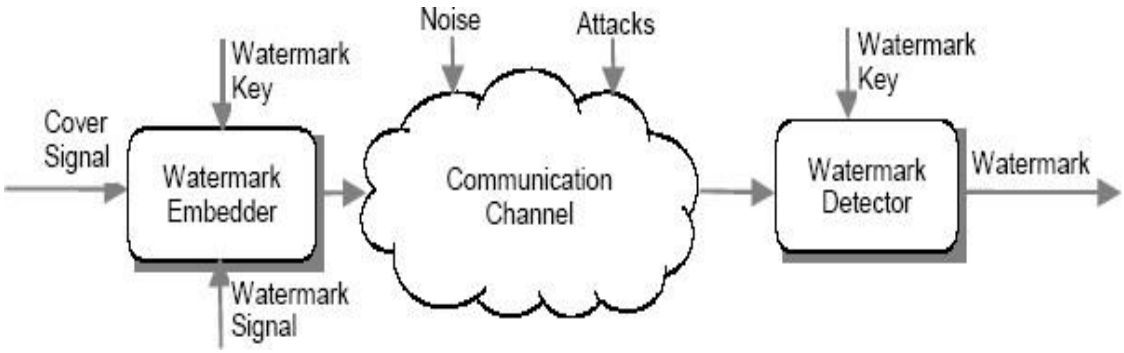


Figure 2.1 Digital watermarking system **(** Preeti Gupta 2012(

Note that an entity called watermark key is used during the processes of embedding and detecting the watermarks. The watermark key and watermark signal has a one-to-one correspondence together (i.s., a unique watermark key exists for every watermark signal).

The watermark key is private and known to only authorized personnel (one or more) and it ensures that only authorized personal can detect the watermark (Er-Hsien Fu, 1998).

The digital watermark includes properties shown below (Er-Hsien Fu, 1998):

1) A digital watermark should be perceptually invisible to prevent obstruction of the original image.
2) A digital watermark can be either statistically invisible so it cannot be detected or erased, or visible to publicly declare the copyright and ownership.
3) The detection process requires too much time or computation. So prefered Watermark extraction should be fairly simple.

4) Watermark detection should be accurate. False positive, the detection of a non-marked image, and false negative, the non-detection of a marked image, should be few.
5) Numerous watermarks can be created. Otherwise, only a limited number of images may be marked.
6) Watermarks should be robust to filtering, additive noise, compression, and other forms of image manipulation.
7) Proof of the true owner of the image is that the watermark embedded within it is able to determine ownership.

2.3 Importance of digital watermarking

The sudden increase in the watermark attention is most likely due to the increase in concern over copyright protection of content. The internet became fundamental being an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However content owners also see a high risk of piracy.

The first technology owners turn to is cryptography. Cryptography can protect in transit, but once decrypted, then the content has no further protection. Thus, there is a strong need for an alternative or complement to cryptography:

There are three important ways to distinguish watermark technology from others. First, watermarks are imperceptible. Second, watermarks are inseparable from the works in which they are embedded. Finally, watermarks undergo the same transformation as the works, i.e. these three attribute make watermarking invaluable for certain application (M. Antonini at el 1992).

2.4 Theoretical Background

Digital watermark techniques are methods used for hiding some data in the form of data or messages W in some form of data or multimedia (cover) C in order to obtain new data C' after it is included using a specific secret key K to ensure the confidentiality of the information that has been hidden, The principles of hiding the message is a one-to-many communications (Goyal, R., & Kumar, N.2014).

Various of Digital watermarking can be listed as follows

- Robustness
- Imperceptibility
- Security
- Verifiability
- Capacity and data payload
- Computational cost
- Watermark detection
- Blind or non-blind detection of watermark
- Tradeoff between performance factors

2.4.1 Watermarking Classification

Digital watermarking can be classified into various types. This section focuses on the domains used for embedding the watermark data (Goyal, R., & Kumar, N.2014).

- First; watermark techniques can be divided in to four groups depending on the type of data to be embedded.

- Text watermarking
- Image watermarking
- Video watermarking
- Audio watermarking

- Second; based on human perception: watermarking algorithms are divided in to two categories; visible watermarks and invisible watermarks, see Fig (2.2).

Visible watermarks:- If the watermark is an integral part of the data in a way that it can be seen by the human eye and without extraction, it is called “visible watermark”.

Logos that style are visual (we can see them clearly) indicating the publisher, which are inserted into or overlaid on images (or video), very similar to visible paper watermarks. They are mainly applied to images.

Logos are placed on images, but when are visible to determine user ownership, and are often placed by institutions as a copyright symbol ("©") as in the case of visual imaging agencies such as satellite channels and others. One of the disadvantages is that it is easy to detect by visual means and does not require disclosure of dedicated programs or devices for that.

The visual tag is often applied to program interfaces, maps, and graphics to keep them from theft and to ensure publisher ownership (F. Hartung and M. Kutter, 1999).

Invisible watermark: is hidden in the multimedia content. It can be detected by an authorized specialist only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copies.

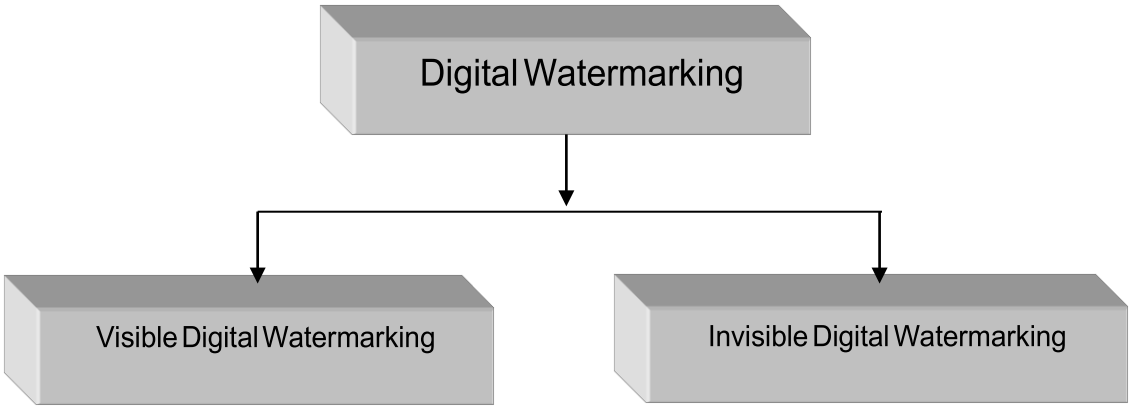


Figure 2.2 Watermarking Types

The watermark, which is an integral part of the data without being seen or affecting the content and can be extracted only by the owner who is authorized to do so, it is called an "invisible watermark", for example the distribution of images over the Internet. The watermark here, which cannot be seen by the human eye, is to ensure copy protection against theft and to protect property rights, and used for ownership judgment (Yeung M& Holliman M ,2002).

- Third; the watermarks are classified according to the information detection) Abdullatif, M 2014) :
    - **Private Watermarking** (also called non- blind watermarking) systems require at least the original data. A private watermark is one embedded using a secret key. The key acts as a selection channel, engineering robustness through the secrecy of this information.

- **Semiprivate Watermarking** (or semi-blind watermarking) potential applications of semiprivate watermarking are to prove ownership, copy control in applications such as digital versatile (video) disc (DVD).
- **Public Watermarking** (referred to as blind or oblivious watermarking) it remains the most challenging problem since it requires neither the secret original nor the embedded watermark to recover the watermark. Indeed such system really extracts bits of information (the watermark) from the watermarked object.

2.4.2 Watermarking Application:

Watermarking can be used in a wide variety of applications. Several applications that can be implemented with watermarking are described here.

1. **Broadcasting monitoring**：

Watermarking is an obvious alternative method of coding identification information for active monitoring. It has the advantage of existing within the content itself, rather than exploiting a particular of segment of the broadcast signal, and is therefore completely compatible with the installed base of broadcast equipment, including both digital and analog transmission. There is also a concern, especially on the part of content creators, that the watermark may degrade the visual or audio quality of the work (Cox, I.J.at el 2000).

2. **Owner Identification :**

Because watermark can be made both imperceptible and inseparable from the multimedia that contains them, they are likely to be superior to text for owner identification. If users of works are provided with watermark detectors, they should be able to identify the owner of a watermarked work, even after the work has been modified in ways that would remove a textual copyright notice (Cox, I.J. at el 2000) (Prabhishek Singh, R S Chadha 2013).

3. **Proof of Ownership:**

Today, the modern digital watermark is a wide spread method that makes a published work unique so that it can be identified automatically. To achieve the level of security required for proof of ownership, it is probably necessary to restrict the availability of the detector. When an adversary does not have a detector and with the help of an unsuspicious mark, removal of a watermark can be made extremely difficult and pirates can easily and inexpensively be caught and prosecuted (A. Nikolaidis at el 2001).

4. **Transaction Tracking :**

In this application of watermarking, the watermark records one or more transactions that have taken place in the history of the copy of a multimedia in which it is embedded. In literature on deal follow up, the person responsible for misuse of a work is sometimes referred to as a traitor, whereas a person who receives the multimedia from a traitor is a pirate (I. J. Cox , M. L. Miller 2002).

5. **Content Authentication :**

In authentication application, the objective is to detect modifications of the data. An exact authentication system seeks to verify that a multimedia has not been changed at all. This can be achieved by a low-level robustness method called fragile watermarks. A selective authentication system seeks to verify that a multimedia has not been modified by any of a predefined set of illegitimate distortions, the approach designed to do this is called semi-fragile watermarks.

2.4.3 Watermarking Techniques

Watermarking techniques can be classified in to three types; spatial domain (time domain), transform domain (frequency domain), and Spread Spectrum.

These three types are described in the following:-

2.4.3.1. Spatial Domain:

This watermark technique is based on or depends on the dissemination of watermark data to be included in pixel values. This approach uses the spectral changes of the density of pixel values. The simplest example of this technique is to include the watermark in the least significant bits (LSB) of the image pixels (Goyal, R., & Kumar, N.2014).

In other words, large parts of the low frequency of the image should be modified in a way that makes it more reliable and powerful, some LSB applications are embedded by splitting the image into blocks, and then a certain watermark data is added to the blocks by some procedures.

A. Least Significant Bit Technique (LSB)

This technique is the most well-known image hiding technique. **LSB** modification techniques are an easy way to embed information. An attacker can simply apply signal processing techniques in order to destroy the secret information.

This method is an easy and effective to hide information within an image, it works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in JPEG image for example, the following steps needed to be taken:

1- Load up both the host image and the image that need to be hidden (signature or logo).

2- Choose the number of bits you wish to hide the secret image in. The more bits to be hidden in the host image, the more deteriorates into the quietly of the host. Decrease the number of bits used in host image has a beneficial reaction on Increase the strength of the secret image and clarity.

3- A new image is created by combining the pixels of both images. For example, if 4 bits of the secret image are used to be hidden in a pixel, there will be four bits left for the host image only.

4- To get the original image back the user just need to know how many bits were used to store the secret image. Then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change, the bits extracted now become the most significant bits.

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed, and

an example of a hidden image with this technique through the least significant bits used to store text or even a small amount of sound. All you need to do is change how the least significant bits are filled in (C. C. Chang at el 2003) (Bamatraf A. at el 2011).

2.4.3.2 Frequency Domain

It is also called transform domain. Values of certain frequencies are altered from their original values. Frequently, these frequency alterations are done in the lower frequency levels, since modifications at the higher frequencies are lost during compression. The watermark is applied to the full image so as not to be removed during a cropping operation. However, there is a tradeoff with the frequency domain technique. Verification can be difficult since this watermark is applied indiscriminately across the whole image (P. Vandewalle at el 2006).

The frequency domain has an advantage over the spatial domain in that frequency-based schemes “spread the watermark over the whole spatial extent of the image, and is therefore it is less likely to be affected by cropping”.

In contrast to the spatial-domain-based watermarking, frequency-domain-based techniques can embed more bits of watermark and are more robust to attacks; thus, they are more attractive than the spatial-domain-based methods (Pintelon, R. at el 1994).

The most important techniques used in this transform domain are: - Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD) and Discrete Furrier Transform (DFT). The first two techniques are briefly defined in the following. Table (2.1) list some show comparison between Spatial Domain and Frequency Domain (Jiang Xuehua 2010) (Mahmoud El-Gayyari 2006).

2.1 Comparison between spatial and Frequency domain

Factors	Spatial domain	Frequency domain
Robustness	Fragile	More Robust
Computation Cost	Low	High
Computational complexity	Low	High
Capacity	High	Low
Computational Time	Less	More
Perceptual quality	High control	Low control
Example of Application	Mainly Authentication	Copy rights

A. Discrete Cosine Transform (DCT)

The cosine transform like the Fourier transform uses sinusoidal basis function. The difference is that the cosine transform basis functions are not complex, they use only cosine functions. The cosine transform yields better performance that the DFT (Discrete Fourier Transform) for all positive values (R M Goudar & Priya Pise 2012).

The DCT has a better energy compaction property and it has useful property of matching highly correlated natural image signals and also has interesting properties if such algorithms are considered as they are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. Besides, they are weak at the same time against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually

important section of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image (Potdar V. at el 2005).

B. Discrete Wavelet Transform (DWT)

The basic idea in the DWT for one dimensional signal is the following a signal is decomposed into two parts, usually high frequencies and low frequencies parts. The edge components of the signal are largely confined to the high frequency part. The low frequency part is decomposed again into two parts of high and low frequencies. This process is continued until the signal is entirely decomposed or stopped before by the application at hand. For compression and watermarking applications, practically no more than five decomposition steps are computed. Furthermore, from these DWT coefficients, the original signal can be reconstructed. The reconstruction process is called the inverse DWT (IDWT). The DWT is applied independently to the image components and de-correlates the image with respect to different length scales, preserving much of its spatial correlation (Potdar V. at el 2005) (Singh A.K at el 2015).

2.4.3.3. Spread Spectrum

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original un-watermarked image and verification of watermark presence relies on the cross correlation between extracted watermark and original watermark. Also it is used to embed the watermark in the frequency components of the host image. First, Fourier Transform is applied to the host image. It is inserted to obtain the

modified values. (Chopra, D et.al 2012) . Experimental results showed that this method resists JPEG compression (Inbarasan, M at el 2015).

2.5 Properties of Watermarking:

Watermarking system can be characterized by a number of properties. The relative importance of each property is dependent on the requirement of the application and the role the watermark will play. Some of these properties are embedding effectiveness, transparency, fidelity, data payload, blind or informed detection, false positive rate, robustness, security, key, and cost.

1. **Transparency:**

   Refers to whether the watermark is perceptible or imperceptible to a human. Imperceptible watermarks are used such that the content appears the same after the watermarking process has been applied. Alternatively, perceptible watermarks are intentionally left visible—to some degree—to the human sensory organ. However this technique makes it very easy to find and remove the hidden data (L. Jian and H. Xiangjian, 2005).

2. **Embedding Effectiveness:**

   A watermarking work is a work that when input to a detector results in appositive detection. With this definition of watermarked work, the effectiveness of a watermarking system is the probability that the output of the embedder will be watermarked (Abdullatif, M at el 2014).

3. Fidelity:

Fidelity of a watermarking system is the perceptual similarity between the unwatermarked and watermarked image at the point when they are presented to a consumer. A watermark is said to have high fidelity if the degradation it causes is very difficult for a viewer to perceive. However, it only needs to be imperceptible at the time that the media is viewed (Abdullatif, M at el 2014).

4. Data Payload:

Fundamentally, the capacity or data payload of a watermark is the amount of information it contains, or the size of information that can be hidden relative to the size of the cover. As with any hiding method data payload (this can be expressed as a number of bits) indicates the number of distinct watermarks that might be inserted into the image (L. Jian and H. Xiangjian, 2005).

5. Blind or Informed Detection:

Informed detector refers to a detector that requires access to the original, unwatermarked work. This term can also refer to detectors that require only some information derived from the original work (Abdullatif, M at el 2014).

6. False Positive Rate:

A false positive is the detection of a watermark in a work that does not actually contain one. When we talk of the false positive we expect the watermark to occur in a given number of runs of the detector (I. J. Cox and M. L. Miller 2002)

7. **Imperceptibility**:

The embedded watermarks are imperceptible both perceptually as well as statistically and do not alter the aesthetics of the multimedia content that is watermarked. The watermarks do not create visible artifacts in still images, alter the bit rate of video or introduce audible frequencies in audio signals

8. **Robustness:**

Robustness determines the algorithm behavior towards data distortions introduced through standard and malicious data processing. The embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition (F. Hartung and M. Kutter, 1999).

Not all watermarking applications require robustness to all possible signals processing operation; rather a watermark need only survive the common signal processing operations likely to occur between the time of embedding and the time of detection. Clearly this application is dependent. For example, in television and radio broadcast monitoring, the watermark need only survive the transmission process (Abdullatif, M at el 2014). In some cases, robustness may be completely irrelevant, or even undesirable. In fact, an important branch of watermarking research focuses on fragile watermark. A fragile watermark is one designed so that it is not robust.

To improve robustness, it may be necessary to reduce the size of embedded data and embed it multiple times under different parts of selected coefficients, where

each embedding responds to a particular attack in a different way (Mahmoud El-Gayyari, 2006).

9. Security:

A security of a watermark refers to its ability to hostile attacks. A hostile attack is any process specifically intended to thwart the watermark purpose. This is a description of how easy it is to intentionally remove a watermark-referred to as an attack. These attacks refer to detection, modification or burying of the watermark in another illicit one. In the case of imperceptible watermark requires knowledge of embedding algorithm used. (Mahmoud El-Gayyari, 2006)

10. Key:

Watermark algorithms can be designed to use keys in a manner similar to that in spread spectrum. Ideally, it should not be possible to detect the presence of a watermark in a work without knowledge of the key even if the watermarking algorithm is known. It is often desirable to use both forms of keys in a watermarking system. That is, message is first encrypted using one key, and then embedded using a different key (F. Hartung and M. Kutter, 1999).

11. Cost:

The economics of deploying watermark embedders and detectors can be extremely complicated and depends on the business models involved. From a technological point of view, the principal issues of concern are the speed with which embedding and detection must be performed and the number of

embedders and detectors that must be deployed. Other issues include-purpose hardware device or as software application. In general, the more numerous a device needs to be for a given application the less it must cost (Prabhishek Singh and R S Chadha , 2013).

2.6 Purpose of Digital Watermarking

Watermarks added to digital content serve a variety of purposes. The following list details six purposes of digital watermarking: (Prabhishek Singh and R S Chadha 2013) (F. Hartung and M. Kutter 1999) (L. Jian and H. Xiangjian 2005).

1- **Ownership Assertion**: to establish ownership of the content.

2- **Fingerprinting**: to avoid unauthorized duplication and distribution of publicly available multimedia content. (I.e. images)

3- **Authentication and Integrity Verification**: The author owns a single key related to the content so that he can verify the integrity of that content by extracting the watermark, which is known as authentication to verify the integrity of the content.

4- **Content Labeling**: bits embedded into the data that gives further information about the content such as a graphic image with time and place information.

5- **Usage Control**: It is added to limit the number of copies created whereas the watermarks are modified by the hardware and at some print would not create any more copies (i.e. DVD).

6- **Content Protection**: content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

2.7 Watermark attacks:

The watermarking attack is the art to remove or disable the watermark. An attacker wants to eliminate (or degrade) the effectiveness of the content owner's mark, which was inserted to protect the owner's claims, and control the watermarked content.

The types of attacks fall into three broad categories: (Cox I.J., at el 2000) (A. Nikolaidis at el 2001)

- **Unauthorized removal**: a form of attack in which an adversary, who should not be permitted to remove watermarks, nevertheless succeeds in removing one. This can take the form of either a masking attack or an elimination attack.
- **Unauthorized embedding**: a form of attack in which an adversary, who should not be permitted to embed valid watermarks, nevertheless succeeds in embedding one.
- **Unauthorized detection**: a form of attack in which an adversary, who should not be permitted to detect and/or decode watermark, nevertheless succeed in detecting or decoding one.

  Unauthorized removal and embedding are referred to as active attacks because these attacks modify the cover work, while unauthorized detection does not modify the cover work and is therefore referred to as a passive attack.

2.7.1 Some significant known attack:

There are many known attacks on the security of watermarking systems (Cox I.J. at el 2000) (Preeti Gupta 2012) (Prabhishek Singh and R .S .Chadha 2013).

1. **Scrambling attacks**: It is a system level attack, in which the samples of a work are scrambled prior to presentation to a watermark detector and then subsequently descrambled. The degree of scrambling necessary depends on the detection strategy. The only constraint is that the scrambling be invertible or near invertible. A near invertible or lossy scrambling attack should result in a work that is perceptually similar to the watermark work.

It's known scrambling attack is the mosaic attack, in which an image is broken into many small rectangular patches, each too small for reliable watermark detection. More general scrambling attacks require the receiver of the pirated works to obtain a descrambling device or program.

2. **Pathological distortions**: any process that maintains the sincerity of the work could be used by an adversary to circumvent the detector by masking or eliminating the watermark. The two most common pathological distortions are:

   - Synchronization attacks.
   - Linear filtering and noise removal attacks.
   - Copy attack: a copy attack occurs when an adversary copies a watermark from one work to another. It is a form of unauthorized embedding. There are particular methods that implement copy attack. It depends on being able to obtain a reasonable approximation of the original work. However,

depending on the watermarking algorithms, there can be other ways of performing a copy attack that do not involve reconstructing the original.

A possible approach to countering copy attack is to use cryptographic signatures that link the watermark to the cover work.

- **Ambiguity attacks**:

  Ambiguity attacks create the appearance that watermark has been embedded in a work when in fact no such embedding has taken place. An adversary can use this attack to claim ownership of a distributed work or even the original work. As such ambiguity attack can be considered a form of unauthorized embedding.

- **Ambiguity attack with informed detection**:

  The ambiguity attack works against systems that use an information detector. The adversary defines his fake watermark to be randomly generated reference pattern. He/she then subtracts this pattern from the watermarked work that the original has distributed, to create his fake original. Thus, a situation is created in which both the original owner and the adversary can make equal claims of ownership.

2.8 Related Work

This section illustrates a number of related works in order to determine the major research techniques and methodologies used in this thesis. Since this research project is concerned with discrete wavelet transform, therefore the following literature survey describes the previous work done on this frequency domain techniques i.e. using DWT.

- **(Hai Gao et.al, 2001);** Submitted this study mathematical morphology claiming is very attractive for automatic image segmentation because it efficiently deals with geometrical descriptions such as size, area, shape, or connectivity that can be considered as segmentation-oriented features.

  The segmentation process is divided into three basic steps, namely: simplification, marker extraction, and boundary decision. Showed the results to used three basic steps as follows:-

  * The first step has removed the troublesome components of the image while kept the basic components.

  * The second step simplifies the definition of flat surfaces; (marker-extraction) output indicates that there are homogeneous areas that are difficult to define accurately.

  * The third and final step determines the last limits of the object / shape accurately and easily in dealing with it.

  This study shows that segmentation technology is strong when not unsupervised, and also the study also gave very good results in the use of spatial segmentation technology.

- **(Shahinfard, E., & Kasaei, S. 2003);** To add highly adaptive ability to an image and to enhance the signal in the watermarking, this study provided a robust multi resolution watermarking algorithm. It aims to protect copyright protection of the digital image and be powerful against manipulation and theft, by adapting the watermark signal to wavelet coefficients, in the most important parts of the image. Hence, it increases these parts of the watermark vision using the human visual system to prevent the perceptual visibility of this embedded signal. The

experimental results showed that the algorithm was able to maintain the quality of the image very well and proved its strength towards the most common distortions in image processing.

- **(Ety Navon, et.al, 2005);** this study presents a new method for color image segmentation. The proposed algorithm divides the image into homogeneous regions by local thresholds. The number of thresholds and their values are adaptively derived by an automatic process, where local information is taken into consideration. First, the watershed algorithm is applied. Its results are used as an initialization for the next step, which is iterative merging process. During the iterative process, regions are merged and local thresholds are derived. The thresholds are determined one-by-one at different times during the merging process. Every threshold is calculated by local information on any region and its surroundings. Any statistical information on the input images is not given. The algorithm is found to be reliable and robust to different kind of color images.

- **(Peng, H, et.al, 2010);** the special structure and property of image in multiwavelet domain are applied to design the watermarking algorithm, and a mean value modulation technique is employed to modulate a set of multiwavelet coefficients in approximation sub-bands. In order to robustly extract watermark, support vector machines (SVMs) is used to learn mean value relationship between watermark and coefficients in multiwavelet sub-bands. In addition to the experimental results, the proposed algorithm is robust to common attacks such as JPEG, low-pass filtering, noise addition, rotation and scaling.

- **(Sharma, P., & Swami, S. 2013);** the watermark is based on 3-level discrete wavelet transforms and compared with 1-level and 2-level DWT. This technique can embed the invisible watermark into the image using alpha blending technique which can be recovered by extraction technique. Results shows that the recovered images and the watermark are better for 3-level discrete wavelet transform compared with the 1 or 2- level discrete wavelet transform. Also the quality of the watermarked images are dependent only on the scaling factors k and q (k varies from 0.2 to 2, q is constant), while the recovered watermark are independent on scaling factor.

- **(Abdullatif, M., et.al, 2014);** This study implemented a watermarking scheme using Discrete wavelet transformations by embedding the watermark as 2- level in the diagonal coefficient , which has provided a good level of deception as well as the image of the watermark being strong against the attacks. The experimental results showed high performance in deception and was achieved in embedding the watermark by selecting seeds that generate a series of semi- pseudo random noise, and the same seeds are used to extract the watermark again.

- **(Thanh, T. M., et.al, 2014);** a proposed new domain, called q- DWT. The watermark is embedded in the low-frequency range of q-DWT domain in order to achieve the robustness of watermark. The experimental results shows that it is useful in order to keep the quality of the embedded image and to archive the robustness against common image processing attacks by Employment of quantization index modulation (QIM) technique for embedding due to its high robustness and blindness. The tradeoff of robustness and quality can be controlled

by the quantization parameter Q of QIM and parameter q of the logarithm function.

- **(Divjot,K. & Sonika,J. 2014);** These researchers proposed a new digital video watermark which collect the Discrete Wavelet Transforms (DWT) and decompose the singular value decomposition (SVD).

  The watermark was placed in high frequency sub band and was then exposed to different attacks in order to determine the strength of this algorithm.

  They used a semi-blind outline of the watermark for digital video, which is considered most powerful against the attacks, then, is embedding the watermark into the original frame which protects against attacks that may lead to the fall of the frame in which the watermark was inserted. Several video and input parameters have been tested and results of general observations have been given over the imperceptibility and robustness against various attacks making this scheme suitable for several applications.

- **(Choudhary, R., & Parmar, G. 2016)**: A variable visibility factor is used for the insertion of watermark into the low frequency component of the host image and the implementation of watermarking technique has been done using 2-level DWT. Simulation results show that the feature of the watermarked image and the recovered watermark are dependent only on the visibility factors and also show that the 2-level DWT gives superior results than 1-level DWT. Using the technique of embedding the image of the binary or grayscale watermark in the cover image or for many images as well as in multimedia images where this

technique was implemented for the watermark using the 2- level Discrete wavelet transforms.

- **(Nasrin, M.M, et.al 2016)**; this study aimed to include the digital watermark as confidential data in the digital image without affecting the quality of the visibility. The researchers presented a strong scheme of the block-based watermark and relied on single value decomposition (SVD) as well as the human visual system (HVS) in the field of discrete wavelet transforms.

  It was started by dividing the image into a number of blocks and then choosing a part of these blocks to place the watermark and then the process of embedding the tag and will affect certain logic in the mass. The HVS characteristics of entropy and edge entropy were used to determine the low frequency as the best area for inclusion. Hence, it provides high durability by selecting the most powerful areas, and the use of blind scheme and keys important extraction process using the AES-192 to maintain the information confidentiality.

- **(Shaekh, H. S, at el 2018);** this study is a proposed new digital model applied to medical images. This is done by applying SMQT (Successive mean quantization transform algorithm) used for image enhancement and the image is being segmented using OTSU thresholding. Discrete Wavelet Transform (DWT) and Inverse (IDWT) are used to embed and extract the watermark on the host image. This algorithm was evaluated and tested using a number of measures to determine the safety and privacy of the medical images used.

  The experimental results showed improved performance in terms of imperceptibility and robustness, showed higher PSNR, lower MSE and improved CC values.

- **(Rashmi, J. and Rajneesh, R. 2018);** this study suggested an improved watermark system for the video, which increases the normal correlation coefficient. This makes the system more stringent for common attacks.

  DWT-2 level has been applied to the proposed algorithm for embedding the watermark of the video, frame by frame along with a Gaussian filter, which further improves the properties of the algorithm to place the watermark while reducing the degradation that affects the image quality.

  The results showed that the proposed algorithm proved consistent against most attacks with improved (PSNR) and imperceptibility level.

In this thesis, the author will use a segmentation technique for both, the watermark logo and the host image, implementing a 2- level DWT processes. This study is intended to benefit from the variation of different frequency component contents in different parts of the host image, hence the localization distribution of these contents is taken in consideration, the algorithm design will be outlined in chapter 3 and the results of the implementation and testing will be displayed and discussed in chapter 4.

Chapter Three

The Research Methodology

Chapter Three

The Study Methodology

3.1 Introduction

The watermarking technique using discrete wavelet transforms (DWT) have proved in many studies that it gives results of high robustness and imperceptibility, which draws the attention of many researchers. This chapter presents the traditional and the proposed methods and the mechanism of its work in the traditional way and the proposed. The same tools were used to compare results of the two methods for the purpose of determining the effect of the segmentation on the results that will be presented in Chapter 4.

This chapter begins with basic principles used in this study and gives an idea about DWT in general. The algorithms are presented in the two ways, illustrated by the drawings, and then the focus on the proposed study is explained in a broad and precise manner, also explain steps for embedding and extraction.

Below the techniques used in the proposal study is reviewed:-

3.1.1 Binary image

It is the simplest digital images and contain only one bit per pixel and is monochrome, that is, the value of representation is 0 or 1 (two colors white or black), and where the black is (0) and white (1) are the two colors prevailing in the picture. As an example (Fig 3.1), represents the watermark that was used for inclusion inside the host image of the cameraman.

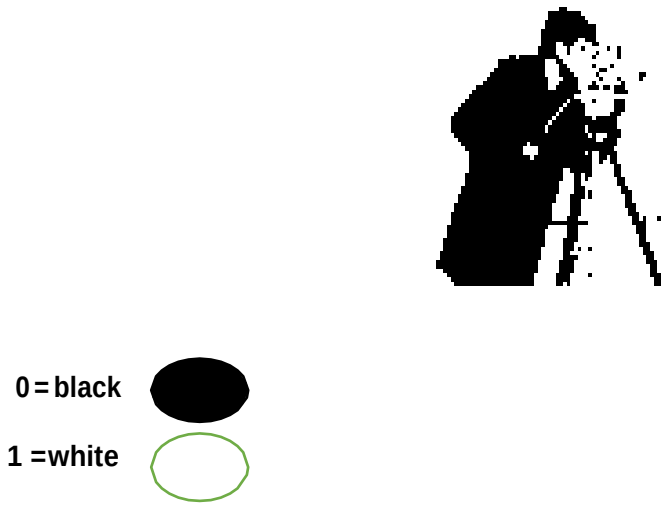


Fig 3.1 Cameraman (Binary image, 1bit/pixel: 2 values [0, 1])

3.1.2 Grayscale image

Is a type of digital image that contains white and black and grayscale and represents its severity as represented by (8 bit / pixel), (12 bit / pixel) or (16 bit / pixel) depending on the color depth where the intensity between the values 0 – 255, , respectively.

The grayscale image contains 256 different gray values and each pixel can then be stored in either 8 bits or (1 byte). A grayscale image representation is illustrated in (Fig 3.2).

Fig 3.2 representation grayscale image value

3.1.3. vectoriaztion

The computer screen is usually represented by bitmap images using a rectangular grid of pixels. Pixels are arranged in rows and columns so that these units of pixels are small and difficult to see by the eye, and can be created in a wide range of shapes and types.

–TIFF (Tagged Image File Format), PNG (Portable Network Graphics), JPG (Joint Photographic Group), GIF (Graphics Interchange Format), and BMP (Bitmap)‖ are the most important Bitmap attributes that are being easy to be used and understandable.

In addition, the research started to search for a technique that increases the accuracy of bitmaps. The starting point for the right option is to convert bitmaps with low precision using vector. The process of converting bitmaps to vector is called vectoriaztion where the pixels are converted into basic geometric shapes such as circles, triangles and rectangles. The use of a bitmap has a number of drawbacks to the representation of graphics on the Internet and from these defects:-

1. Fixed resolution

The bitmap has a fixed resolution, since the image is finely selected so it is difficult to increase scalability. This in turn causes the image to deteriorate when zoomed in or reduced in size, in other words the bitmap scalability is weak.

2. Image size

The image is defined by its size (height and width) and the number of bits assigned to each pixel in the image, which is a kind of threat in the transfer of images stored in this format Figure 3.3.

Illustrates the image resolution and size

(a) **(b)**

Figure 3.3 (a) Flower.bmp (File size: 187KB) (b) Flower.bmp (File size: 3.18MB)

The image in fig (3.1.a) is the original raster image, and that in fig (3.1.b) is the same Raster image when zoomed at 130%. The image gets distorted when zoomed as indicated in the original image was obtained from the internet, (Lai et al 2009).

After reviewing the bitmap, we will mention the most important features of vector image

1. Scaling: One of the important characteristics in the use of this vector property is the possibility of the user to zoom in and out without deterioration in the appearance of the image as the image vector can be enlarged while the image remains soft without distortion. The ability to resize the image is essential in image processing.

2. Storage space: The use of the image vector is an important. Features in that it provides a small storage space if compared with the bitmap, where the useful part of this property is that the mathematical factor accompanying the size of each image is the same in the image of the carrier but its information is less than that of the vector.

3. Color: The vectors have the possibility to make a large area of color with somewhat small file size. This feature is necessary when images have high resolution for this reason, their use is very important.

4. The ability to edit: It is very easy to edit vector drawing. This feature has led to the development of many algorithms that convert colored bitmap to vectors. The ability to edit the image enables users to process other images

5. Image Quality: Highest quality can be obtained using the vector. For example, the image used in the following example, JPG is a bitmap that is often used for photographs. The purpose of optimizing JPG files is to find the perfect balance between small file size and high quality. When you want your image files to be as small as they are easy to handle and do not affect image resolution, they are large enough to appear crisp and not clear .

JPG can not be shown on a transparent background of high quality, but always appear In forms of a rectangle or box with solid background is not clear, but when converted into vectors, the image format and quality can not be affected. Figure (3.4) shows the difference between these two images

(A) **(B)**

Figure 3.4 (A) JPG (bitmap image) (B) vector image (fiverr 2017)

3.1.4 Discrete Wavelet Transform (DWT)

In the second chapter, we discussed briefly the conversion of separate wavelets in general, but here in this chapter we discuss in detail how to analyze the image to the second level which is the level used in the study and the characteristics that distinguish it from other technologies

DWT is one of the frequency domain techniques that improve effective in terms of the imperceptibility and robustness requirements of digital watermarking algorithms. The basic idea of DWT is to separate frequency detail, which in can be improved by increasing the levels of DWT as (2-level DWT, 3-level DWT) so on, also it considered a technology that collects information about frequency and location at the same time, for this reason it is preferred to be used for the rest of the wavelet transform (Darshana Mistry. 2010).

The main idea of DWT is a mathematical tool to analyze the image hierarchically. The image is divided into levels according to the components of the signal. The low-frequency signal which continues to be divided into sub-bands with low and high frequencies, as for high frequencies, it is not splitted again and contains the edge components of the image.

In two dimensional applications for each level of decomposition, it first executes in a vertical direction and then follows the horizontal direction after completing the first level of decomposition. There are 4 sub-bands:

• Low-low (LL) sub band,

• Low-high (LH) sub band,

• High-low (HL) sub bands and

• High-high (HH) sub bands.

Generally, LL band is more significant because it has maximum magnitude of the wavelet coefficient.

The lower resolutions are computationally more effective for watermark detection. So of the energy is concentrated at the lower resolution part of the image. Therefore, the watermark is embedded in the lower part of the cover image and the resulted watermarked image is more robust without losing the quality of the image (Mehta Gaurav. N at el 2012). On the other hand, the high frequency sub bands are not preferred for watermarking.

Furthermore, to recover the image back to the original format after watermark embedding, the reconstruction process is called the inverse DWT (IDWT) (Choudhary, R.,Parmar, G. 2016). Figure 3.5 (A and B) shows the idea of decomposing the image into 2- level DWT.

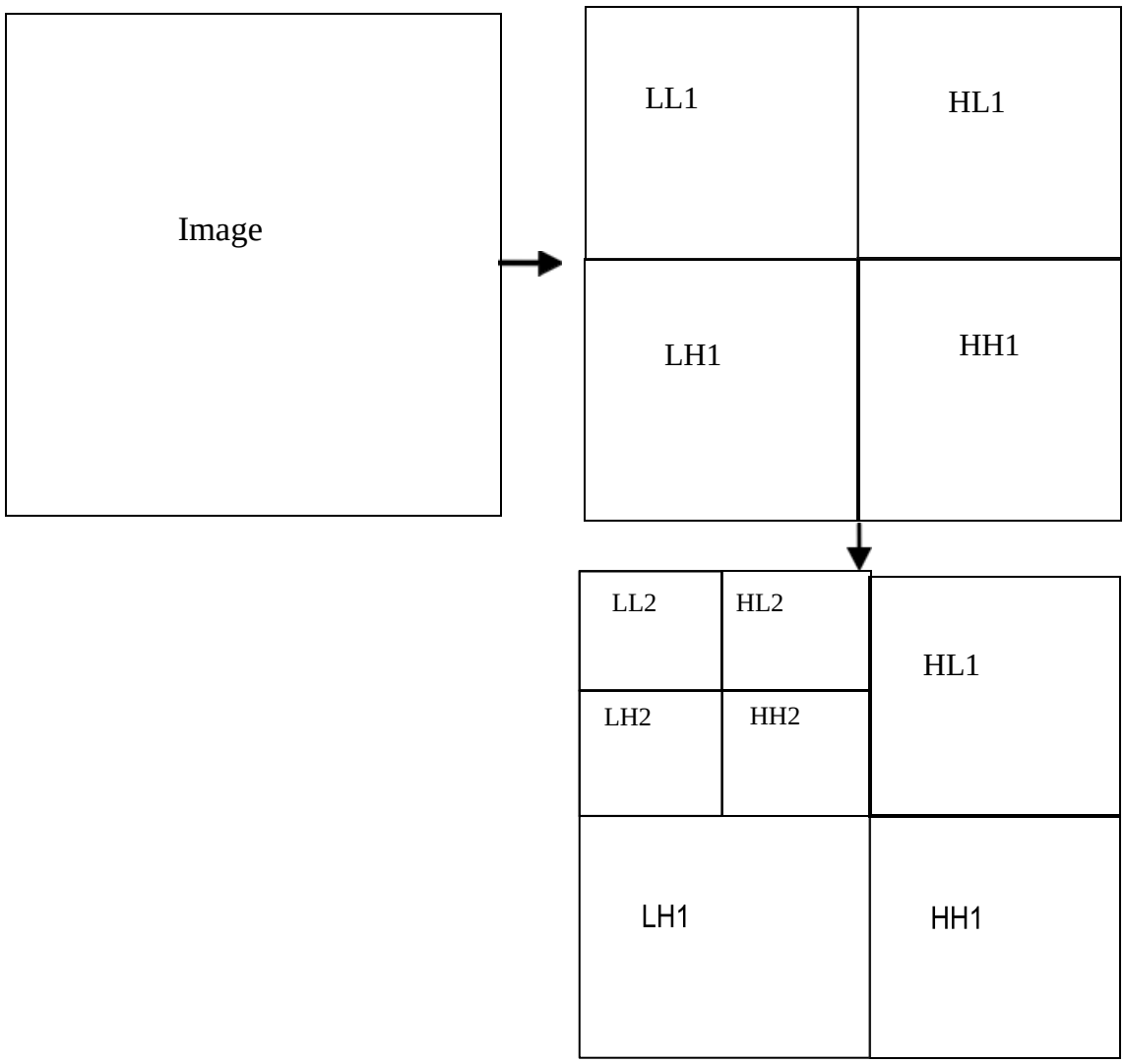


Figure 3.5 A. block diagram for the image decomposition for 2-level (DWT)

Figure 3.5 B. Pyramidal decomposition of Lena image (1and 2 times**)**

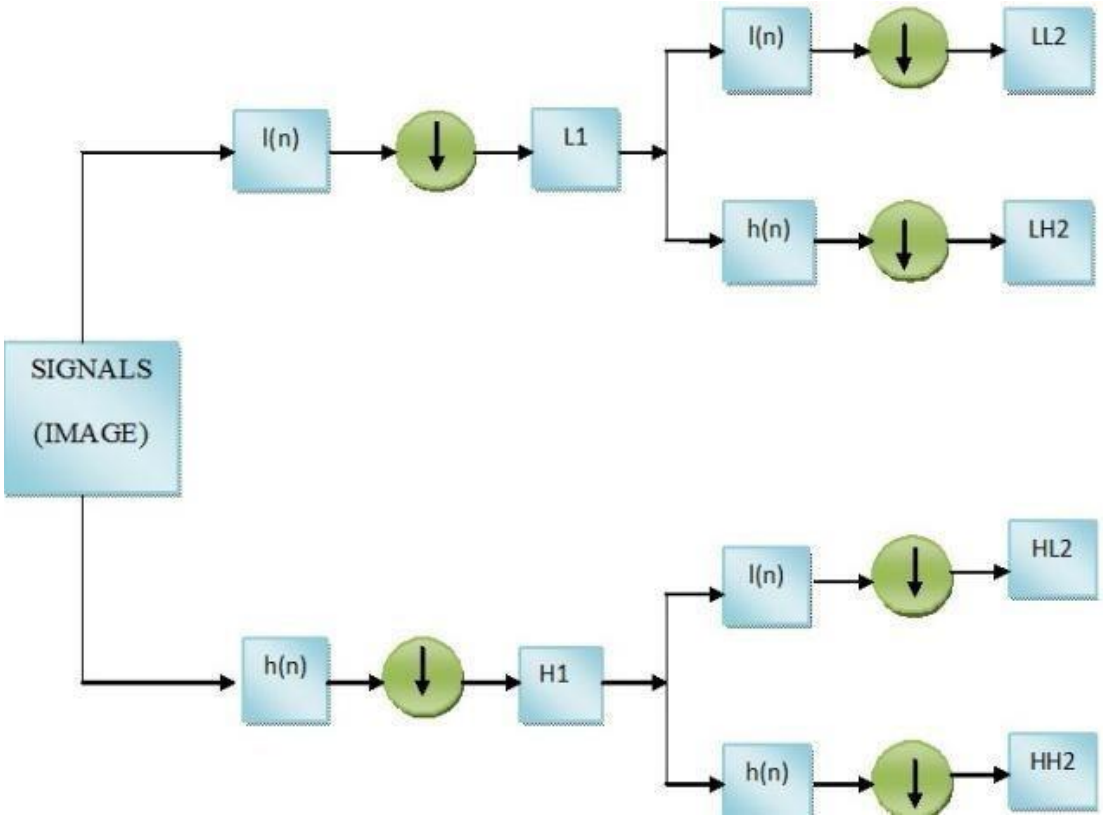


Figure 3.6 One decomposition step of the two dimensional image

(Choudhary, R., Parmar, G. 2016(

Figure (3.6) illustrates the DWT decomposition structure. In the 1-level DWT the size of each part of the divided image is one-fourth of the original image. This represents the decomposition of the image using 2-level DWT.

There are a number of features that have made choosing a DWT useful as compared with other transform, they are:-

i. It's a modern technique that in frequently domain used to process digital images, the property of decomposition to levels that give flexibility in processing.

ii. It has applications in wide areas such as signal processing, compression (audio, video), noise removal, and wireless antenna distribution simulation.

iii. Spatial accuracy of frequencies is high

iv .The wavy transform is achieved in three spatial directions (horizontal, vertical, diagonal) and the waves reflect the different characteristics of the human visual system (HVS) and more accurately.

v.The frequency range is the largest in the lowest band of LL and is the smallest when decomposition levels relative to other bands (HL, LH, and HH), so it is preferable to include the watermark in high-frequency bands because it is computationally more effective.

vi. Provides enough information for analyzing transient and time-varying signals.

vii. Provides spatial and frequency information for measuring information.

viii. The edges and textures in the image are easily defined in high frequency bands

ix. The image is not fully affected if there is a change in conversion transactions because the conversion is not a complete frame as opposed to the rest of the conversions.

3.1.5 Advanced Encryption Standard (AES)

In cryptography, the Advanced Encryption Standard (AES) is an encryption standardized by NIST in 2001 and adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256 published by Rijndael (J. Daemen, V. Rijmen . 2002). Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as a successor for the Data Encryption Standard (DES), which became vulnerable to attacks.

AES was announced by National Institute of Standards and Technology (NIST) at U.S.A Federal Information Processing standards Publications (FIPS PUBS) 197 (FIPS 197) on November 26, 2001 after a 5-years standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable.

AES is one of the most popular algorithms used in cryptography. It is available in many different encryption packages. AES is fast in both software and hardware, it is relatively easy to implement, and requires little memory . AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

Table 3.7 Different keys and its attributes

Algorithm	Key length	Block Size	Number of rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key. (L.Thulasimani & M.Madheswaran, 2010)

3.2 Proposed Watermarking Method

The main idea of this study is to investigate the possible improvement by using segmentation with frequency domain which mainly used in images and Videos because of its robustness and imperceptibility which is the primary requirement of watermarking techniques, whereas spatial domain based watermarking is easily affected by attacks and has a problem in robustness to resist attacks (Ahmad, A. at el 2014).

Before the embedding phase the watermark and the carrier image are segmented into n segments each. These segments are W1, W2 …Wn for the watermark and H1, H2….Hn for the carrier image (host). Then 2D-DWT processes are applied to each segment of the segmented host image, and then each segment of the watermark is embedded the corresponding segment of the host image. This means that (Wi) will be embedded in to the 2D-DWT of (Hi) where i=1, 2…, n.

The watermark is taken as a binary image (PNG) consisting of two colors only (black and white), which one of the simplest types of image, easy to handle in terms of the process of embedding. it is also is used the watermark in different sizes to test it, the Watermark (W) will be segmented into blocked or segments (W1, W2, ..., Wn). The process means partitioning a digital image into multiple segments (sets of pixels). In addition, watermark has a condition:, segment of watermark must be less than the size of the embedding place by 8 times in order to prevent distortion within the host image, if the watermark's size larger than the place, then the process will be rejected .

The goal of segmentation is to simplify and/or change the representation of an image into something that is less complicated and easier to analyze i.e. using the divide and conquer principles. Then, it uses vectoriaztion for each part of the watermark to perform a linear transformation that converts a matrix into a column vector. A vector graphic is made up of points, lines and curves related to one another using mathematical formula. However, a vector image is based on mathematical formula, it can be doubled—or tripled—in a size and still retain crisp, with high-quality details.

Vectorized images can also be edited to change color or shapes of a section without affecting the whole image the segmented, and then encrypt each part using an (AES-128) algorithm using a cryptographic key one (K1) to encrypt each segment and to obtain cipher text before it is included in the host image. The watermarked image or the host image (H) will also be segmented into blocks (H1, H2..., Hn). Before the embedding phase, the segmented host image will undergo 2D-DWT for each segment to produce segmented Host image with 2D-DWT. Then the vectorzed segmented watermark will be embed in segment host image by using new key (K2) for the embedding operation, The aim of using a second key (K2) is to increase the security of the watermark after the embedding process in the host image. The embedding within the host image is inside the sub-bands of HH2, since it a (HH2) contains the large number of difficult transactions of the human eye in perceive.

Thereafter, an inverse discrete watermarking transformation 2D-IDWT is applied to each of the resulting segment in order to restore the watermarked host segment. The watermarked image (Hw) will be inverted by inverse-DWT (2D-IDWT) and recombine the segmented watermark images (Hw). The number of segments that will be adopted for both, (host image and watermark) in the proposed work is included (two cases) they are (2*2=4 segments) and (4*4=16 segments).

Finally, we compare the results obtained from the proposed method with the results of the traditional method using the same elements in chapter 4.

As illustrated in the block diagrams shown traditional method in **Fig (3.8)**, and the proposed method in **Fig (3.9)** when the segmentation case 2 * 2. As for the schema representation of the segments 4 * 4, it is similar to the idea of the scheme 2 * 2.

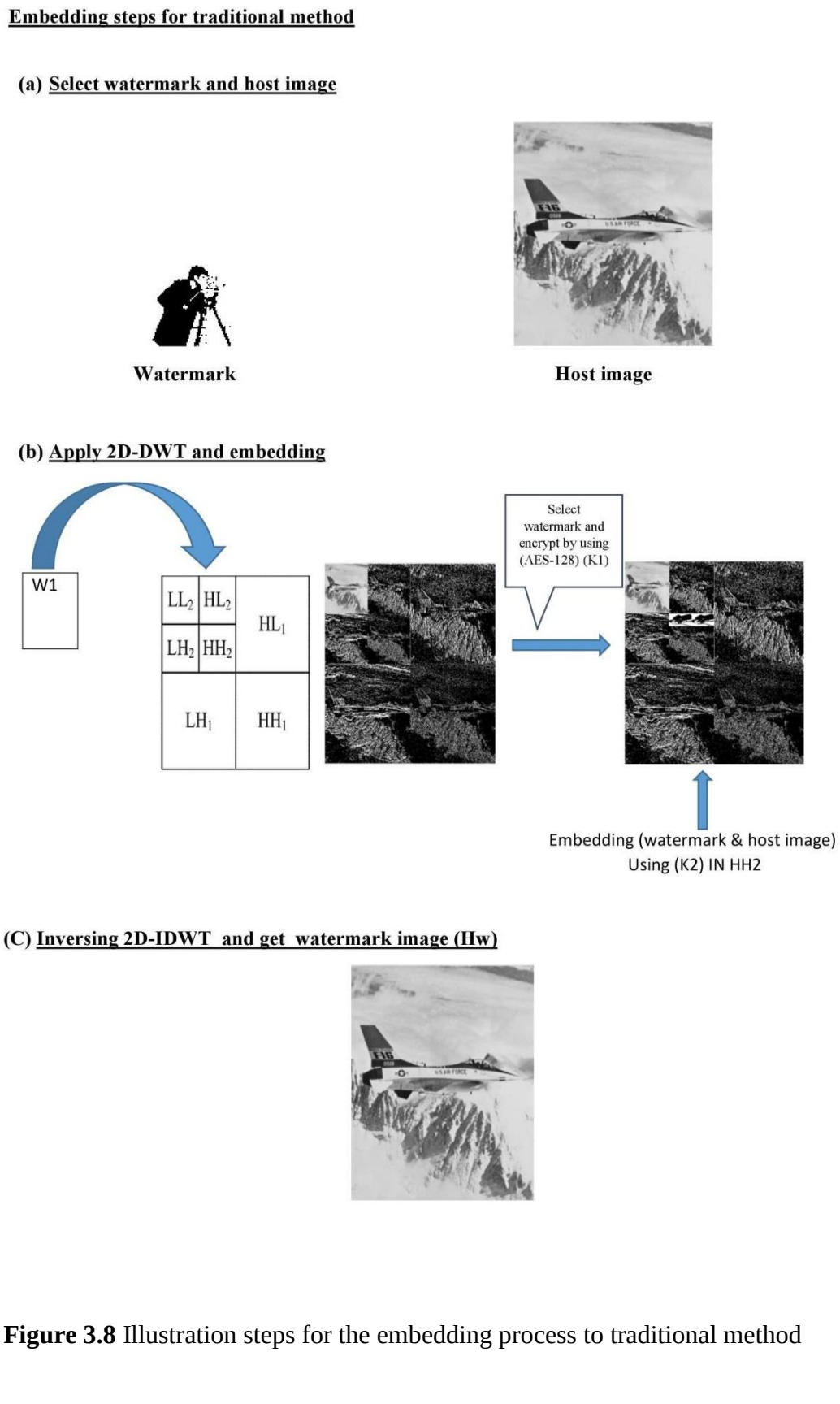


Figure 3.8 Illustration steps for the embedding process to traditional method

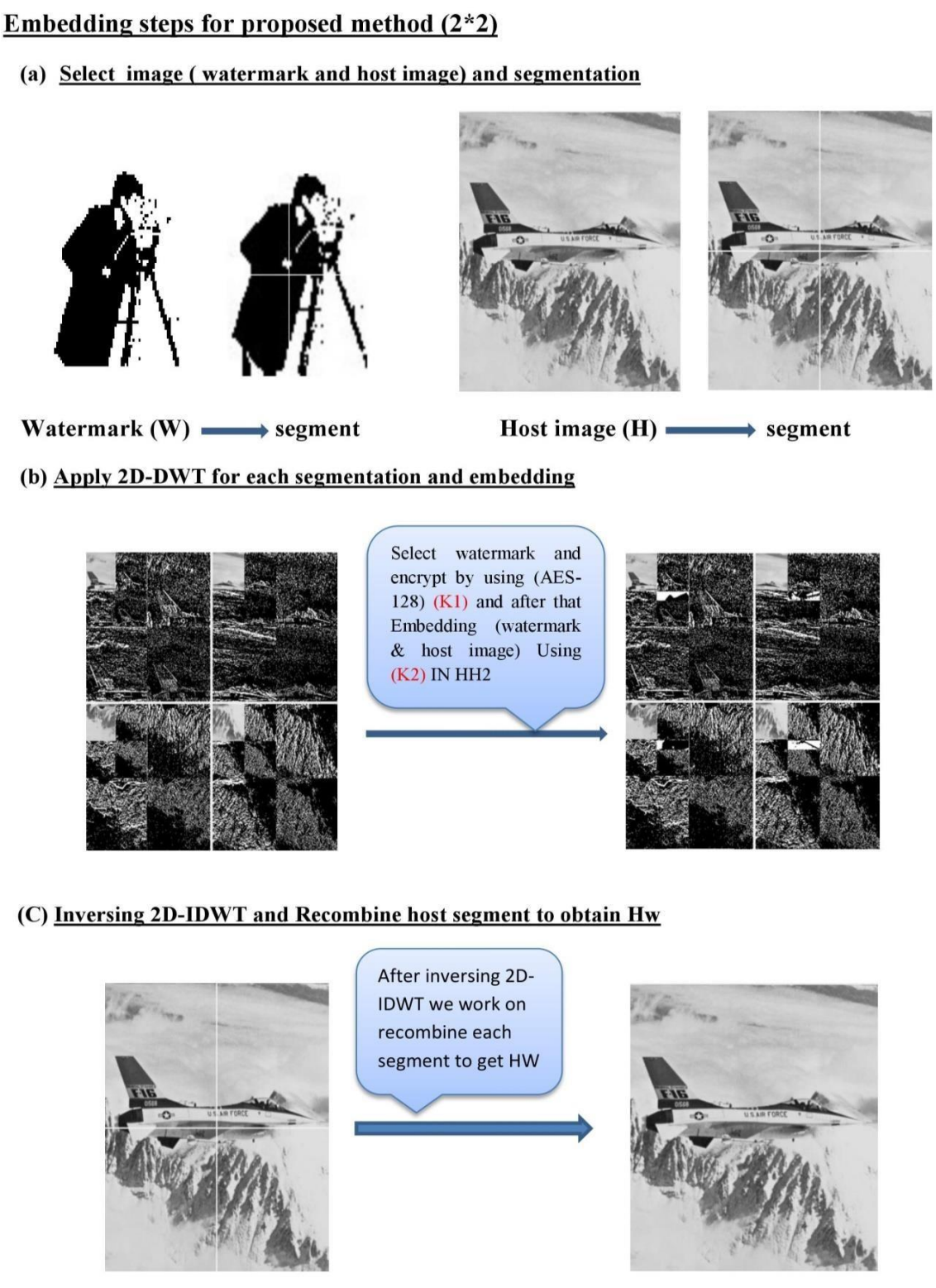


Figure 3.9 Steps for the embedding process to proposed method

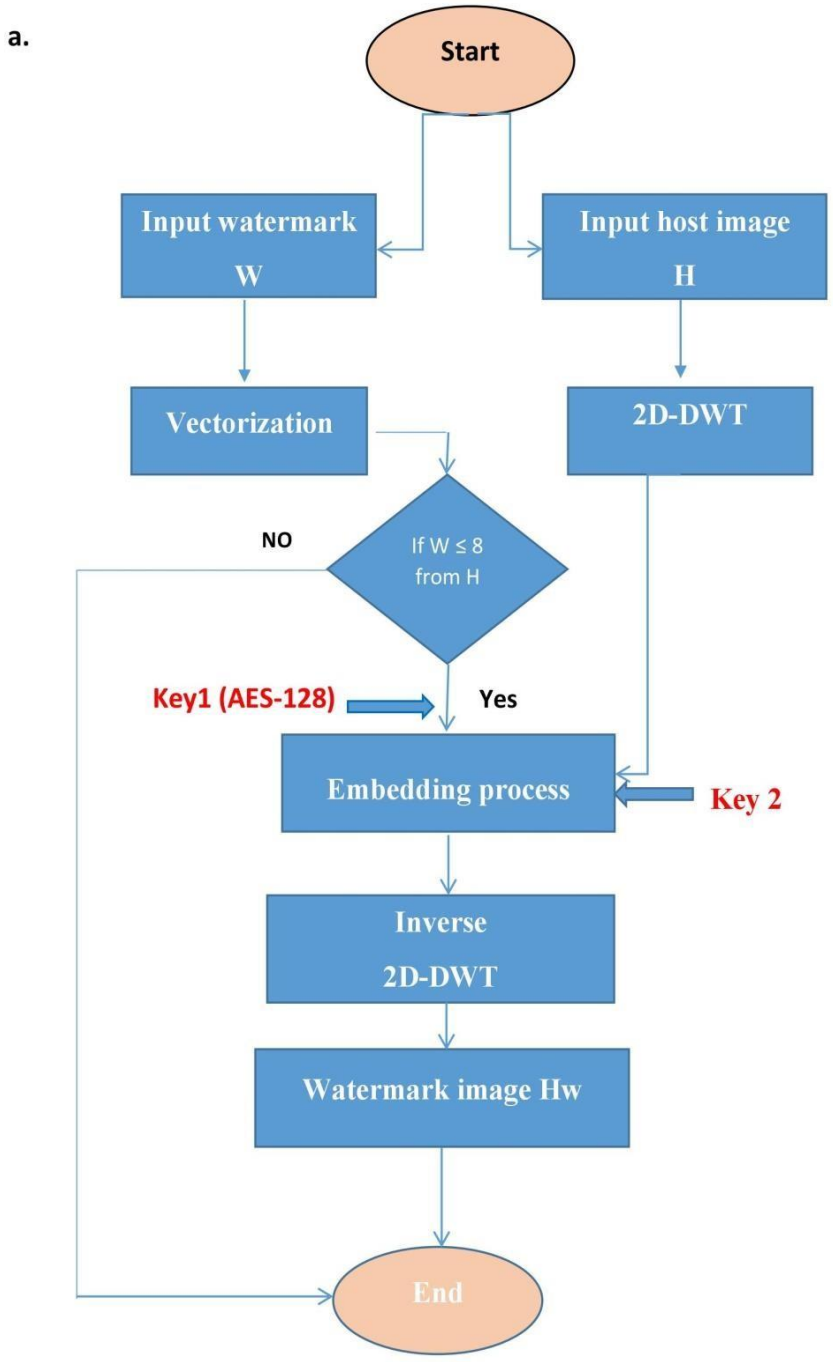


Figure 3.10-a Flowchart for the embedding process using the traditional DWT scheme

b.

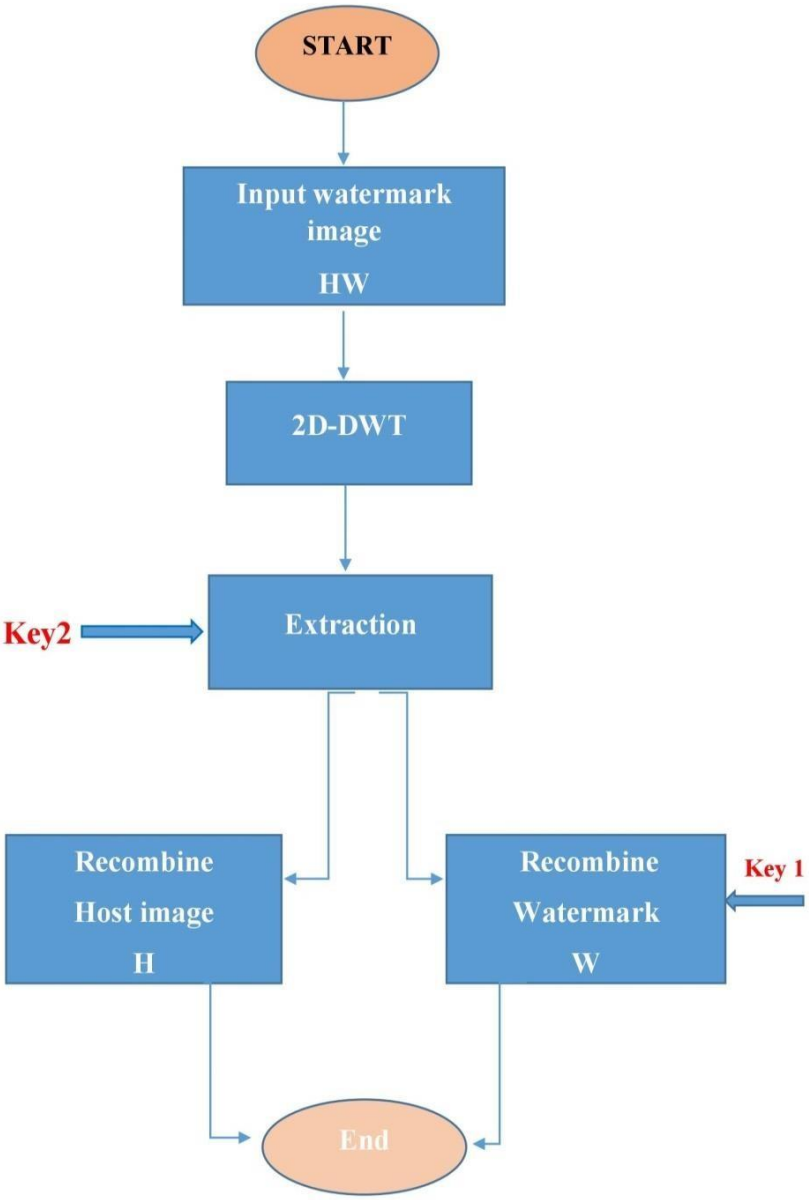


Figure 3.10-b Flow chart for the extraction process using the traditional DWT scheme

Here, in these two forms, the diagram of the embedding and extraction process appears in the traditional way, showing the use of the 2D-DWT and vectors. This is the difference between the traditional method and the proposed method in which we use the segmentation of both the host image and the watermark. The two methods will be compared in terms of the results produced by this method and their effect in concealment with will be compared the results with obtained for the traditional DWT technique.

In the following, the proposed embedding and extraction processes will be outlined in more details.

3.2.1 Embedding process

For the embedding of the logo image (watermark) into the host image, the flow chart of Figure (3.11) is followed. It consists of the following steps.

Step 1: input watermark **(binary image)** and the host image **(input image and convert to Grayscale 512).**

Step 2: Segment the watermark in to **n** segments (W1, W2, W3,….,W n) and also host image in to **n** segment, (H1,H2,H3, ...,H n). The value for segmentation in this thesis will be n=2*2 divided to 4, and 4*4 divided to 16.

Step 3: Use the vectorization for each segment of both, the watermark and the host image.

Step 4: The watermark size must be less than eight times the size of the each segment host image before encryption to prevent image degradation.

Step 5: Encrypting all segments of the watermark if (2*2 or 4*4), using the same key by AES-128 algorithm.

To obtain cipher text before embedding the host image, the formula is:-

Enc = (Wn, K1) 3.1

Where Wn= watermark segment n=4 or 16, K1= key use to encrypt each segment of watermark.

Step 6: Use discrete wavelet transform (2D-DWT) technique for each segment of the host image.

Step 7: each segment of the watermark (W1,W2,W3…,Wn) after encrypt we do embedding inside the corresponding host image Which are also divided (H1,H2,H3…Hn) using the key (K2) in segment HH2 according to the following formula:-

CWn.hh2 = Enc (Wn, K1) $\oplus$ **K2 .....** 3.2

Where **n=**4 or 16, and **CWn.hh2 =** watermarked image where the logo is embedding inside level HH2 for each segmentation in host image.

Wn = represents the number of divisions of the watermark. **K2=** key use for embedding in host image.

Step 8: perform the Inverse (2D – IDWT) to recover the image for each segment.

Step 9: Recombine segments of watermarked host image in order to get complete watermarked image (Hw).

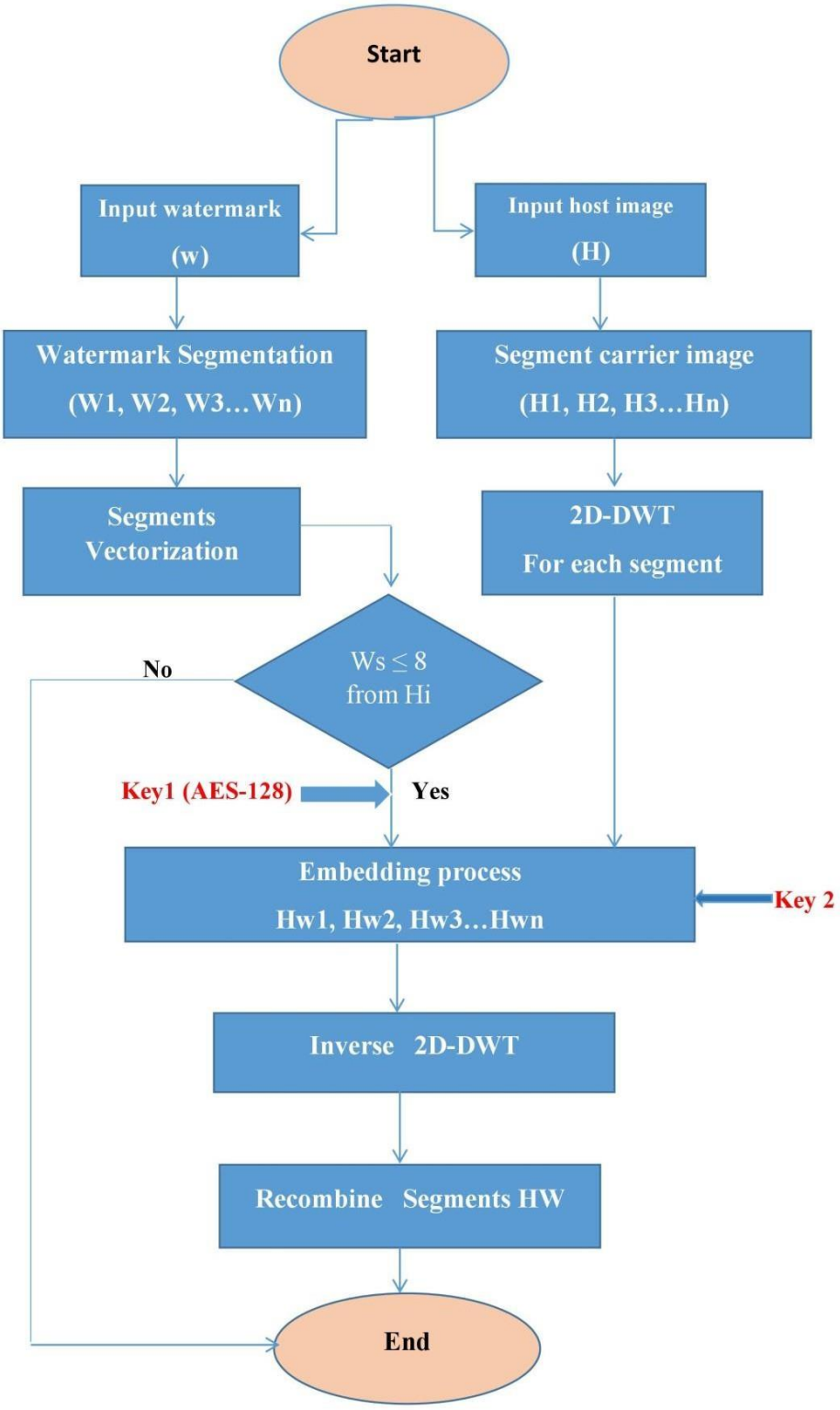


Figure 3.11 Flow chart for the proposed segmented DWT embedding process

3.2.2 Extraction process

To extract the embedded logo watermark image from the watermarked image, a process similar to embedding process is conducted but in reverse order. It starts with the watermarked image (Hw) using the same key. The flow chart of Figure 3.12 is followed. The process consists of the following steps.

Step 1: Input the watermarked image (Hw)

Step 2: segment the image in **n** segments of equal size.

Step 3: Use 2D-DWT technique for each segment of the watermarked image

Step 4: Extraction each watermark segments from host image segments using

Key (K2) that is a used in the embedding process.

Hw = Dec (CWn.hh2, K1) ⊕K2 ..... 3.3

Step 5: Recombined the extracted watermark segment to get the watermark W using key (K1).

Wn = Dec (Wn` , K1)

Step 6: Restore host image by applying the inverse 2D-DWT for each segment

Step 7: Recombine host image segment in order to restore original host image (H).

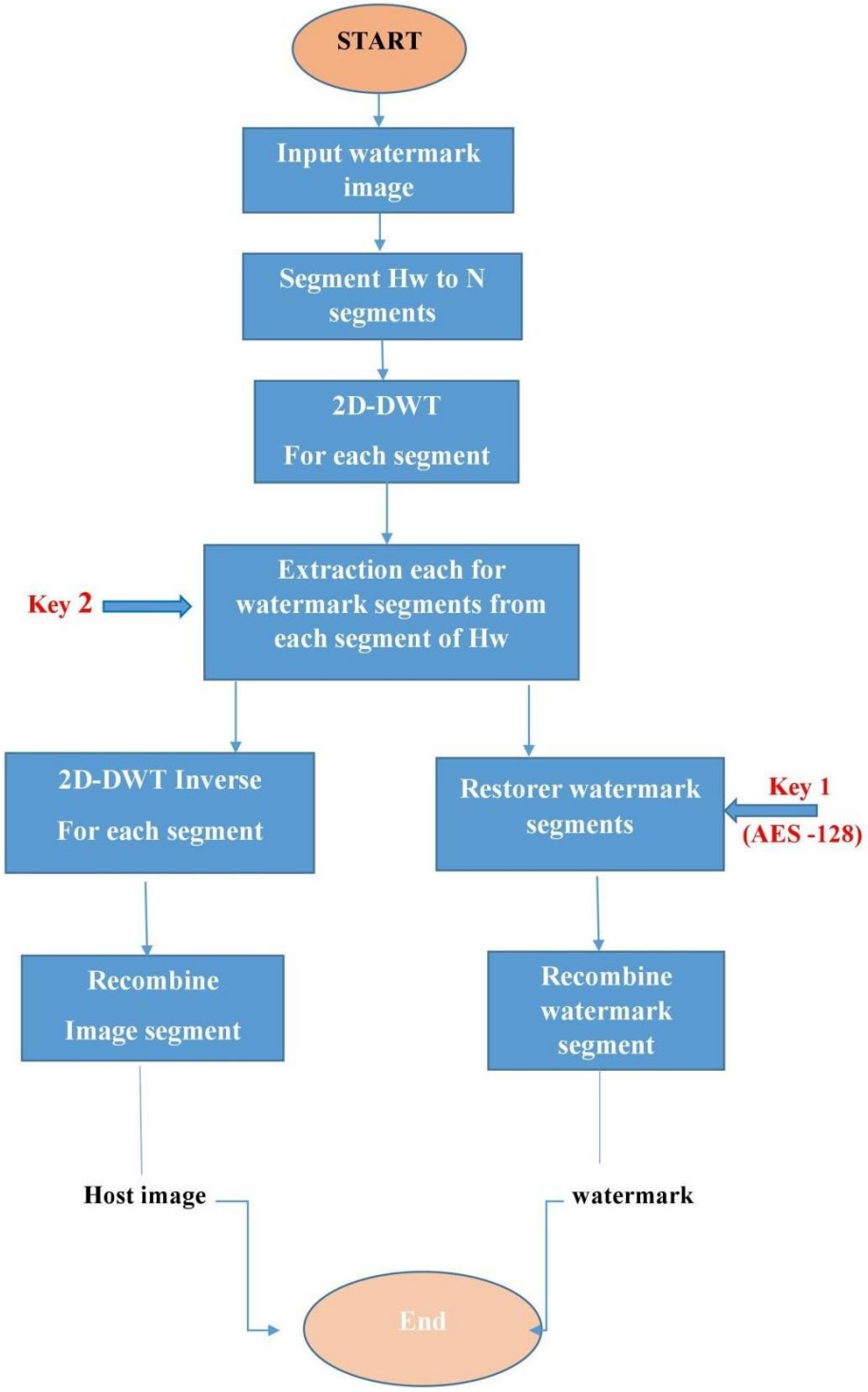


Figure 3.12 Flow chart for the proposed DWT extraction process

Chapter Four

Implementation and Results

Chapter Four

Implementation and Results

4.1 Introduction

This chapter is devoted to discuss the overall performance of the proposed system on investigates the implementation of the proposed algorithms in chapter three and review the results of the measurements used to evaluate the algorithm through the embedding process in two parts, the first part takes the host images and watermark in different sizes without using the division of the image, as for the second part takes the same criteria but using the division and all this gets technique Discrete wavelet transform-2D. Also summarize the difference between the use of image division and non-use, and the consequences of that in terms of testing the robustness of the image and imperceptibility and their effects on the images and different sizes of watermark.

This chapter also deals with measurements used in image measurement before and after embedding so that we can determine the difference between the without segmentation and proposed methods and testing the images on the wide range of attacks. These attacks include the effect of adding various noise such as (Gaussian, salt and pepper, additive), Rotating, and Cropping.

In this research, C# software is basic feature of the program is the speed of the programming, which is a prerequisite for applications that fast direct and rapid processing of images.

c# is designed for the .net platform, considered Powerful programming platform with integrated visualization programming environment, also it's modern, object -oriented and type-safe

programing language that combines the high productivity of rapid application development languages and c# provides friendly interface, the fast execution speed, high security with creating EXE files, and can be run with.net framework instead of the software. In contrast Matlab has some disadvantages, m-file prepared by Matlab is a text file with bad confidentiality and it function of graphical user interface is not flexible enough.

4.2 Evaluation Metrics

The process of evaluating the algorithm is important to know the strengths and weaknesses. In order to test the inherent image and verify the imperceptibility, robustness, and structural similarity, there are important measures for these characteristics which are as follows:-

4.2.1 Peak signal-to-noise ratio (PSNR)

An important way of evaluating watermarking algorithms is to compare the amount of distortion introduced into a host image by a watermarking algorithm.

The widely used **peak signal-to-noise ratio (PSNR)** measurement, which measures the maximum signal to noise ratio found on an image has been used as an objective measure for the distortions introduced by the watermarking system. Is commonly used measure for imperceptibility level, the unit of PSNR is decibels (db) and defined as following:-

PSNR (C, Cw) **= 10 (** ————) **…….**(4.1)

Where MAX is equal to 255 in grayscale images, and **MSE** is **mean square error** between the original image C and the watermarked image Cw. The MSE is defined as following:

$$- \sum \quad \text{..... (4.2)}$$

N: number of pixels in each image, **C:** Original image, **Cw:** Watermarked image

4.2.2 Normalized Correlation (NC) test

The robustness is measured by performing some attacks such as additive filter, salt and paper filter, and Gaussian noise. Then **Normalized Correlation (NC) test** between the embedded and extracted watermarks is calculated for embedding strength. The NC is defined as following:-

$$\frac{\sum \sum}{\sqrt{\sum \sum}\ \sqrt{\sum \sum}} \quad \text{..... (4. 3)}$$

W: the embedded watermark. **WR:** extracted Watermark

4.2.3 Structural Similarity Image Quality Measure (SSIM) test

One of the perceptual metric to determine the quality of the image through the amount of degradation in quality due to treatment such as data compression or loss of data transmission, with The measurement of similarities between the two images (original and distorted).

SSIM includes three parts:

(μx,μy) the contrast luminance comparison function which measures the closeness of the two images "mean luminance". (σx,σy) the contrast comparison function which measures the closeness of the contrast of the two images. (σxy) the contrast structure comparison function which measures the correlation coefficient between the two images x and y. (C1, C2, C3) the positive constants are used to avoid a null denominator.

Note when (μx,μy) =1 or maximal this means μx=μy, (σx,σy) =1 or maximal this means σx=σy

The positive values of the SSIM is located in (0,1) when value 0= mean no correlation between images, but value 1= mean have correlation between images (x=y).

The without segmentation methods of combining errors in image, make it SSIM to represent any error in the image depends on three factors namely loss of correlation, luminance distortion and contrast distortion. In general the formula SSIM is:-

[ ] [ ] [ ]

4.3 Embedding algorithm tests

The proposed method is tested through the process of inclusion, and this is done by testing the image extracted by the measurements mentioned in PSNR, MSE, SSIM, CORRELATION (CC) and Normalized Correlation (NC) To see the extent of robustness and imperceptibility, Were taken two image (512 * 512), which represents the host image and include different sizes of logo which represents (watermark) and the following table 4.1 shows the Used Images for the tests**.**

Table 4.1 Used Images for the tests

HOST IMAGE **Gray scale PNG (512*512)**	**WATERMARK** **Binary image (monochrome)**	**Dimensions**
		8*8
		16*16
		24*24
		32*32
		64*64

After the embedding of each image (host) with the image of the different logo size (Watermark) results appear in the following are in two methods, first without segmentation embedding method i.e. without the use of the partitioning process. Then, the same watermarks and host image were used for the testing of the proposed method in the application but by using the 2*2 partitioning and 4*4 partitioning. For each of the image (host) and logo (watermark), all implement the Discrete wavelet transforms (2D-DWT) technique. For a more detailed explanation of the embedding process, refer to Chapter three.

Tables (4.2) show the results that are obtained for the without segmentation method and the proposed method (two cases) of the embedding process, (2*2 and 4*4) partitioning or segmenting techniques.

Table 4.2 MSE& PSNR comparison between without segmentation and proposed method (2*2&4*4)

Host image	watermarks	Without segmentation method		Proposed method (with segmentation)			
				2*2		4*4	
		MSE	PSNR	MSE	PSNR	MSE	PSNR
Airplane	8*8	0.0041	90.436 db	0.0042	90.326 db	0.0041	90.327 db
	16*16	0.0042	90.293 db	0.0042	90.140 db	0.0042	90.028 db
	24*24	0.0042	90.112 db	0.0043	89.460 db	0.0043	89.384 db
	32*32	0.0043	89.843 db	0.0044	88.326 db	0.0044	88.423 db
	64*64	0.0047	87.976 db	0.0055	82.411 db	0.0053	83.375 db
Sydney	8*8	0.0032	87.914 db	0.0033	83.27 5db	0.0033	87.757 db
	16*16	0.0033	87.841 db	0.0034	80.862 db	0.0034	79.301 db
	24*24	0.0033	87.781 db	0.0036	75.251 db	0.0036	73.611 db
	32*32	0.0034	87.625 db	0.0037	74.308 db	0.0039	71.525 db
	64*64	0.0039	86.459 db	0.0053	64.200 db	0.0052	63.633 db

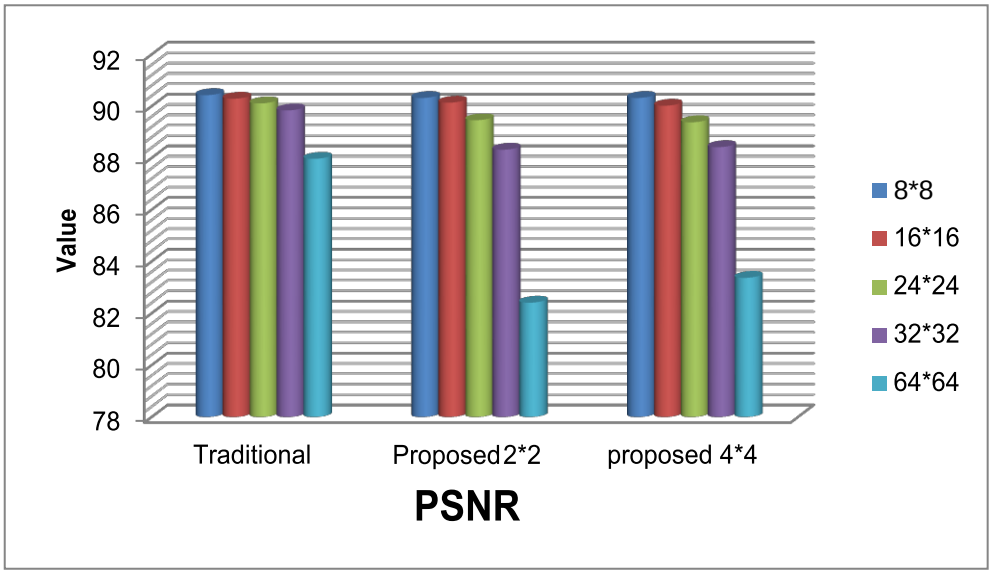


Figure 4.3 PSNR value (Airplane image)

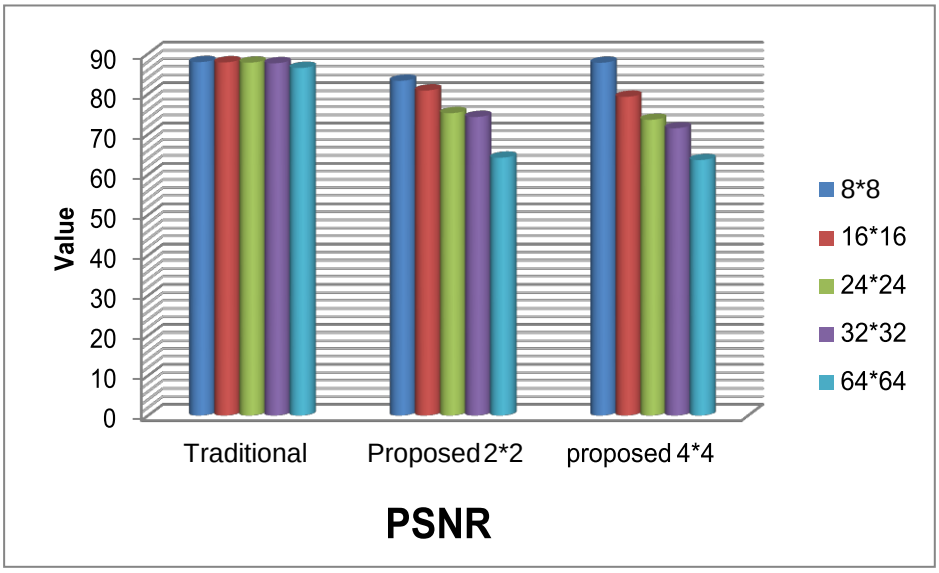


Figure 4.4 PSNR value (Sydney image)

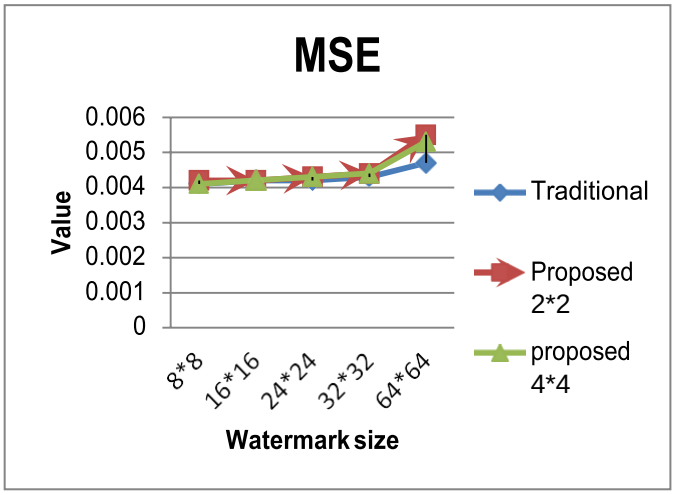


Figure 4.5 MSE value (Airplane image)

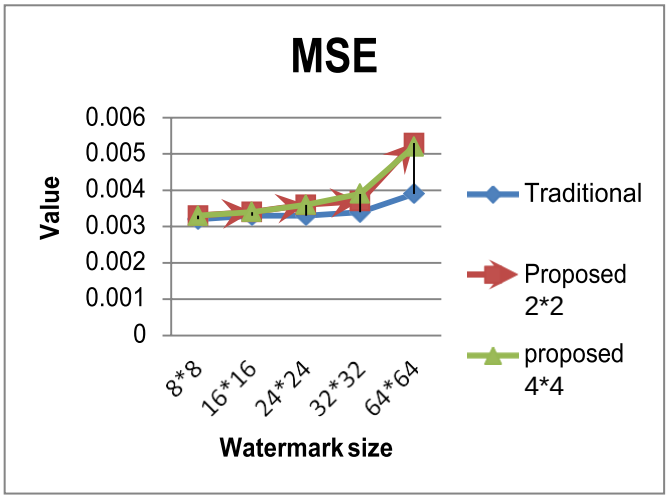


Figure 4.6 MES value (Sydney image)

In these figures (4.3& 4.4), (4.5&4.6) we show without segmentation method and proposed method in two cases (2*2, 4*4) to values MSE& PSNR for two images.

- Notice from the results presented that the values **PSNR** decrease with the increase of the size of the watermark in both methods, but the values of the image (Airplane) in both methods remain higher than the values of the image (Sydney).
- As for the values of **MSE** in the without segmentation method, it remain fixed or a little change, the reverse of the proposed method use of segment (2*2&4*4) increase value with the use of the largest size of the watermark 64 * 64 only.

Table 4.7 SSIM& Correlation comparison between without segmentation and proposed method (2*2&4*4)

Host image	watermarks	Without segmentation method DWT		Proposed method (with segmentation)			
				2*2		4*4	
		SSIM	CORR.	SSIM	CORR.	SSIM	CORR.
Airplane	8*8	0.9942	0.9584	0.9942	0.9584	0.9942	0.9584
	16*16	0.9941	0.9584	0.9941	0.9584	0.9941	0.9584
	24*24	0.9938	0.9584	0.9938	0.9584	0.9939	0.9584
	32*32	0.9933	0.9584	0.9933	0.9584	0.9932	0.9584
	64*64	0.9886	0.9420	0.9889	0.9584	0.9889	0.9584
Sydney	8*8	0.9972	0.9827	0.9966	0.9827	0.9972	0.9827
	16*16	0.9970	0.9827	0.9961	0.9827	0.9960	0.9827
	24*24	0.9966	0.9827	0.9943	0.9827	0.9942	0.9827
	32*32	0.9959	0.9827	0.9936	0.9827	0.9917	0.9822
	64*64	0.9911	0.8914	0.9852	0.9872	0.9825	0.9827

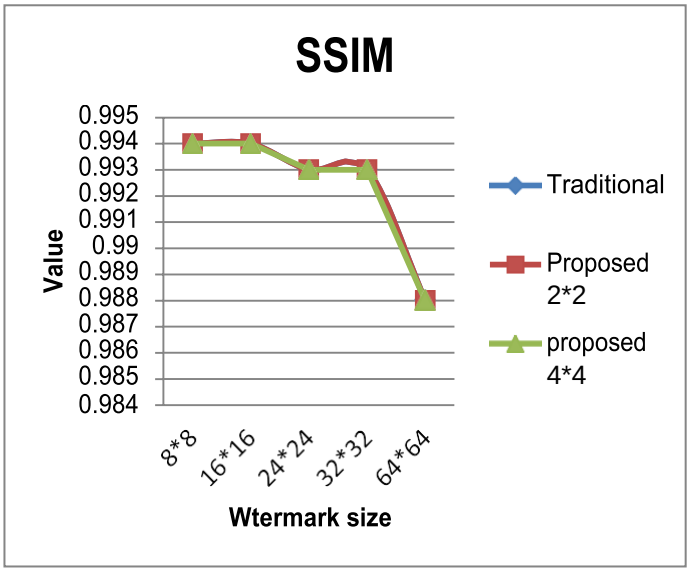


Figure 4.8 SSIM value (Airplane)

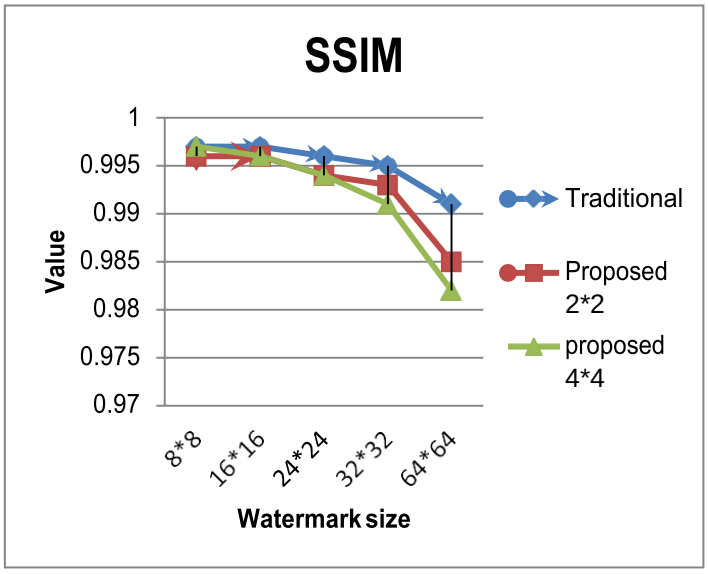


Figure 4.9 SSIM value (Sydney)

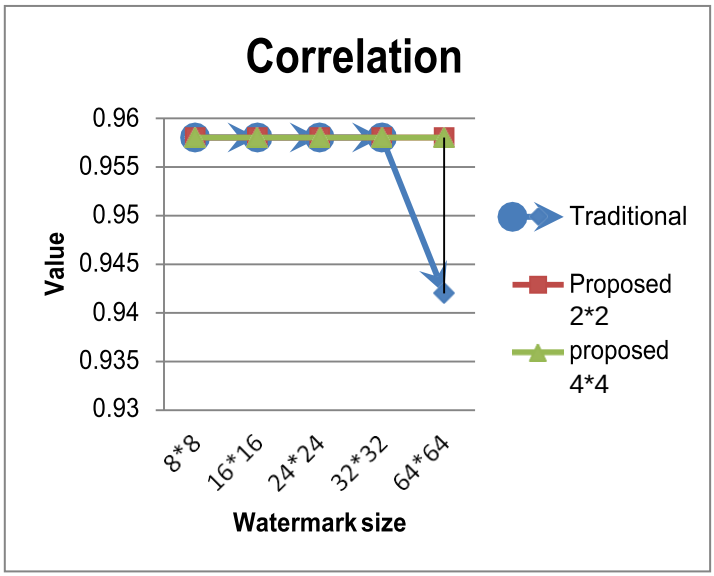


Figure 4.10 CORR. Value (Airplane)

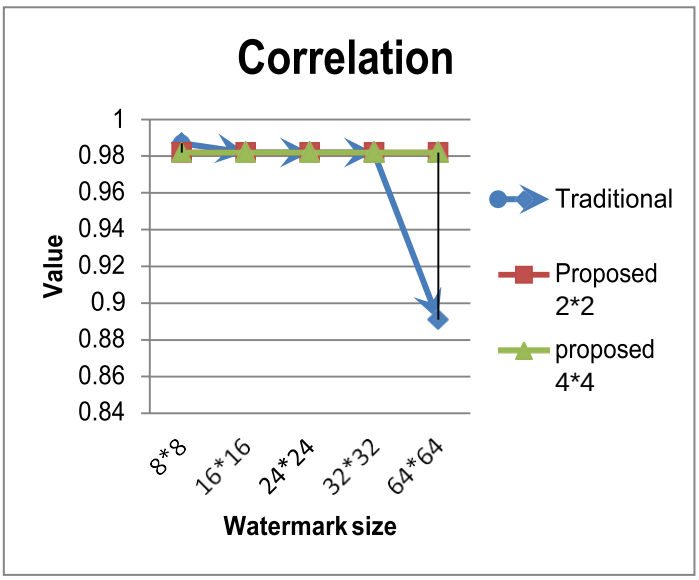


Figure 4.11 CORR. value (Sydney)

In these Figures (4.8& 4.9), (4.10&4.11) we show without segmentation method and proposed method in two cases (2*2, 4*4) to values SSIM& CORR. for two images.

What is shown in the graphs of Figures above are that the changes that appear between the without segmentation and proposed method (in both cases) are few changes.

The following are observed in the values (SSIM&CORR.) shown in the table (4.7):

- As for the values SSIM the without segmentation method of the image (Sydney) has values higher than that of (Airplane). Generally start decreases in both methods as the size of the watermark increases.
- As for the values of correlation coefficient **(CC),** the without segmentation method of the image (Sydney) has higher values compared to the image (Airplane) but these values remain constant with a little decrease in the value of without segmentation method using the largest size of the watermark (64*64). As for the proposed method (using two images) the results remain constant without change in the values.

  For the calculation of both the time of embedding and extraction in the without segmentation and proposed methods in the two cases (2*2&4*4), as show in table following (4.12)

Table 4.12 T.EM& T.EX Comparison between without segmentation and proposed method (2*2&4*4)

T.EM= Embedding time **T.EX= Extraction time** **MS= millisecond**

Host image	watermarks	Without segmentation method DWT		Proposed method (with segmentation)			
				2*2		4*4	
		T.EM	T.EX	T.EM	T.EX	T.EM	T.EX
Airplane	8*8	1 Ms	7 Ms	2 Ms	7 Ms	5 Ms	10 Ms
	16*16	1 Ms	6 Ms	2 Ms	8 Ms	7 Ms	10 Ms
	24*24	1 Ms	6 Ms	2 Ms	7 Ms	4 Ms	9 Ms
	32*32	1 Ms	6 Ms	3 Ms	7 Ms	4 Ms	10 Ms
	64*64	2 Ms	7Ms	3 Ms	8 Ms	4 Ms	9 Ms
Sydney	8*8	1 Ms	7 Ms	2 Ms	12 Ms	3 Ms	13 Ms
	16*16	1 Ms	6 Ms	2 Ms	7 Ms	3 Ms	16 Ms
	24*24	2 Ms	7 Ms	2 Ms	7 Ms	3 Ms	14 Ms
	32*32	2 Ms	7 Ms	2 Ms	7 Ms	6 Ms	13 Ms
	64*64	1 Ms	6 Ms	3 Ms	7 Ms	4 Ms	13 Ms

The results showed that for the time embedding (T.EM) and time for extraction (T.EX), there are largest values in the proposed method to (4 * 4) and then the time of embedding and extraction showed less values when the division (2* 2) and the lowest values at without segmentation method. As for the changes of the execution time of the embedding and the extraction processes, the difference is that the more the number of division increased the time of embedding and extraction increase too, that it was expected. Note that unit time measurement is **millisecond.**

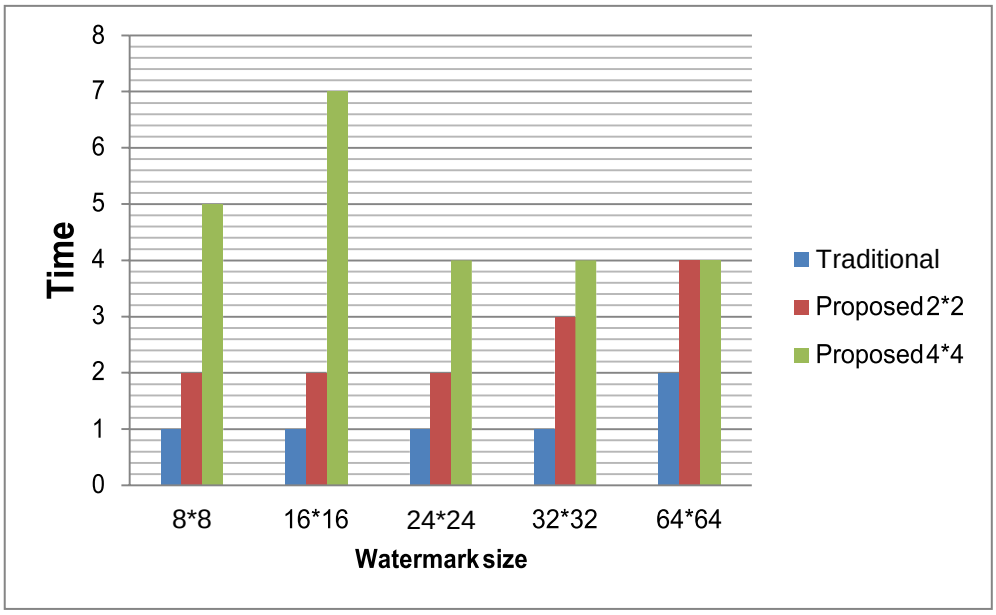


Figure 4.13 Embedding time (T.EM) Value (Airplane)

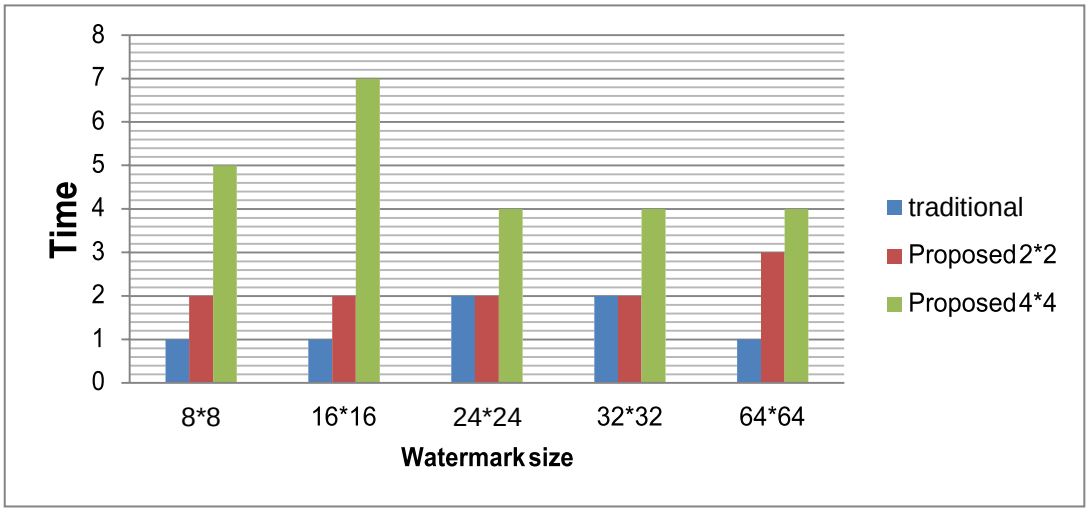


Figure 4.14 Embedding time (T.EM) value (Sydney)

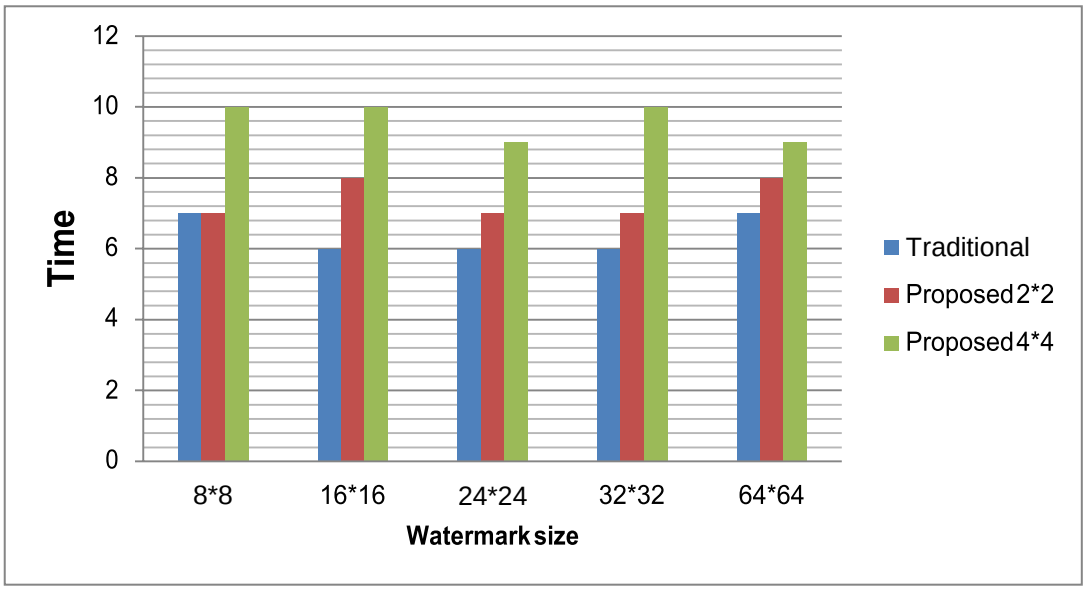


Figure 4.15 Extraction time (T.EX) Value (Airplane)

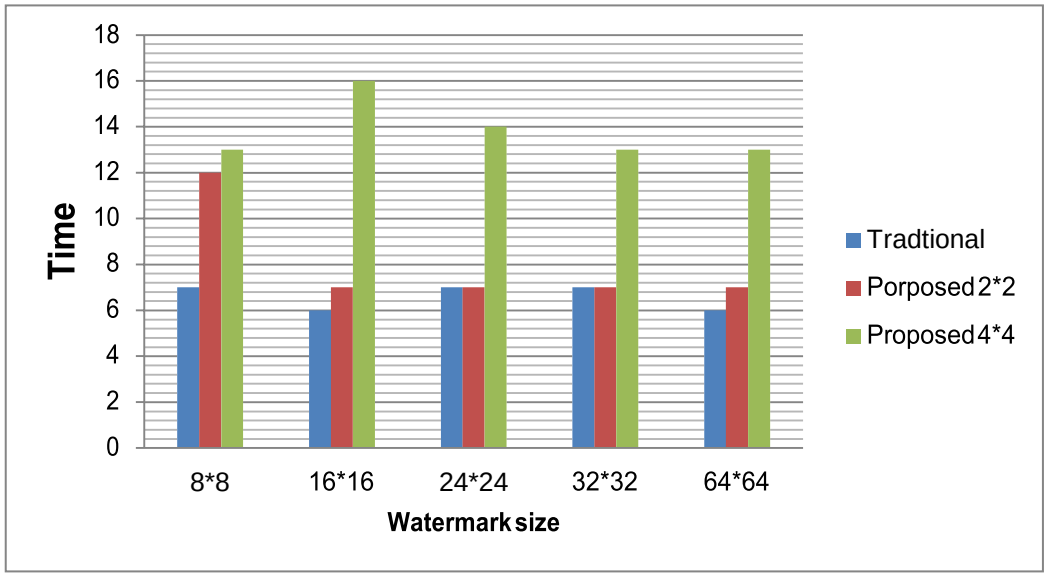


Figure 4.16 Extraction time (T.EX) value (Sydney)

4.4 Performed Attacks

Watermarking systems are susceptible to many kinds of attack. These attacks could be performed intentionally or unintentionally. Watermarking systems utilized in copy protection or data authentication schemes and are especially susceptible to intentional attacks. Unintentional attacks usually come from common signal processing operations done by legitimate users of the watermarked materials, for example a user might want to compress a bitmap image using JPEG compression simply to conserve disk space. Intentional attacks are usually done by more competent people with more knowledge of watermarking systems and more resources to make the attack.

In this part, various attacks were applied on different size watermarked images obtained by the proposed method and without segmentation method. Although the discrete wavelet transform, watermarking is known to be strong against different types of attacks on the watermarked images were conducted to see if any possibility of watermark survival when different percentages of effects (Noise or Distortion) are used.

All experiments have confirmed that the watermarks were lost in some kinds of attacks and unaffected or mildly affected in others. These attacks included the following:

4.4.1 Salt and pepper Noise

It is one of the types of noise used to test images, and this type occurs because of sharp and sudden changes of image signal. Its shape appears as high spike.

Images damaged by salt and pepper noise are taking the minimum and maximum values in the dynamic range. The noise can take noisy pixels only in which values of the pepper are 0 but the salt noise values are 255, the malfunctioning caused by these noise are in pixels of camera sensors, Faulty memory locations in the devices, or an error in the timing digitization process.(Chan et.al 2005). A Figureure 4.17 shows an image before and after being effected by the salt & paper noise.

Original Image **(salt and paper noise) Image**

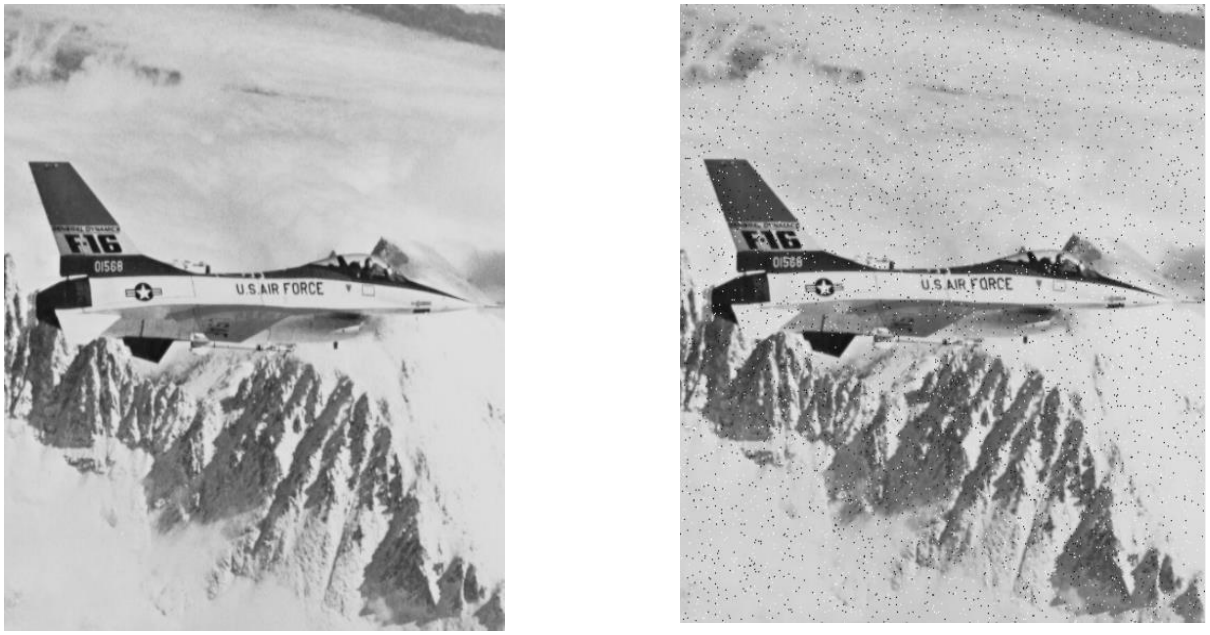


Figure 4.17 An image before and after the inclusion of salt & paper noise

The following table 4.18 shows evaluation of the PSNR and NC for the effect of the addition of salt and pepper noise both images (Airplane, Sydney). In this experiment different noise degrees (**0.5 - 2)** are included.

Table 4.18 Comparison noise Salt and pepper value of (PSNR & NC) for the without segmentation and proposed method for (2*2 &4*4) segmentation

images	Watermark size	Noise degree	Without segmentation method		Proposed method (2*2)		Proposed method (4*4)	
			PSNR	NC	PSNR	NC	PSNR	NC
AIR PLANE	8*8	0.5	56.07db	1	55.68db	1	55.87db	1
		2	44.06db	1	43.83db	1	43.86db	1
	16*16	0.5	55.69db	0.995	55.78db	0.995	55.62db	1
		2	43.62db	0.990	43.82db	0.995	43.67db	0.990
	24*24	0.5	55.97db	0.997	56.03db	0.995	55.75db	0.995
		2	43.79db	0.987	43.77db	0.991	43.75db	0.982
	32*32	0.5	55.74db	0.994	55.75db	0.998	55.53db	0.996
		2	43.94db	0.987	44.09db	0.990	43.82db	0.991
	64*64	0.5	56 db	0.998	55.27db	0.997	55.59db	0.997
		2	44.03db	0.988	43.73db	0.991	43.84db	0.990
SYDNEY	8*8	0.5	54.43db	1	54.35db	0.974	54.31db	1
		2	42.47db	0.974	42.28db	0.923	42.45db	1
	16*16	0.5	54.43db	0.995	54.32db	0.995	53.94db	0.995
		2	42.60db	0.981	42.49db	0.981	42.55db	0.990
	24*24	0.5	54.54db	0.995	53.77db	0.993	53.73db	1
		2	42.45db	0.987	42.36db	0.987	42.29db	0.998
	32*32	0.5	54.48db	0.997	53.58db	0.996	53.28db	0.998
		2	42.52db	0.989	42.20db	0.986	42.32db	0.986
	64*64	0.5	54.33db	0.997	51.98db	0.997	52.13db	0.997
		2	42.65db	0.990	41.87db	0.994	41.81db	0.991

From table 4.18 it can be seen that

- The values of PSNR when compared in terms of use in a manner without segmentation with the method of the proposal found very little difference, and as for the difference in value when using the watermark in different sizes with different degrees of noise (0.5 and 2) found that the values PSNR give a slight difference or Maintains the same values.
- The values of the normalized correlation NC are gave higher value when the size of the watermark is small after gradually decreases with the watermark increases size, and also the values did not differ but difference between them was slightly than what exists in a way that is not segmented with compare the proposed method.

4.4.2 Additive Noise

This is one of the simple types of noise that affects digital images that are characterized by random white noise. The spectral image I (x, y) of the original image element is equal to R (x, y) plus noise N (x, y), which is not usually dependent on the signal (that is, it is caused by external factors that have nothing to do with the real signal) and are characterized by a zero rate and their variation can take specific values depending on the adopted imaging system and the nature of the target. The group noise can be represented as follows: (Huda, 2001)

The original image and that containing the additive noise is shown in Figure 4.19

Original Image **(Additive noise) Image**

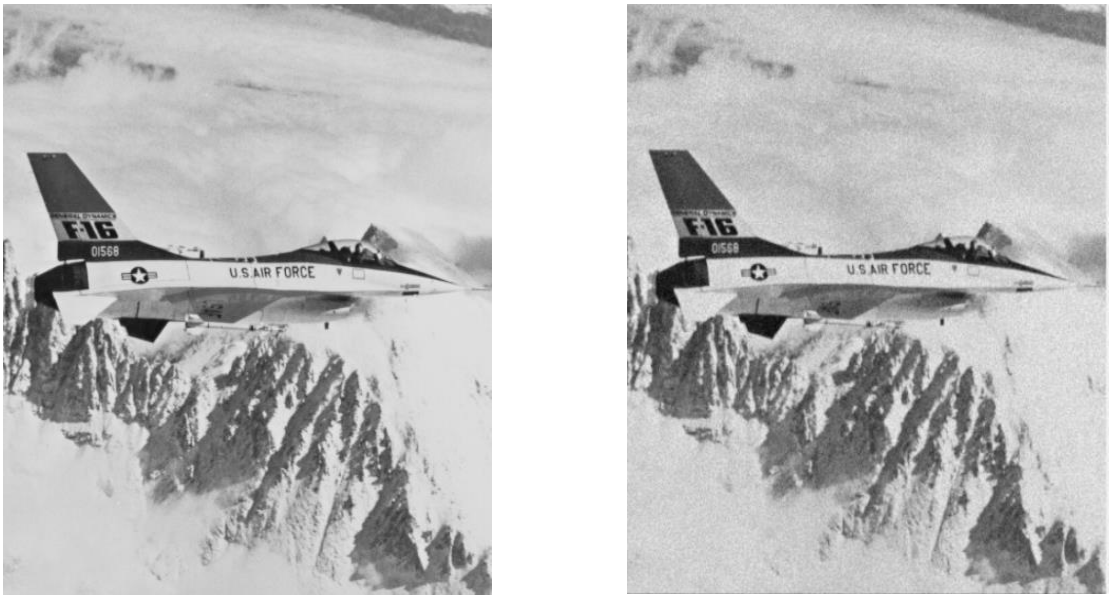


Figure 4.19 An image before and after the inclusion of additive noise

The additive noises are tested on the two images having the same dimensions, taking different sizes of the watermark in the without segmentation and proposed methods (two cases 2*2 and 4*4). As this noise has taken two different degree to test is (0.5 and 2), showed that the values PSNR of the image (Sydney) was higher than the values of the image (Airplane). In addition the Normalized Correlation (NC) showed slight change but it remains of good value and the highest value of NC was obtained by the proposed method (2 * 2) at the watermark size (24 * 24), which is 1 in noise of (0.5). But in general, values are lower in all cases when the watermark size increases. The results are listed in table 4.20.

Table4.20 Comparison value additive noise of (PSNR & NC) for the without segmentation and proposed method for (2*2 &4*4) segmentation.

images	Watermark size	Noise degree	Without segmentation method		Proposed method (2*2)		Proposed method (4*4)	
			PSNR	NC	PSNR	NC	PSNR	NC
AIR PLANE	8*8	0.5	75.47db	0.999	75.46db	0.999	75.46db	0.999
		2	53.62db	0.998	53.61db	0.998	53.61db	0.998
	16*16	0.5	75.45db	0.999	75.42db	0.999	75.40db	0.999
		2	53.62db	0.999	53.61db	0.998	53.61db	0.998
	24*24	0.5	75.41db	0.999	75.30db	0.999	75.28db	0.999
		2	53.61db	0.998	53.60db	0.998	53.60db	0.998
	32*32	0.5	75.37db	0.999	75.07db	0.999	75.09db	0.999
		2	53.61db	0.999	53.58db	0.999	53.58db	0.998
	64*64	0.5	74.97db	0.999	73.40db	0.999	73.73db	0.999
		2	53.58db	0.999	53.43db	0.999	53.46db	0.999
SYDNEY	8*8	0.5	74.98db	0.999	73.67db	0.999	74.91db	0.999
		2	54.06db	0.998	53.90db	0.998	54.02db	0.998
	16*16	0.5	74.97db	0.999	72.80db	0.999	72.15db	0.999
		2	54.06db	0.999	53.81db	0.998	53.74db	0.998
	24*24	0.5	74.95db	0.999	75.25db	1	69.20db	0.999
		2	54.05db	0.998	53.47db	0.998	53.33db	0.998
	32*32	0.5	74.92db	0.999	69.60db	0.999	67.87db	0.999
		2	54.05db	0.999	53.40db	0.999	53.11db	0.998
	64*64	0.5	74.62db	0.999	62.45db	0.999	61.98db	0.999
		2	54.02db	0.999	51.87db	0.999	51.72db	0.999

4.4.3 Gaussian blur noise

This Gaussian blur usually reduces the image details and this noise is known as another (Gaussian smoothing). To achieve Gaussian blur, the function must be taken to blur the image to be smooth, which means that the visual effect of a blurring technique makes the image similar to the display through a transparent screen. It also has extensive uses in graphics software. Two different images are also studied here with different degrees of noise ranging from 0.5 to 2. Figure 4.21 shows the images with & without Gaussian noise.

Original Image **(Gaussian blur noise) Image**

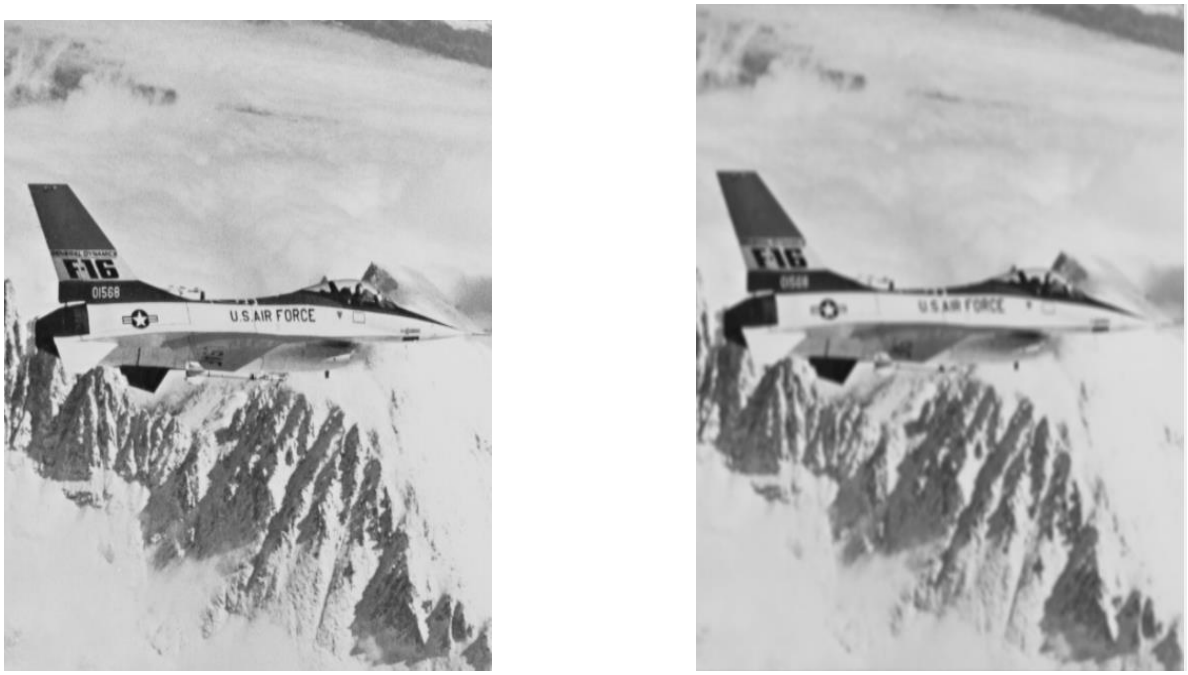


Figure 4.21 An image before and after the inclusion of Gaussian blur noise

The following table 4.22 shows the results of the two images in the without segmentation and proposed method in (two cases 2*2 and 4*4).

Table4.22 Comparisons value Gaussian blur of (PSNR & NC) for the without segmentation and proposed method for (2*2 &4*4) segmentation.

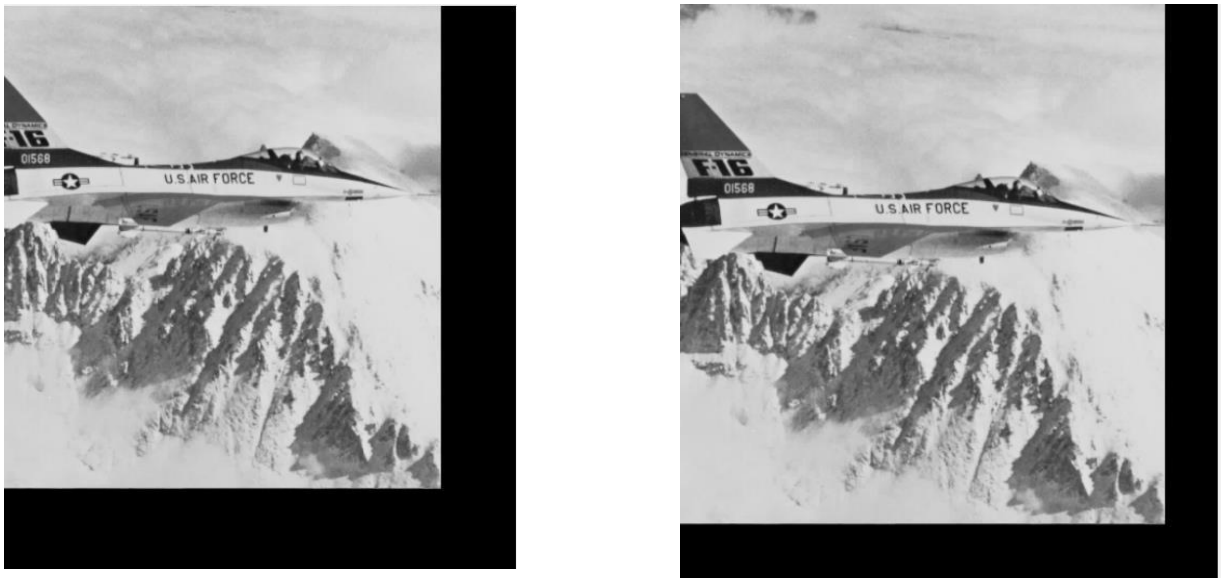
images	Watermark size	Noise degree	Without segmentation method		Proposed method (2*2)		Proposed method (4*4)	
			PSNR	NC	PSNR	NC	PSNR	NC
AIR PLANE	8*8	0.5	61.69db	0.854	61.69db	0.705	61.69db	0.735
		2	56.06db	0.811	56.06db	0.653	56.06db	0.664
	16*16	0.5	61.69db	0.727	61.68db	0.796	61.68db	0.829
		2	56.06db	0.708	56.06db	0.732	56.06db	0.777
	24*24	0.5	61.69db	0.742	61.67db	0.802	61.67db	0.801
		2	56.06db	0.685	56.05db	0.752	56.05db	0.747
	32*32	0.5	61.69db	0.866	61.65db	0.880	61.65db	0.917
		2	56.06db	0.820	56.05db	0.862	56.05db	0.891
	64*64	0.5	61.67db	0.946	61.48db	0.963	61.52db	0.853
		2	56.05db	0.926	55.99db	0.950	56db	0.889
SYDNEY	8*8	0.5	55.44db	0.897	55.38db	0.774	55.43db	0.708
		2	50.50db	0.854	50.49db	0.700	50.50db	0.601
	16*16	0.5	55.43db	0.767	55.35db	0.822	55.31db	0.805
		2	50.50db	0.754	50.47db	0.746	50.46db	0.748
	24*24	0.5	55.43db	0.724	55.21db	0.809	55.14db	0.800
		2	50.50db	0.658	50.42db	0.770	50.40db	0.751
	32*32	0.5	55.43db	0.856	55.16db	0.879	55.03db	0.914
		2	50.50db	0.804	50.40db	0.859	50.36db	0.888
	64*64	0.5	55.42db	0.944	54.43db	0.962	54.36db	0.852
		2	50.50db	0.923	50.11db	0.948	50.10db	0.887

The results shown in the table 4.22 for the without segmentation and proposed (2*2 and 4*4) proposed methods showed that the values of PSNR for the Airplane image were higher than those of the Sydney image, but PSNR value gradually decrease when the size of the watermark is increased slightly. The Normalized Correlation (NC) values gave the highest results in the proposed method (2*2) when watermark 64*64 size compared with the without segmentation method of the two images.

4.4.4 Cropping

It is the process of cropping parts of the image, which is one of the most used processes for processing images, mainly that cropping results in the removal of the upper and lower edges of the image, which leads to manipulation. Here we crop (50%, 75%) of the embedded image as shown in Figure 4.23.

Cropping 50% **Cropping 75%**



(a) **(b)**

Figure 4.23 Image cropping

Table 4.24 lists the computed PSNR and NC result for the cropping effect on the without segmentation DWT compared with these for the proposed technique using 2*2 and 4*4 segmenting processes.

Table 4.24 Comparison value cropping for the proposed segmented DWT with the without segmentation DWT

images	Watermark size	Noise degree	Without segmentation method		Proposed method (2*2)		Proposed method (4*4)	
			PSNR	NC	PSNR	NC	PSNR	NC
AIR PLANE	8*8	50%	13.76db	0.236	13.76db	0.146	13.76db	NaN
		75%	16.16db	0.113	16.16db	0.149	16.16db	NaN
	16*16	50%	13.76db	0.248	13.76db	0.239	13.76db	NaN
		75%	16.16db	0.307	16.16db	0.177	16.16db	NaN
	24*24	50%	13.76db	0.233	13.76db	0.232	13.76db	NaN
		75%	16.16db	0.347	16.16db	0.256	16.16db	NaN
	32*32	50%	13.76db	0.250	13.76db	0.167	13.76db	NaN
		75%	16.16db	0.289	16.16db	0.208	16.16db	NaN
	64*64	50%	13.76db	0.285	13.76db	0.173	13.76db	0.519
		75%	16.16db	0.324	16.16db	0.229	16.16db	0.519
SYDNEY	8*8	50%	23.78db	0.068	23.78db	0.262	23.78db	NaN
		75%	25.13db	0.326	25.13db	NaN	25.13db	NaN
	16*16	50%	23.78db	0.272	23.78db	0.211	23.78db	NaN
		75%	25.13db	0.282	25.13db	0.271	25.13db	NaN
	24*24	50%	23.78db	0.296	23.78db	0.158	23.78db	NaN
		75%	25.13db	0.355	25.13db	0.224	25.13db	NaN
	32*32	50%	23.78db	0.332	23.78db	0.141	23.78db	NaN
		75%	25.13db	0.340	25.14db	0.238	25.13db	NaN
	64*64	50%	23.78db	0.286	23.81db	0.143	23.77db	0.519
		75%	25.13db	0.388	25.14db	0.284	25.11db	0.519

NAN: There is no numerical value for the loss of the embedded watermark.

The results of the normalized correlation shown in the cropping process are of low value compared to the values tested as they gave fewer results in the proposed method than the without segmentation method and also when increased segmentation in proposed method (4*4), it has vanished watermark and cannot be retrieved, but the values of PSNR remained unchanged even with changing of the watermark size and also in both cases (2*2 and 4*4).

Therefore, the results for cropping are very bad. The reason is that when a part of the embedded image of a watermark is cropped, the mark inside the image of the carrier is lost and cannot be retrieved.

Note that in the case of division 4 * 4 when the size of watermark (64 * 64) it has given a value which is weak but not completely lost. The reason is that the larger the size of the watermark can be retrieved but the value is weak in contrast to the small size of the watermark that is lost to this is difficult to give a value to determine the deterioration of the watermark

4.4.5 Rotating

The application of the rotating test on the images is included in two angles; 45 and 90 degree counterclockwise, as in Figure 4.25, and test for the without segmentation and compared. Table 4.26 showing the measured values used for testing the image of the watermark.

Rotating (45) degree **Rotating (90) degree**

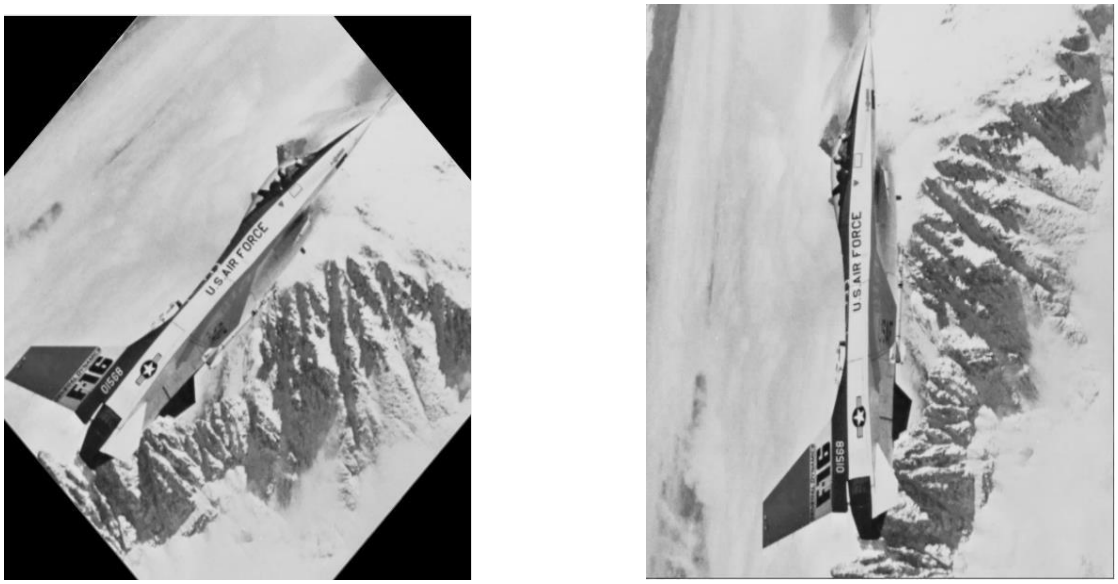


Figure 4.25: Image Rotating

Table4.26 Comparison value Rotating for the proposed segmented DWT with the without segmentation DWT

images	Watermark size	Noise degree	Without segmentation method		Proposed method (2*2)		Proposed method (4*4)	
			PSNR	NC	PSNR	NC	PSNR	NC
AIR PLANE	8*8	**45**	16.74db	0.328	16.74db	0.250	16.74db	0.274
		90	23.64db	0.433	23.64db	0.294	23.64db	0.246
	16*16	**45**	16.74db	0.392	16.74db	0.471	16.74db	0.390
		90	23.64db	0.347	23.64db	0.374	23.64db	0.349
	24*24	**45**	16.74db	0.360	16.74db	0.379	16.74db	0.349
		90	23.64db	0.363	23.64db	0.380	23.64db	0.353
	32*32	**45**	16.74db	0.402	16.74db	0.488	16.74db	0.431
		90	23.64db	0.385	23.64db	0.382	23.64db	0.343
	64*64	**45**	16.74db	0.465	16.74db	0.524	16.74db	0.469
		90	23.64db	0.431	23.64db	0.451	23.64db	0.374

SYDNEY	8*8	**45**	25.51db	0.359	25.51db	0.416	25.51db	0.286
		90	24.34db	0.453	24.34db	0.310	24.34db	0.451
	16*16	**45**	25.51db	0.441	25.51db	0.258	25.51db	0.350
		90	24.34db	0.326	24.34db	0.198	24.34db	0.338
	24*24	**45**	25.51db	0.494	25.51db	0.283	25.51db	0.300
		90	24.34db	0.464	24.34db	0.332	24.33db	0.314
	32*32	**45**	25.51db	0.458	25.52db	0.356	25.51db	0.403
		90	24.34db	0.387	24.35db	0.326	24.33db	0.321
	64*64	**45**	25.51db	0.395	25.51db	0.384	25.51db	0.427
		90	24.34db	0.423	24.37db	0.348	24.33db	0.351

From table 4.26, it can be seen that the results for the image rotation are generally weak, but there are some differences between PSNR &NC. The results are shown for PSNR are the highest value in the image of Sydney. As for values normalized correlation they gave the highest value with Rotation (45) degree in the image of the airplane at the size of the watermark 64 * 64 of the proposed method.

It can be notice also, that the results for the proposed segmented DWT method are almost the same as that for the without segmentation DWT technique.

4.5 Summary

The results included in this chapter can generally be summarized as follows:-

- Acceptable results were generally found for the robustness and imperceptibility. The values of measured PSNR for the proposed segmentation algorithm were slightly less than those for un-segmented algorithm, but were within reasonable values. This decrease in the values were manifested clearly as the size of the watermark increases, as well as when the segmentation size was increased.

- Some of measurements were still unchanged and fixed performance as those for the segmentation of DWT, whereas the other measurement showed minor changes that were hardly noticeable.
- It is noticed that measured embedding and extraction time increases as the segmentation processes increase.
- The images are tested with inclusion of different types of noise, such as (salt and paper, additive, Gaussian blur) the results most of them are the similar to the results of without segmentation method no big change in results, so this study proofs a strong result (robustness, imperceptibility) against noise.
- Regarding to Cropping, Rotation effects, the results remain unsatisfactory. The badness increase when the segmentation increased especially for the Cropping. As the watermark disappear and the normalized correlation (NC) was not measured.

Chapter Five

Conclusions and Future Work

Chapter Five

Conclusions and Future Work

5.1 Conclusion

The main idea of this study was to investigate the effect of segmented process on the DWT watermarking techniques .i.e. the term segmentation was the main idea, regarding to watermark and the host image using the technique of the discrete wavelet transform (leve-2), which is a frequency domain, (DWT) that proved high performance in terms of robustness and imperceptibility, which is the core of this study.

In this study so many images with different type and sized were used for watermarking propose, however, a host image of size 512 * 512 pixels were chosen to be listed in the thesis using different sizes of the watermark sizes, namely (8 * 8, 16 * 16, 24 * 24, 32 * 32, and 64 * 64) pixels.

This study adopted two methods in order to get its results, the first one is traditional method, and the second one is proposed method.

The proposed method used the segmentation which was in two cases (2 * 2 and 4 * 4). Whereas, the traditional method used same items in the proposed method but without segmentation in order to know the effect of the segmentation on the results.

In order to evaluate the images of this study a number of measurement (PNSR, MSE, SSIM, and CORRLATION) are determined and compared. The results generally were good in terms of robustness and imperceptibility. However, the values of PNSR have decreased slightly when the size of watermark was big, and the segmentation was increased.

Some of measurements were still unchanged and fixed performance as those for the traditional DWT, whereas the other measurement showed changes that were hardly noticeable. As was calculated, the embedding and extraction time is measured, and also it is found that it is increased when the segmentation increased too.

The images are tested with inclusion of different types of noise, such as (salt and paper, additive, Gaussian blur), the results most of them are the similar to the results of traditional method. There is no big change in results, so this study proofs a strong result (robustness, imperceptibility) against noise. Regarding to Cropping, Rotation effects, the results remain unsatisfactory. The badness increase when the segmentation increased especially for the Cropping. As the watermark disappear and the normalized correlation (NC) was not measured.

5.2 future works

Some suggestions can improved the proposed technique in future working methods, but the most important suggestions in order to increase the strength of the watermark system and the possibility of solving the problems that have emerged in the study:

1. Use color images that have a large capacity compared to grayscale images. After the basic colors are separated, it is better to use the watermark using the blue color less sensitive to human visual system.
2. The possibility of finding a solution to the problem of loss of watermark, which was observed when using Cropping.
3. Different segmentation scheme may be investigated and may prove useful, such as selection areas rather than even segmentation.

Reference

Abbate, J. (1999). "The electrical century: Inventing the Web". Proceedings of the IEEE, 87 (11).

Abbasfard, M. (2009). "Digital image watermarking robustness: A comparative study" (Doctoral dissertation, TU Delft, Delft University of Technology).

Abdullatif, M., Khalifa, O. O., Olanrewaju, R. F., & Zeki, A. M. (2014, September). "Robust image watermarking scheme by discrete wavelet transform". In Computer and Communication Engineering (ICCCE), IEEE 2014 International Conference on (pp. 316-319).

Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd Salleh, (April, 2011). "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", Journal of Computing, ISSN 2151-9617, vol. 3, issue 4.

Abou Ella Hassanien,(2006)."A Copyright Protection using Watermarking algorithm Informatica", 2006, Vol. 17, No. 2, PP 187–198.

Ahmad, A., Sinha, G. R., & Kashyap, N. (2014). "3-Level DWT Image Watermarking Against Frequency and Geometrical Attacks", International Journal of Computer Network and Information Security (IJCNIS), 6(12), 58.

A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi (Oct. 2001). "A survey on watermarking application scenarios and related attacks", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993.

Awad, A. (2017). "A Survey of Spatial Domain Techniques in Image Steganography", Journal of Education College Wasit University, 1(26), 497-510.

Cayre, F., Fontaine, C., & Furon, T. (2005, September). "A theoretical study of watermarking security. In Information Theory", IEEE, ISIT 2005. Proceedings. International Symposium on (pp. 1868-1872).

C. C. Chang, J. Y. Hsiao, and C. S. Chan, (2003). "Finding optimal least significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, vol. 36, no. 7, pp. 1583–1595.

Chopra, D., Gupta, P., Sanjay, G., & Gupta, A. (2012). "LSB based digital image watermarking for gray scale image", IOSR Journal of Computer Engineering (IOSRJCE) ISSN, 2278-0661.

Choudhary, R., &Parmar, G. (2016, November). "A robust image watermarking technique using 2-level discrete wavelet transform (DWT)", In Communication Control and Intelligent Systems (CCIS), IEEE, 2016 2nd International Conference on (pp.120-124).

Cox, IJ, Miller, ML & Bloom, JA, (2002). "Digital Watermarking", Morgan Kaufmann Publisher, San Francisco, CA, USA.

Daemen, J., Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard, Springer, Heidelberg.

Darshana Mistry,(2010). "Comparison of Digital Watermarking methods", 21st Computer Science Seminar SA1-T1-7, IJCS.

Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, (Sep-Oct. 2012). "LSB Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1, pp. 36-41.

Divjot Kaur Thind, Sonika Jindal, (2014). "A Semi Blind DWTSVD Video Watermarking", International Conference on Information and Communication Technologies (ICICT 2014), Elsevier Proceedings of Computer Science 46, 2015, pp. 1661 – 1667.

Er-Hsien Fu, (1998). "Literature Survey on Digital Image Watermarking", EE381K Multidimensional Signal Processin.

ETY NAVON, OFER MILLER*, AMIR AVERBUCH, (2005). "Color Image Segmentation Based on Adaptive Local Thresholds, School of Computer Science", Tel-Aviv University, Israel.

Fabien A. P.Petitcolas, Ross J. Anderson and Markus G. (1999, July). "Information hiding-a survey", Proceedings of the IEEE, vol. 87, pp. 1062-1078.

F. Hartung and M. Kutter, (July, 1999). "Multimedia watermarking techniques", Proc. IEEE, vol. 87, pp.1-79-1107.

Jonathan M. Bloom, Revolution by the Ream: A History of Paper, Saudi Aramco World May/June 1999 print edition, vol. 50, pp. 26-39, May/June 1999. Available: http://archive.aramcoworld.com/issue/199903/revolution.by.the.reama.history.of.paper.htm.

Hai Gao, Wan-Chi Siu, and Chao-Huan Hou, (December, 2001). "Improved techniques for automatic image segmentation". IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 12.

https://www.fiverr.com/metadesign0/convert-any-of-bitmap-design-to-vector last visited in 15/4/2018.

Huda, S., (2001). "Quantum analysis of noise in photonic system", M.Sc. thesis, physics Dept., College of Education for Women, Baghdad University.

Indradip Banerjee, Souvik Bhattacharyya, and Gautam Sanyal, (2012). "Text Steganography through Quantum Approach", 6th International Conference on Information Processing, ICIP 2012, Bangalore, India, August, pp 632-653.

Gaurav N Mehta, Yash Kshirsagar, Amish Tankariya, (April, 2012). "Digital Image Watermarking: A Review", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.2 pg:169-174 01.

Goyal, R., & Kumar, N. (2014). "LSB Based Digital Watermarking Technique". International Journal of Application or Innovation in Engineering & Management (IJAIEM), 3(9), 15-18.

Giuseppe Schirripa Spagnolo, C. Simonetti, L. Cozzella, (2005). "Content fragile watermarking based on computer generated hologram coding technique", J. Opt. A: Pure Appl. Opt. 7(7), 333-342.

Khanzode, P., Ladhake, S., & Tank, S. (2011). "Digital watermarking for Protection of Intellectual Property". IJCEM, 12.

Lai, Y., HU, B., Martin, R. (2009). "Automatic and Topology Preserving Gradient Mesh Generation for Image Verification" .ACM Trans. Graph.28.

L. Jian and H. Xiangjian, (2005). "A review Study on Digital Watermarking in Information and Communication Technologies", 2005. ICICT. First International Conference on, 2005, pp. 337-341.

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics", IET Image Processing, 10(1), 34–52.

M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies. (April, 1992). "Image coding using wavelet transform", IEEE Trans, Image Proc., 1(2):205–220.

Mahmoud El-Gayyari, (2006) .Watermarking Techniques Spatial Domain Digital Rights Seminar ©‖, Media Informatics University of Bonn Germany.

M. Holliman and M. Young, (2002). Watermarking for automatic quality monitoring, in SPIE Electronic Imaging, Proc. SPIE Security and Watermarking of Multimedia Contents, San Jose, CA, USA 4675.

Manpreet Kaur , Sonika Jindal , Sunny Behal (February 2012) . "A Study of Digital Image Watermarking", IJREAS Volume 2, Issue 2 ISSN: 2249-3905, pp. 126-136.

Patrick Vandewalle, Sabine Susstrunk and Martin Vetterli, (2006). "A frequency domain approach to registration of aliased images with application to super resolution", EURASIP J. Appl. Signal Process.

Peng, H., Wang, J., & Wang, W. (2010). “Image watermarking method in multiwavelet domain based on support vector machines”. Journal of Systems and Software, 83(8), 1470-1477.

Pintelon, R., Guillaume, P., Rolain, Y., Schoukens, J., and Van Hamme, H. (1994). “Parametric identification of transfer functions in the frequency domain-a survey”, IEEE Trans. Autom. Control, AC-39, No. 11, pp. 2245– 2260.

Prabhishek Singh, R S Chadha .(March , 2013) . “A Survey of Digital Watermarking Techniques”, Applications and Attacks, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9.

Preeti Gupta, (September, 2012). “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research, Volume 3, Issue 9, ISSN 2229-5518.

Provos, N., & Honeyman, P. (2003). “Hide and seek: An introduction to steganography”. IEEE security & privacy, 99(3), 32-44.

Raymond H. Chan, Chung-Wa Ho, and Mila Nikolova. (October, 2005). “Salt-and- pepper noise removal by median- type noise detector and detail- preserving regularization”, IEEE Transaction on image processing, vol. 14, No. 10.

R M Gouda, Priya Pise. (January, 2012). “Compression Technique using DCT & Fractal Compression – A Survey”, IFRSA‟s International Journal of Computing, Vol2, issue 1.
Shahinfard, E., & Kasaei, S. (2003). Digital image watermarking using wavelet transform. In Iranian Conference of Mechatronics Engineering, ICME, Qazvin, Iran (pp. 363-370).

Sharma Manoj Kumar and P. C. Gupta, (2012). “A Comparative Study of Steganography and Watermarking”, International Journal of Research in IT &Management, Vol. 2, PP. 2231-4334.
Sharma, P., & Swami, S. (2013). Digital image watermarking using 3-level discrete wavelet transforms. In Conference on Advances in Communication and Control Systems, Vol. 24, pp. 3-24.

Singh AK, Kumar B, Dave M, Mohan, (2015). “A Multiple watermarking on medical images using selective DWT coefficients”, J Med Imaging Health Informatics, American Scientific Publisher, USA, vol. 5, 1-8.

S. Katzenbeisser and F. A. P. Petitcolas, (2000). “Information hiding Techniques for Steganography and Digital Watermarking”, Artech House.

S. Liu, B. M. Hennelly, C. Guo, and J. T. Sheridan, (2015). “Robustness of double random phase encoding spread-space spread-spectrum watermarking technique,” Sig. Process. 109, 345–361.

Sun, Y., Zhan, R., Han, Z., & Lin, Q. (2015, November). “A Watermark algorithm for Image Content Authentication and Correcting Errors in Terms of Pixels”. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE, 2015 10th International Conference on (pp. 760-765).

Thanh, T. M., & Tanaka, K. (2014, September). “A proposal of novel q-DWT for blind and robust image watermarking”. In Personal, Indoor, and Mobile Radio Communication (PIMRC), 2014 IEEE 25th Annual International Symposium on (pp. 2061-2065).

Thulasimani, L., Madheswaran, M. (2010). “A single chip design and implementation of aes128/192/256 encryption algorithms”. International Journal of Engineering Science and Technology 2(5), 1052–1059.

T. Morkel, J.H.P. Eloff, and M.S. Oliver, (2005). “An overview of image steganography”, in Proc. ISSA, pp. 1-11.

Yusnita Yusof and Othman O. Khalifa, (2007). “Digital Watermarking For Digital Images Using Wavelet Transform”, IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, May, Penang, Malaysia.

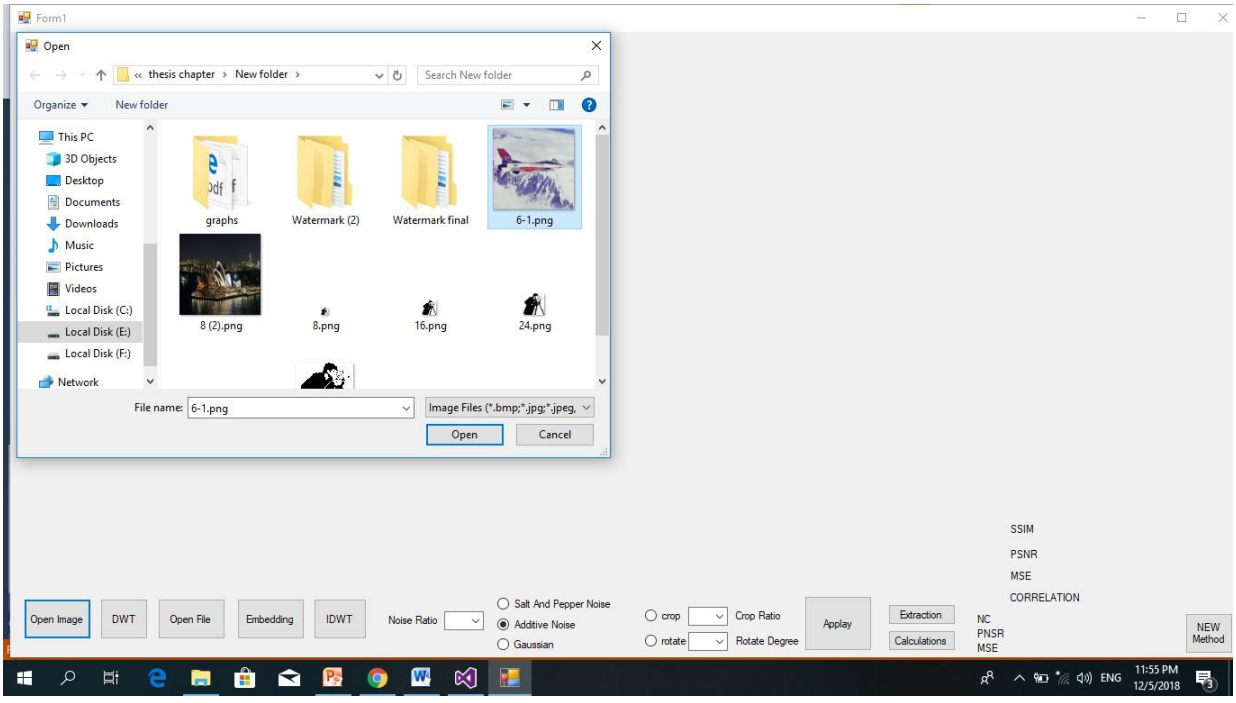
Appendices

Graphical User Interface (GUI) for used algorithm and tests implementations

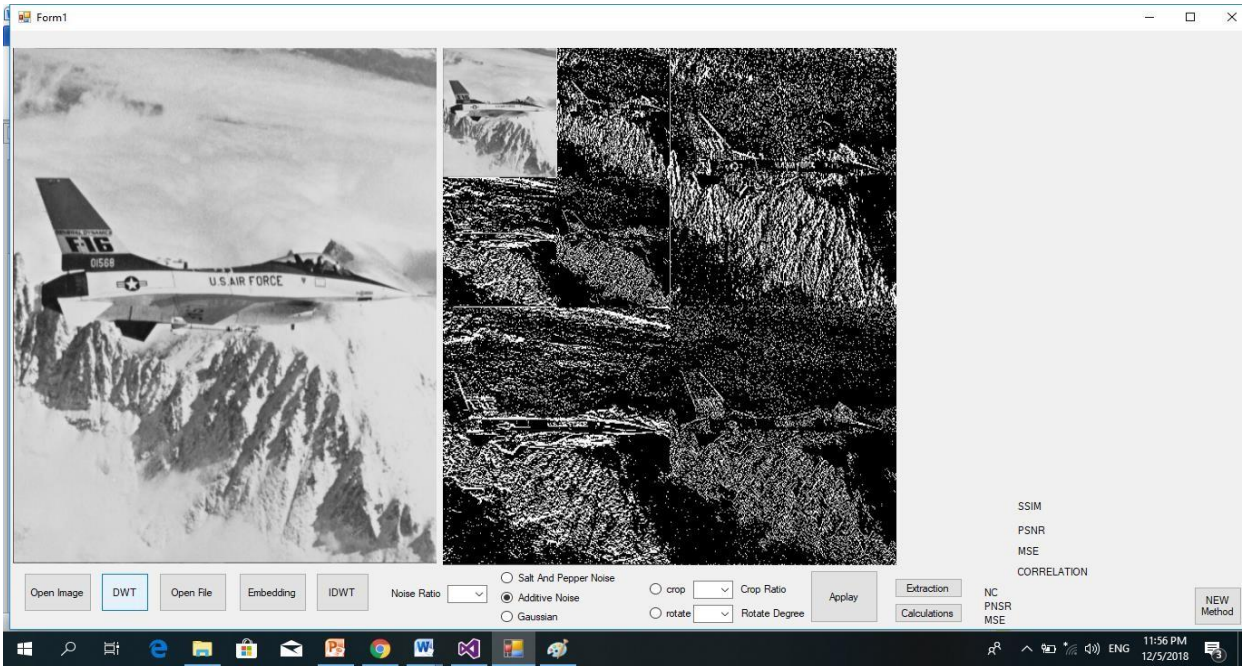
The proposed watermarking scheme is user to simplify implemented program using GUI. It allows the user to embed different sizes of logos from a database also can be selected carrier image from another file. These processes of embedding about the traditional and proposed methods in two cases (2*2) & (4*4) can be illustrated as shown in the following steps:

Appendix A: Modulation Process (traditional method)

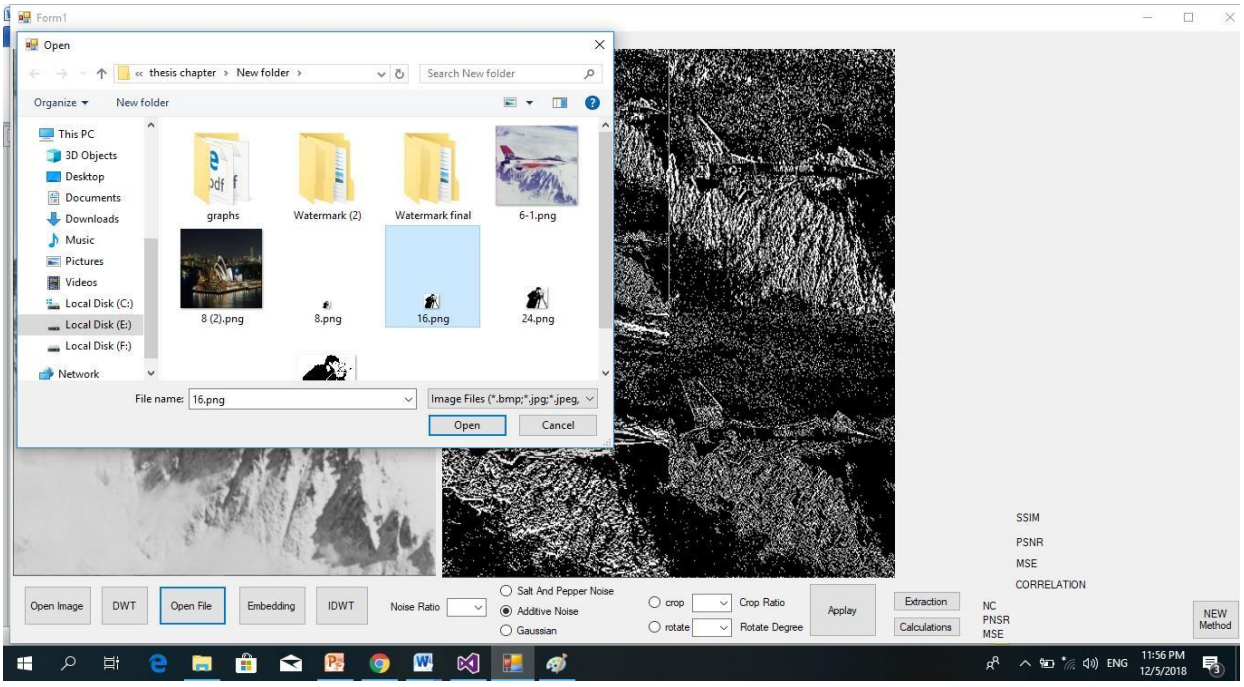
Step1: Selected carrier image which used to traditional & proposed method, the database that is available in the carrier folder as shown in Figure a.1.



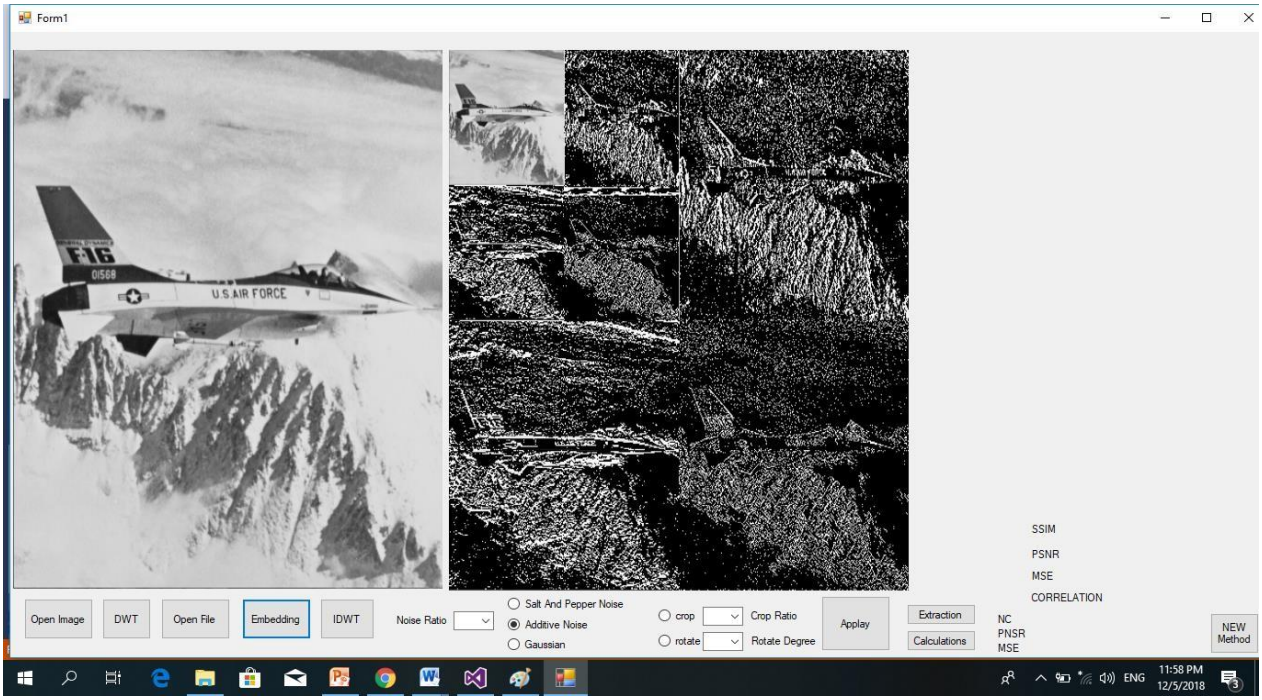
Step 2: after select carrier image should executed discrete wavelet transform -2 level technique as shown in Figure a.2.



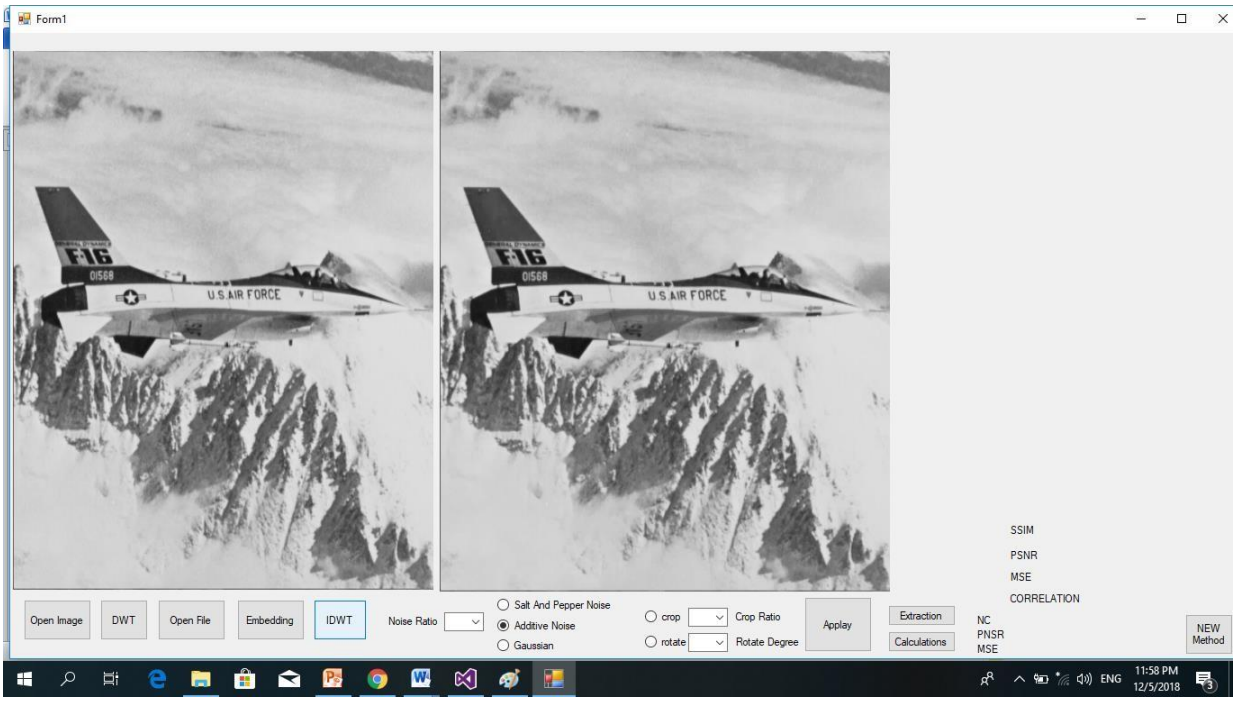
Step 3: We select the watermark from the file and specify the size we want to include in the carrier image as shown in Figure a.3.



Step 4: embed the selected watermark that uses itself in both the traditional and proposed method and in both cases as shown in Figure a.4.

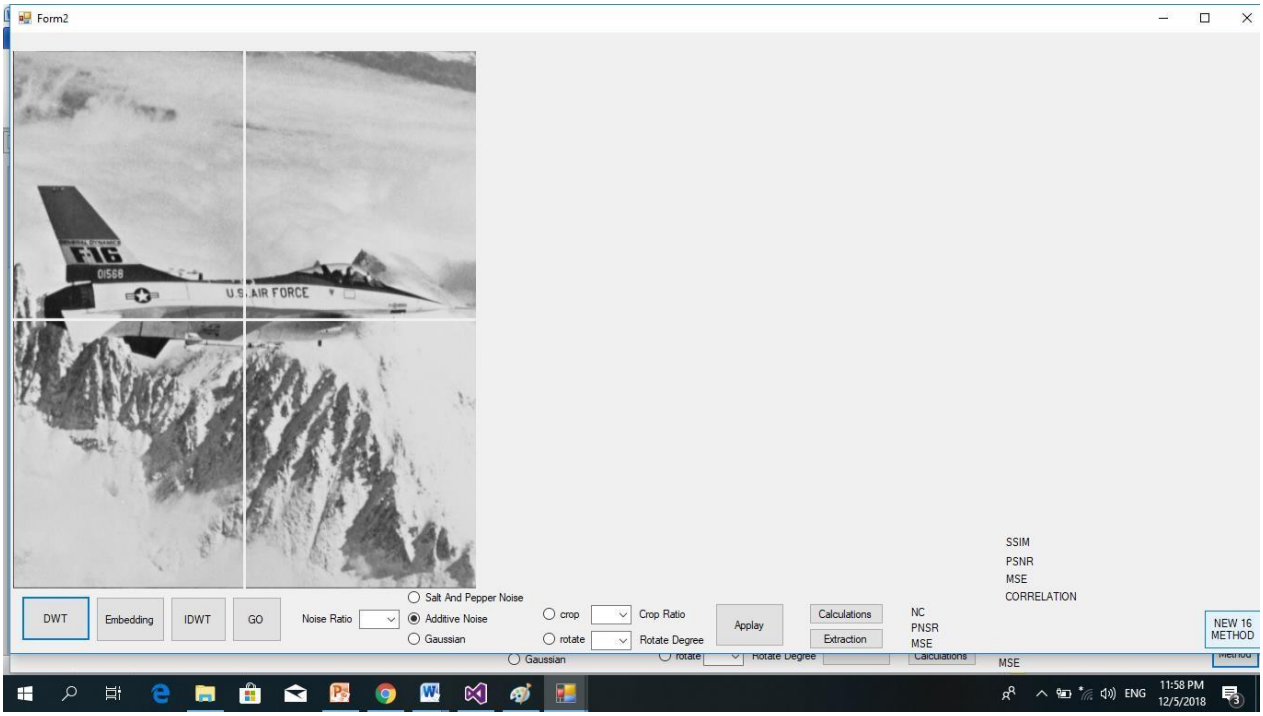


Step 5: use a (IDWT) feature to obtain a watermarked image after the logo is embedded inside it as shown in Figure a.5.

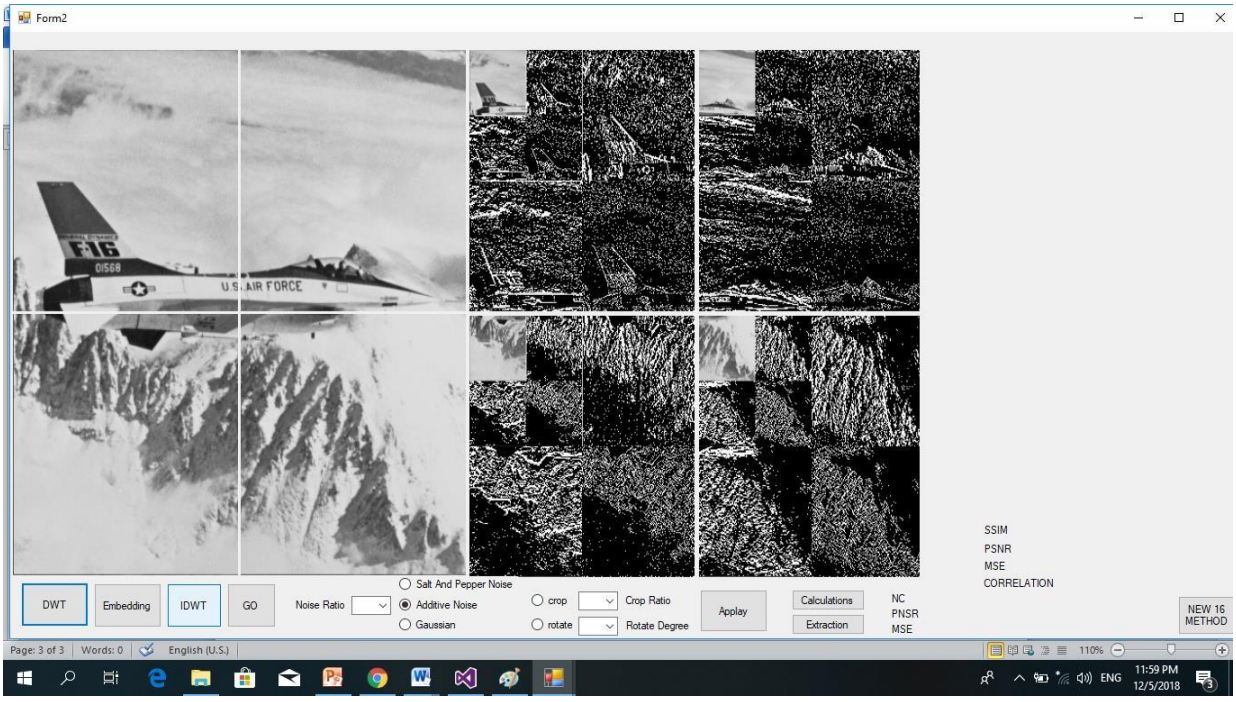


Appendix B: Modulation Process (proposed method) case (2*2).

Step 1: Use the same carrier image chosen in the traditional method but here we use the segmentation in a case (2 * 2) as shown in Figure B.1**.**

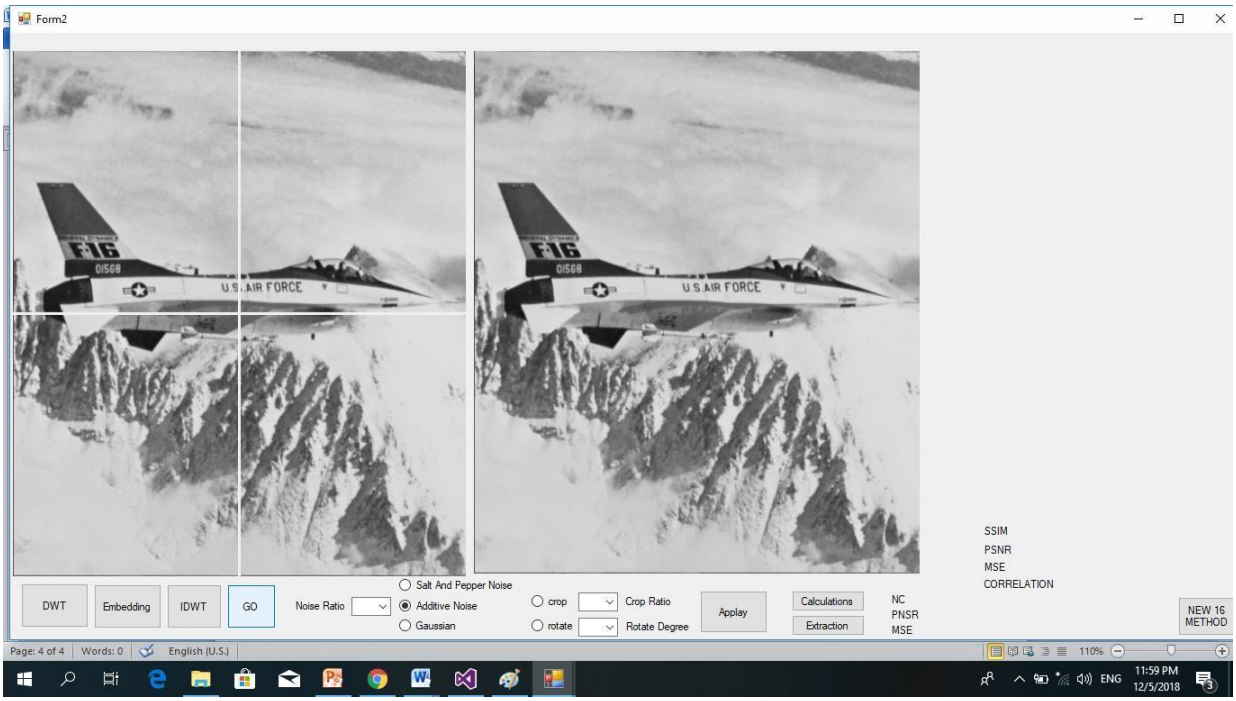


Step 2: apply discrete wavelet transform - 2 level technique for each segment of the carrier image and after that embedding each part of the watermark(2*2) inside each part of the carrier image (2*2) as shown in Figure B.2.



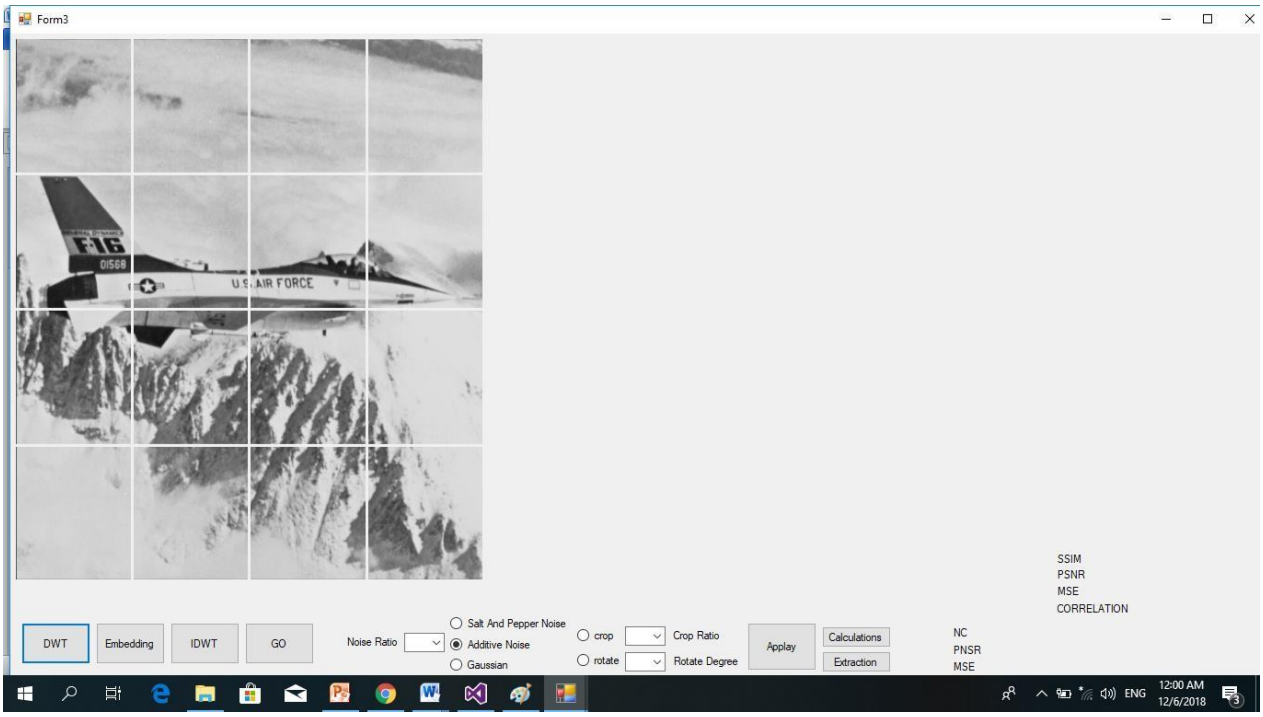
Step 3: retrieve segment image using (IDWT) as shown in Figure B.3.

Step 4: Restore the image with a watermark in full form without segmentation as shown in Figure B.4.

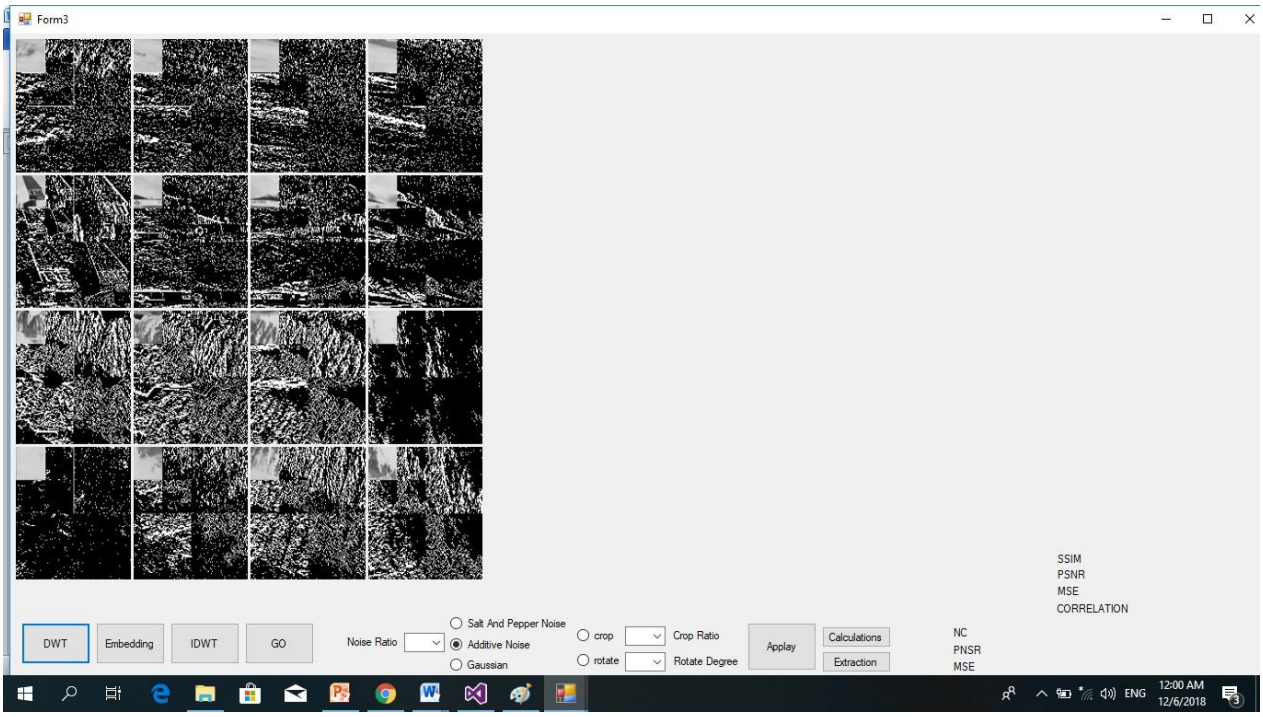


Appendix C: Modulation Process (proposed method) case (4*4).

Step 1: divided the carrier image into (4*4) as shown in Figure C.1



Step 2: apply discrete wavelet transform - 2 level technique for each segment of the carrier image and after that embedding each part of the watermark(4*4) inside each part of the carrier image (4*4) as shown in Figure C.2



Step 3: retrieve segment image using (IDWT) and Restore the image with a watermark in full form without segmentation as shown in Figure C.3