Sudan University of Science and Technology

College of Graduate Studies

College of Computer Science and Information Technology

Evaluating Performance of Text Watermarking in Digital Images

تقويم الأداء في العلامات المائية للنص في الصور الرقمية

Thesis submitted in partial fulfillment of the academic requirements for the degree of Master in Information Technology

Presented By:	**Supervised By**:
Mai Khairy Abdaljaleel	Dr. Mohammed Elghazali Hamza

2022

الآيات

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

اقْرَأْ بِاسْمِ رَبِّكَ الَّذِي خَلَقَ (1) خَلَقَ الْإِنْسَانَ مِنْ عَلَقٍ (2) اقْرَأْ وَرَبُّكَ الْأَكْرَمُ (3) الَّذِي عَلَّمَ بِالْقَلَمِ
(4) عَلَّمَ الْإِنْسَانَ مَا لَمْ يَعْلَمْ (5)

صدق الله العظيم

« سورة العلق الآيات من (1) ــ (5) »

Dedication

This thesis is dedicated, with deepest love and everlasting respect, to numerous precious persons.

To my parents for their continuous love, support and encouragement which helped me to achieve my dream.

To my family and all my friends, for their support and patience throughout these stressful years.

To the principles of each and every ambitious person who knows that patience and hard work make the dreams.

Acknowledgment

Firstly, all praise is due to Allah, without his immeasurable blessings and favors none of this could have been possible. During the course of this research, there have been numerous people who have provided me with guidance, inspiration and support for completing this thesis.

I would like to express my thanks and gratitude to my supervisor Dr. Mohammed Elghazali for his patience, motivation, encouragement and continuous scientific support at all stages of this research, and also for sharing his immense knowledge and for his useful and valuable advices, his involvement proved vital to the completion of this thesis. Thanks are also due to the Sudan University of Science and Technology College of computer science and all its faculty members of who were generous in their teaching and academic services. On the personal front, I would like to express my gratitude to my family, for their continuous love, support and sincere prayers during the course of this research. Finally, very special thanks to my friends for the motivation and unconditional support along the way.

Table of Content

List of Tables

List of Figures

List of Abbreviations

LSB	Least-Significant Bit
DCT	Discrete Cosine Transform
FFT	Fast Fourier Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
DLT	Discrete Laguerre Transform
DHT	Discrete Hadamard Transform
HVS	Human Visual System
SVD	Singular Value Decomposition
MSB	Most Significant Bit
PSNR	Peak Signal-to-Noise Ratio
MSSIM	Multi-Scale Structural Similarity Index Measure
NCC	Normalized Cross Correlation
RGB	Red-Green-Blue
WRA	Watermarked Removal Attack
AWGN	Additive White Gaussian Noise
S & P	Salt and Pepper Noise
PDF	Probability Density Function
YCbCr	Y Luminance, Cb Blue Difference, and Cr Red difference
DC	Direct Current
AC	Alternate Current
ZZ	Zigzag Scan
RLE	Run Length Encode
DIP	Digital Image Processing

DSP	Digital Signal Processing
SSM	Spread Spectrum Modulation

Abstract

Copyright protection and ownership proof of digital multimedia (such as text, audio, images and videos) nowadays are achieved using digital watermarking technique. This thesis, used a text watermarking method for protecting the property rights and ownership judgment of multimedia. However, it focuses on the process of hiding a small text or owner information in images. In this thesis, two watermarking domains techniques are introduced which are spatial domain and frequency domain by comparing three different watermarking techniques which are LSB, DCT and FFT. The LSB is considered the basic and traditional technique which is a special domain watermarking technique, while DCT and FFT are the frequency domain watermarking technique. The Evaluation extended to include investigation of different types of watermarking attacks namely geometrical attacks and noise attacks. Also, different types of image formats are evaluated which are the BMP, JPG, PNG, and TIFF. Finally watermark extraction results and image evaluation performance metrics (PSNR, NCC and MSSIM) are mathematically described, and the impact of watermarking techniques, types of image format, and different types of attacks on these evaluation performance metrics. The used text watermarking method is suitable for SMS text messages embedded in digital image for the purpose of copyright protection and proprietary rule applications, rather than applying steganography that is used for secure information exchange purposes.

المستخلص

تتم حماية حقوق الطبع وأحكام الملكية الفكرية للوسائط الرقمية المتعددة (كالنصوص والصوت والصور الثابتة والمتحركة) في الوقت الحالي بإستخدام العلامات المائية الرقمية. في هذا البحث تم إستخدام خوارزمية للعلامات المائية النصية لحماية حقوق وأحكام الملكية للوسائط المتعددة. وهي تركز على عملية الإخفاء لنصوص صغيرة أو معلومات المالك في الصور. في هذه الدراسة ، تم استخدام إثنين من تقنيات مجالات العلامات المائية وهما المجال المكاني ومجال التردد من خلال مقارنة ثلاث تقنيات مختلفة للعلامة المائية وهي إل إس بي ، دي سي تي، إف إف تي . تعتبر إل إس بي هي التقنية الأساسية والتقليدية وهي تقنية العلامة المائية للمجال المكاني ، بينما دي سي تي و إف إف تي هي تقنية العلامة المائية لمجال التردد. إمتد التقييم ليشمل التحقيق في أنواع الهجمات المختلفة على العلامات المائية مثل الهجمات الهندسية وهجمات الضوضائية. يتم أيضًا تقييم أنواع الصور المختلفة وهي بي إم بي، جيه بي جي ، بي إن جي، تي آي إف إف. ثم يتم حساب نتائج استخراج العلامة المائية ومقاييس أداء تقييم الصور (بي إس إن آر، إن سي سي، إم إس إس آي إم) رياضياً، وتأثير كل من تقنيات العلامات المائية وأنواع الصور وأنواع الهجمات المختلفة عليها. المنهجية المستخدمة لوضع العلامة المائية النصية مناسبة للرسائل النصية القصيرة المضمنة في الصورة الرقمية لغرض حماية حقوق النشر والملكية الفكرية ، بدلاً من تطبيقات إخفاء المعلومات التي يتم استخدامها لأغراض تبادل المعلومات بشكل آمن.

Chapter One

Introduction

1.1 Overview

As computers and internet became more dispersed in our daily lives, protecting digital media, such as text, image, audio, and video files during storage or transit from being leaked, modified, misused, or stolen and claimed by others is a crucial mater. Information Security became more of an issue of preserving data and protecting its copyrights, ownership, and validity, as well as keeping the secrets not being unveiled to unauthorized persons. Sending confidential data over internet is risky task. The primary concern is to protect data from intruders. Information security can be classified into two types; Cryptography and Data Hiding. In cryptography the clear text is converted into cipher text by means of some procedures and secret keys, whereas in data hiding the clear text is embedded into another multimedia with unnoticeable effect. Therefore, cryptography serves the purpose of protecting data or information from being leaked, tampered with or modified during storage or transit over the communication channels. On the other hand, data hiding comes into two types; steganography by hiding secret messages into multimedia, and watermarking which serves to protect the multimedia by embedding certain information into it to be used for copyright protection and ownership judgement.

So many watermarking techniques were developed ranging from the simple least significant bit (LSB) to the sophisticated transformation techniques such as discrete wavelet transform (DWT), and discrete Fourier transform (DFT). [1]

For some applications, the speed of embedding text or signature watermarks into images is required, hence LSB technique is suitable for being simple and comparatively fast than other techniques. This thesis is concerned with watermarking; hence it will give an introduction to data hiding techniques first and then will suggest and test a modified watermarking scheme for hiding text watermarks into still images. Over the internet the most widely used medium for the communication is image. There is various type of image file such as jpg, jpeg, png, bmp, tiff, gif, type and many more, which required more security and safety from the various violators of copyright.

Digital watermarking is the method of embedding an identical watermark within the content for the reason to protect the content from unauthorized copying and from other copyright violation. The whole procedure in which to embedding the watermark within the content and extract the watermark from the content is to verify the original copyright author of that content or data is known as the digital watermarking. The principles used by an image, video and audio watermarking is same as the principles of text watermarking. For various tempering attacks the watermark should stay durable and they are untraceable to any other third party except the original creator of the text, at the same time the watermark can be simply and completely reproducible automatically through the watermark extraction algorithm. [1]

1.2 Research Questions

The proposed work in this thesis is supposed to answer the following questions:

1. What would be the effectiveness of the environment effects such as noise and deformation on extracted watermark?
2. What is the effect of different Attack and external factors on watermarked image? And what the effect of attacks in evaluation performance?
3. How much effect of embedded watermark on the image size? And does the format of image affect the evaluation performance?
4. What are the main enhancements and weaknesses of the used watermarking scheme? And what are the most important suggestions that we may recommend?

1.3 Problem Statement

The wide spread of digital communication over the internet have exposed paintings, digital images, private medical documents, X-ray scans, national security maps, etc. to the serious situation of being easily copied, misused, and possibly claimed by people other than their creators. Therefore, protecting copyrights and ownership judgment problem of digital assets became an essential matter nowadays. This problem has escalated the research in the field of watermarking, resulting into so many techniques and tools with different speed and efficiency. These watermarks can be of any digital data type and might be visible or invisible that are either robust or fragile depending on their aim and the application. The aim of this thesis is to use and test a watermarking technique that is fast and secure. An evaluation of both spatial and frequency domain watermarking techniques is introduced by comparing three different watermarking techniques which are the LSB, DCT, and FFT. These techniques used for hiding the text watermark in image to produce a high level of imperceptibility and content authentication.

1.4 Research Objectives

- To reduce illegal copying, forgery, redistribution and copyright violations in digital image. Similarly, decrease unprotected digital image for send and transmit over the internet.
- To establish a fast text watermark embedding scheme as notes or signature that used for protecting the property rights and support ownership judgment of images or paintings using spatial and frequency domain watermarking.
- To determine the various environmental disturbances and the effects of noise addition, filtering, rotation, skewing.

1.5 Motivation

During exchange of multimedia (such as images which are the subjects or this thesis) over communication channels or the internet, unauthorized users might download these images and claim their ownership, use them socially or commercially, hence digital techniques are sought to do the protection. The significance of the used watermarking scheme is to increase imperceptibility and robustness of watermarking technique using a spatial domain and frequency domain which is less complex than other techniques. The short text information or signature are embedded into the images. The used methodology introduces an improved approach to protect the image for the purposes of copyright, ownership and intellectual property.

1.6 Research Scope

Watermarking techniques are commonly used nowadays for copyright protection, ownership proof and dispute judgments for digital multimedia. The scope of the research in this thesis will be limited to embedding of text digital information into images (different image type of format), and will be involved with spatial domain and frequency domain. I will also cover Different options are performed for attack type, image format and embedding mechanism, and finally show extraction results and image evaluation performance metrics.

1.7 Thesis Layout

This thesis contains five chapters. Chapter one includes an introduction of digital watermarking, the problem statement, objective of the study in the thesis, motivation and the scope and limitations. Chapter two includes information hiding, digital watermarking classification, watermarking properties, watermarking application, digital watermarking attacks, image processing techniques, image watermarking domains techniques, metrics for evaluating image quality, properties and techniques used for watermarking, and literature review. Chapter three considers two main parts of watermarking domains techniques which are the spatial domain watermarking and frequency domain watermarking for embedding text watermarking in digital image, and mathematically describe image evaluation performance metrics. Chapter four presents the implementation and results. Chapter five presents conclusions and suggestions for recommendations.

Chapter two

Literature Review

2.1 Introduction

This Chapter covers the theoretical background of watermarking techniques in general and the related work. It includes digital watermarks classification, properties, and application of watermarking first, then describes important watermarking techniques, and attacks. Finally, a literature survey of the related works is included.

Text watermarking is a challenging area of research and the volume of work done in the past in this area is quite inadequate. Text watermarking began in 1993 with the advent of the Internet. After this, a number of text watermarking techniques have been proposed. These include text watermarking using text images, synonym based, pre supposition based, syntactic tree based, noun-verb based, word and sentence based, acronym based, typo error based methods and many others.

2.2 Digital Watermarking

The process of embedding a digital watermark into a digital image that carries information unique to the copyright owner or the creator of the document is called Digital Text Watermarking. An illicit re-distribution and reproduction of images information and copyright violations can be avoided by applying text watermarking methods. Watermarking solutions for image already in place and a number of research groups are working in these domains. Images is an extensively used medium travelling over the internet for information exchange. The major component of websites is the image file; therefore, it is necessary to protect it. Digital watermarking solution for image protection is the need of the day. Text watermarking is an important area of research; however, the previous work on digital text watermarking is quite insufficient [2].

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly and it quickly became clear that people wanted to exchange and download pictures, music, and videos. The internet is 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. Hence watermarking has been considered for copyright protection and ownership judgement applications and many copy prevention. In copy prevention, the watermark may be used to inform software or hardware devices that copying should be restricted. In copyright protection applications, the watermark may be used to identify the copyright holder and ensures proper payment of royalties. Although copy prevention and copyright protection have been major driving forces behind research in the watermarking field, there are a number of other applications for which watermarking has been used or suggested. These include broadcast monitoring, transaction tracking, authentication, copy control, and device control. [3]

2.3 Information Hiding, Steganography, and Watermarking

Information hiding, steganography, and watermarking have a great deal of overlap and share many technical approaches. However, there are fundamental philosophical differences that affect the requirements, and thus the design, of a technical solution [4]. The differences between these three terms are briefly discussed here.

Information hiding is a general term that include covert channels, anonymity, steganography, and watermarking. It means embedding secret information or messages into a cover multimedia (such as text, audio, image or video) and ensures that they do not raise any suspicion of their existence during their storage or transfer. Historically, people used hidden tattoo and invisible ink to transfer these hidden contents or messages. Today, in the digital era, computer technologies and networks have made it easy to send digital data over communication channels. Such data can be used to hide secret information, basically, the process of digital information hiding system begins with identifying redundant bits in the multimedia cover (i.e., those bits that can be modified without destroying the integrity of that medium). This merger creates a medium stego by planting the data to be hidden in the place of the redundant bits. The aim is to hide information and to maintain the existence of the message undetectable by unauthorized access [5].

Steganography is a term derived from the Greek words steganos, which means "covered or hidden" and graphia, which means "writing". It includes a vast number of methods used for secret communications by concealing the very existence of secret messages. In short, it is the art of concealed communication. A steganography system thus embeds secret content into unremarkable cover media so as not to arouse an eavesdropper's suspicion. Hence Computer-based steganography techniques introduce changes to digital covers to embed information foreign to the native covers [5].

Digital watermarking is also the act of hiding digital data into another digital multimedia, therefore, it is a concept closely related to steganography, in that they both hide messages inside a digital multimedia. However, what differs is their goal, as watermarking is used to embed information such as logo or signature related text into the actual content of the digital media to protect it, while in steganography, the multimedia is only a cover that holds the secret message and has nothing to do with it. The cover multimedia is used merely as a cover to hide the existence of the message. Hence, watermarking is used for ownership judgement and copyright protection while Steganography is used for secret message exchange [6].

Watermarking has been around for several centuries, in the form of watermarks initially found in plain paper and then in stock. However, the development of the field of Digital

Watermarking is only during the last 15 years or so, but is now being used in many different applications.

2.3.1 Steganography vs. Digital Watermarking

In order to outline the differences between steganography and digital watermarking techniques, their various features are summarized in Table (2-1) [7].

Table 2-1: Comparison of Steganography with Watermarking

Steganography	Digital Watermarking
Steganography conceals a message, where hidden message is the object of the communication.	Digital Watermarking extends some information that may be considered attributes of the cover such as copyright.
Always invisible.	Mostly visible.
Steganography tools hide large blocks of information.	Watermarking tools place less information in digital data.
Steganography is usually involves very limited number of people, only two in most cases.	Watermarked products can be distributed freely among large groups of people.
Stenographic communication is usually point-to point or one to few.	Watermarking techniques are usually one- too- many points.
The existence of the hidden data is not known to the parties, so they will not have the interest in getting the embedded data.	Its popular application, it gives proof of ownership, so the existence of the hidden data is known to the parties, and they have the interest of removing it.
It is not robust against modification of the data, or has limited robustness.	Its technique is more robust to attacks such as compression, cropping, and some image processing.

2.3.2 Information-Hiding Techniques Classification

Information hiding (or data hiding) is a general term encompassing a wide range of problems beyond that of embedding messages. It can be classified as shown in the diagram of Figure (2-1).

Information hiding covers covert channels, anonymity, steganography, and copyright watermarking techniques. Detailed definitions and descriptions of all these terms can be found in [8].

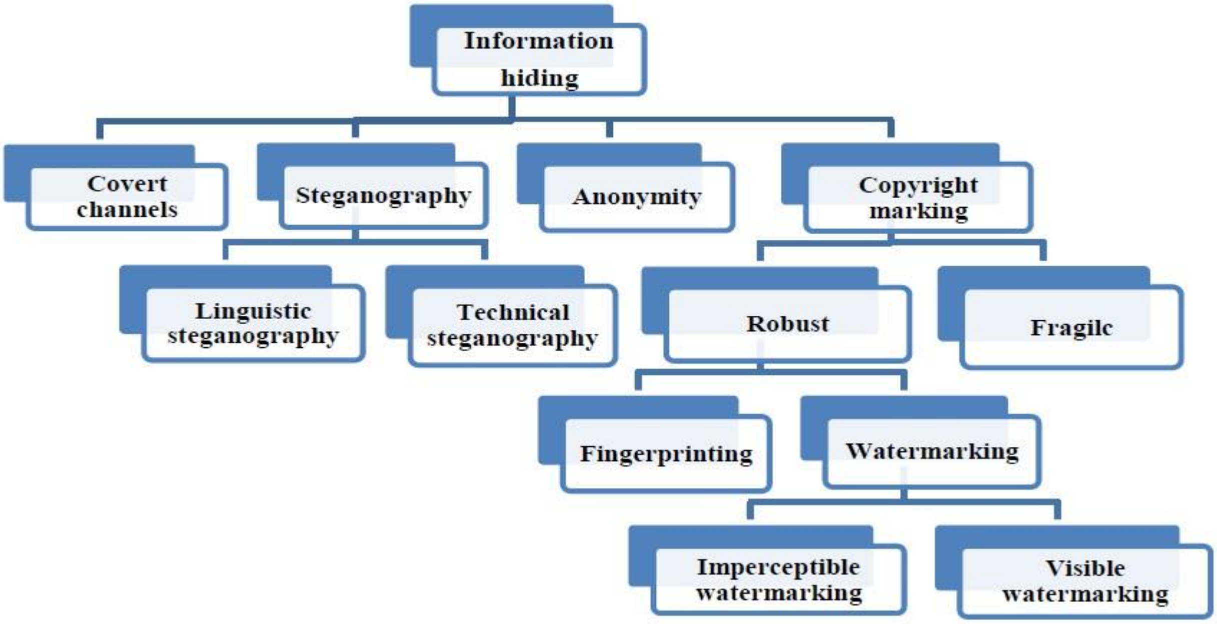


Figure 2-1: A Classification of Information-Hiding Techniques [8]

Moreover, another very common data hiding classification is done according to the technical way of hiding, which come in two types or domains; time domain (or spatial domain) and frequency domain (or transformation domain).

2.4 Digital Watermarking Classification

Watermarking is a branch of information hiding which is used to embed some information into multimedia data like digital images, text documents, audios, or videos. The importance of watermarking stems from the purposes for which it is copyright protection, multi-media authenticity, and ownership proof, preventing misuse of sensitive information, and hiding crime traces [9].

Generally, digital watermarking techniques can be classified into different categories according to host type, perceptibility, extraction method, domain, and robustness as illustrated in Figure (2-1), and briefly defined below:

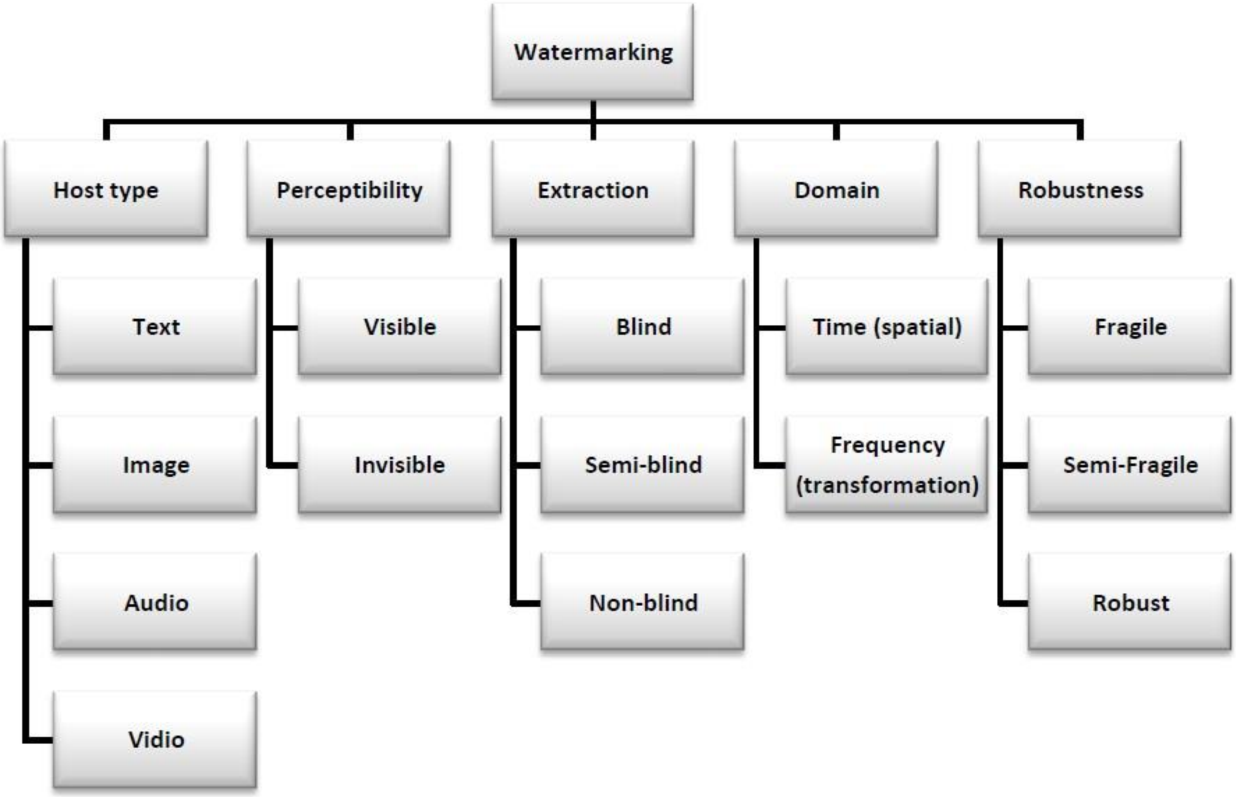


Figure 2-2: Digital Watermarking Classification [9]

According to host type: The watermarked multimedia host can be text, image, audio, or video files. Text watermarking is the oldest type and is the most difficult kind of watermarking type among all, largely due to the relative lack of mark information in the text, as the structure of text documents is identical with that observed by the user, while in the other types of multimedia, the structure of the document is different from the observed one. Basically, in text documents, one can embed information by introducing changes in the structure of the document without making a noticeable change in the concerned output [10]. Watermarking of the image, audio, and video files relies on the imperfection of the human senses. For example, minor modifications of the pixel intensities may not be noticed by the naked eye. However, human ear is much more sensitive than other sensory motors. Thus, good audio watermarking schemes are difficult to design. On the other hand, digital video is a sequence of still images, providing large video bandwidth which means that large amount of information can be easily embedded into videos [11].

***According to the perceptibility*:** Digital watermarks can be classified into either visible or invisible types. For visible, the watermark is intended to be seen by naked eye like on the watermarked media, such as the watermark on bank notes and the television Channels logos on TV screens, i.e. publicly declare the ownership of the asset. On the other hand, the watermark is hidden for the invisible type, but can be recovered using the appropriate decoding mechanism [12].

According to data extraction: Watermarking can be public, private, or semi- private (referred to as blind, semi-blind, or non-blind, respectively). They differ from each other in the nature and combination of inputs and outputs. Blind remains the most challenging problem since it requires neither the original secret key nor the embedded watermark in order to be detected for proving ownership. It usually contains copyright or licensing information, such as the identifier of the copyright holder or the creator of the material. On the other hand, non-blind watermarking requires at least the original media. It can be used as authentication and content integrity mechanisms in a variety of ways. This implies that the watermark is a secured link readable only by authorized person with the knowledge of the secret key. Finally, semi-blind watermarking does not use the original media for detection. Potential applications of semi-blind and non-blind are used for evidence in court to prove ownership, copy control, and fingerprinting where the goal is to identify the original recipient of private copies. [13]

According to Domain: In images, audio and video files, if some bits or parts of the file content are altered, this is called spatial (or time) domain. But if the alteration is done in the spectral coefficient of the file, it is called transformation (or frequency) domain. These two domains will be explained in more details later in the thesis. Although it is conceivable that a watermark could alter other features such as edges or textures, they are commonly used and acceptable. [14]

According to robustness**:** Watermarks can be robust, fragile, or semi-fragile. It is robust if it has immunity against attacker, and fragile if any manipulation or modification of the data would alter or destroy the watermark as well as the watermarked multimedia [15]. Semi-fragile watermarks are more robust than fragile watermarks and less sensitive to classical user modifications. The aim of this method is to discriminate between malicious and non-malicious attacks.

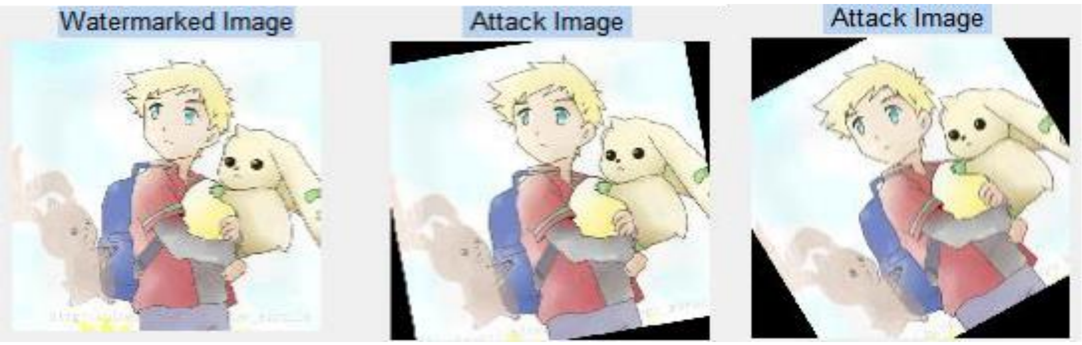
2.6 Digital Watermarking Attacks

Watermarking techniques should be tamper resistant to hostile attacks. Depending on the application, the watermarked content encounters certain types of attacks. This section describes different types of simulated attacks performed on watermarked images that can cause distortion on embedding information that may further lead to watermark or secret message extract corruption. In the following, a definition some basic types of attacks are briefly explained [16].

1. **Geometrical attacks:** In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information [17]. Geometrical attacks can be rotation or cropping, defined in the following:

➢ ***Rotation:*** A rotation attack rotates the image by a certain angle degree in clockwise or counter clockwise direction. For the image shown in Figure (2-

2.a), Rotation by 10° and 30° in a counter clockwise direction will give the image shown in Figure (2-2.b) and Figure (2-2.c). The image is cropped to include only the central portion of the rotated image and is the same size as the original image [18].



(a) (b) (c)

Figure 2-3: Original and attacked test image

2. **Removal attacks:** Watermarked Removal Attack (WRA) are attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Removal attacks aim at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding) [19]. Watermark removal attacks can be performed by adding some type of noise such as Additive White Gaussian Noise (AWGN) and Salt and pepper or by performing any type of compression such as JPEG or Wavelet Compression, (AWGN) and Salt and pepper are defined in the following:

- ***Additive White Gaussian Noise (AWGN):*** An amount of noise of mean and variance is added to every part of the picture. This means that each pixel in the noisy image is the sum of the true pixel value and a random Gaussian distributed noise value [20], as shown in Figure (2-3). When noise of Mean =

0.0, Variance = 0.05 is added to the image in Figure (2-2.a), the result is as shown in Figure (2-4).

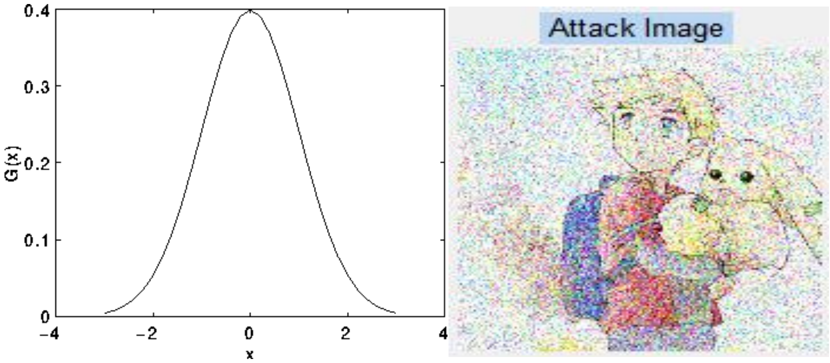
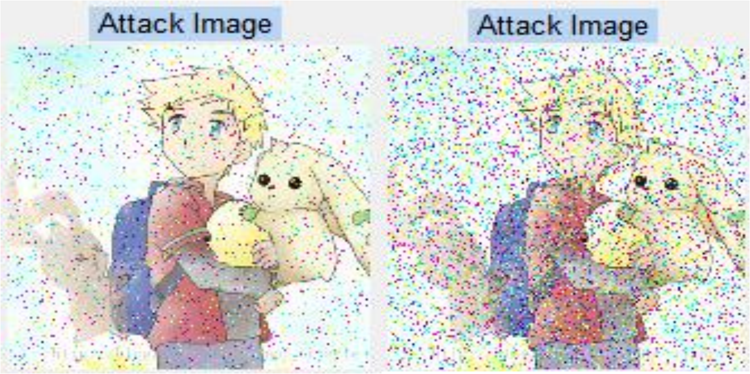


Figure 2-4: Random Gaussian distribution noise value and effect

➢ ***Salt and pepper noise:*** Is another example of statistical noise albeit with a very different probability density function (PDF) than Gaussian noise. Its PDF takes the form of two impulse functions at two discrete locations [21]. The visual effect of adding salt and pepper noise on the watermarked image can be seen in Figure (2-4). The experiment uses a number of different values to allow better observation on the effect of salt and pepper noise on watermarked image. The values used are 0.05 and 0.15.



(a) (b)

Figure 2-5: Effect of adding salt & pepper noise to an image (a) 0.05 and (b) 0.15

An observation of the image histogram and Fourier spectrum yields similar conclusion as that of Gaussian noise. In both cases, the image histogram and Fourier spectrum shows the same indication of an increase in pixel value variation and high frequency component of the image as stronger noise is added. This gives a clear indication that salt and pepper noise attack is also essentially a high pass filter function.

Here in this thesis, we had used three types of attacks (explained above), which are the Rotation, Additive (AWGN) and Salt and Pepper.

3. **Active Attacks:** Mean that the hacker tries to remove the watermark or make it undetectable. This type of attack is critical for many applications, including owner identification, proof of ownership, fingerprinting, and copy control, in which the purpose of the watermark is defeated when it cannot be detected. However, it is not a serious problem for other applications such as authentication or covert communication.
4. **Passive Attacks:** The hacker dose not try to remove the watermark, but he/she simply tries to determine whether a watermark is present or not, i.e. he/she tries to identify a covert communication.

5. **Collusion Attacks:** These are special cases of active attacks, in which the hackers use several copies of one piece of multimedia, each with a different watermark, to construct a copy with no watermark.
6. **Forgery Attacks:** The attacker tries to incorporate a valid watermark, rather than removing one. These are the main security concerns in authentication applications, because if hackers can embed valid authentication marks, they can cause the watermark detector to accept forged or modified multimedia. In addition, this type of attack is a serious concern in proof of ownership.
7. **Fragility Attacks:** Fragility is opposite of robustness. In some application, the watermark is required to survive certain transformations and be destroyed by others. For example, watermark should survive in case of content authentication. This property makes the design of fragile watermarking scheme highly difficult.

2.7 Image Watermarking Techniques

Since color images are planned to be used as the protected multimedia using text watermarks, this section will define briefly digital color image red-green-blue (RGB) structure first, then it will explain the possible techniques used for embedding and extraction into these images. Digital image watermarking schemes mainly fall into two broad categories: Spatial-domain and Frequency-domain techniques, as briefly defined later in this section, then the widely used evaluation metrics for image quality, namely mean square error (MSE), peak -signal-to-noise ratio (PSNR), Multi-scale structural similarity index measure (MSSIM) and Normalized Cross Correlation (NCC) are defined [22].

2.7.1 Digital Color Image structure

A digital color image is an image that includes color information for each pixel. For visually acceptable results as shown in Figure (2-6), it is necessary and sufficient to provide three samples color channels for each pixel, which are interpreted as coordinates in some color space. They are the red, green and blue channels, and the image is referred to as RGB. [23]

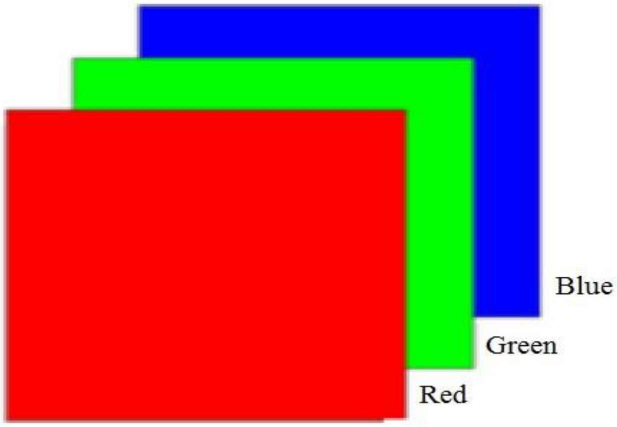


Figure 2-6: Digital Color Image Channels

Digital color image can be manipulated as a 3 separate pixel arrays of similar dimensions as shown in Figure (2-7). Each color component pixel is represented by 8 bits, therefore each image pixel consists of 24 bits length. Where IR(u,v), IG(u,v), and IB(u,v) are the intensity of the red, green, and blue pixel at the point with (u,v) coordinate, respectively.

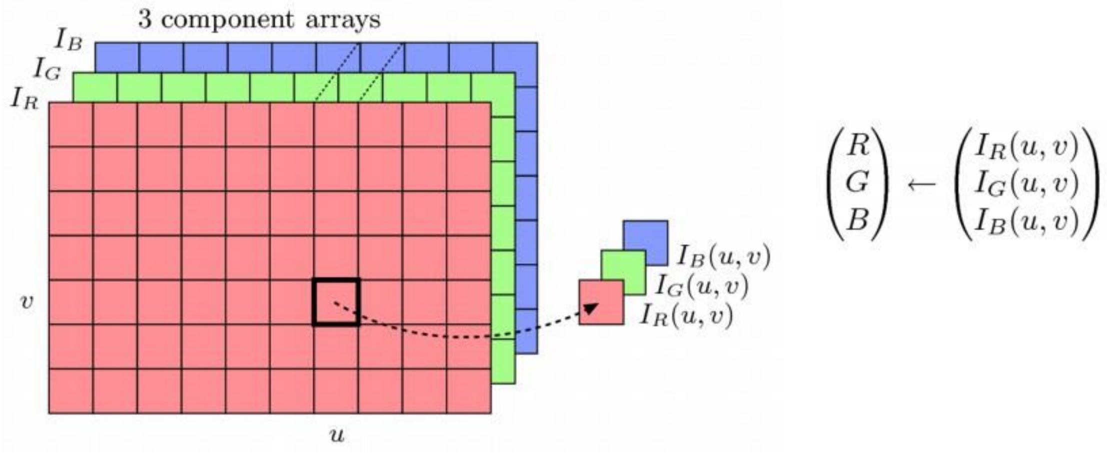

3 component arrays
I_B
I_G
I_R
v
u
$I_B(u,v)$
$I_G(u,v)$
$I_R(u,v)$
$\begin{pmatrix} R \\ G \\ B \end{pmatrix} \leftarrow \begin{pmatrix} I_R(u,v) \\ I_G(u,v) \\ I_B(u,v) \end{pmatrix}$

Figure 2-7: Color Image as a 3 Arrays

The RGB component intensity values representing pixel's colors are packed together into single element as shown in Figure (2-8). However, for gray images only one array of pixels represents the image pixels intensities (each of 8 bits length) are used. [23]

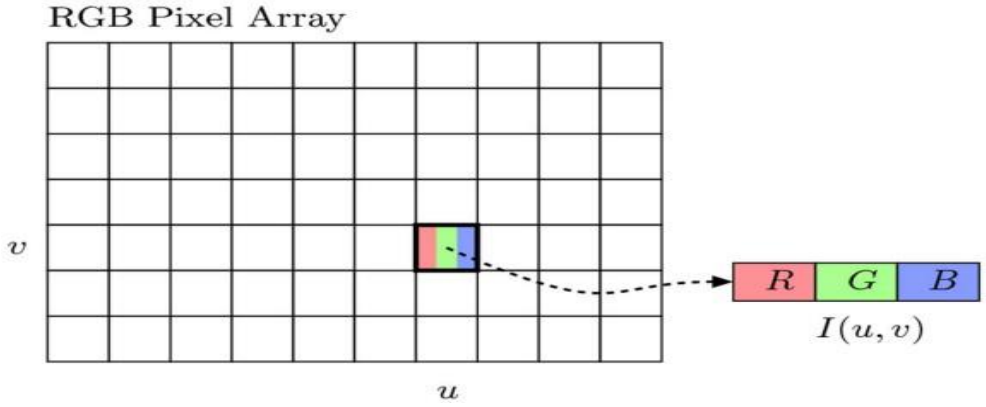


Figure 2-8: RGB Component intensity values

Embedding any multimedia such as text and logos into a color image requires manipulation of the image pixel components. Different methods may be used to manipulate digital color image that are summarize in the next chapter.

2.7.2 Digital Image Watermarking Domain Techniques

Images can be represented in spatial domain and or frequency domains. In the frequency domain, images are represented in terms of their frequencies, while in the spatial domain images are represented by pixels.

2.7.2.1 Spatial Domain Techniques

This watermark technique is based on insertion of watermark data directly into pixels of a host image. Simple watermarks can be embedded by modifying the pixel values or the least significant bit (LSB) values. Least significant bits have the lowest effect on the pixel value, and therefore any changes in these bits would have very low effect on the overall appearance of the image [24]. Spatial domain is generally simple and faster than the frequency domain. The strength of the spatial domain is due to the following:

- Simplicity.
- Very Low mathematical Computational efforts.
- Less time consuming.

This technique of watermarking is easier and computing speed is higher than transform domain, but it is not robust enough to protect watermark information against different kinds of attacks such as the lossy compression. The spatial domain methods are applicable for fragile watermarking scheme.

Basically, in these techniques, some bits or parts of the host image are replaced or shifted in position according to the watermarking patterns. Some Spatial Techniques of watermarking are defined below:

2.7.2.1.1 Least-Significant Bit (LSB)

It is a very common and one of the earliest methods work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Each image consists of pixels, and each pixel being represented by some number of bits sequence (for example 8 bits gray image). The watermarks bits are embedded in the right most bit (i.e., least significant) of selected pixels of the image. However, for an RGB host image, each color component pixel is 8-bits lengths and may all be used for embedding the watermark bits. For example, to embed the character with binary code 10111010, then if the original pixel components of the host image are:

(10100001 10001000 00110011)

(01011111 11001110 11110001)

(10101100 10101010 10110110)

Then after embedding the character in the least significant bit, the watermarked image pixels will be as follows:

(1010000**1** 1000100**0** 0011001**1**)

(0101111**1** 1100111**1** 1111000**0**)

(1010110**1** 1010101**0** 10110110)

Therefore, the watermark data undergoes two processes before embedding, it is converted to ASCII code first, and then it is converted to binary representation. There are many algorithms for embedding watermarks into images. Some LSB applications perform the embedding randomly into all the image pixels, other applications performed embedding by splitting the image into blocks, then watermark data is embedded or added to the blocks using certain procedures. [25]

The LSB method is easy to implement and does not generate serious distortion to the image. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information, or can simply do it by image cropping, etc.

2.7.2.1.2 Spread Spectrum Modulation (SSM)

Spread-spectrum modulation techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time or frequency domains. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark [26].

2.7.2.2 Frequency Domain Techniques

Compared to spatial-domain, frequency-domain techniques are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Laguerre Transform (DLT) and the Discrete Hadamard Transform (DHT). The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, HVS is more sensitive to low-frequency coefficients, and less sensitive to high-frequency coefficients. In other words, low-frequency coefficients are perceptually significant, which means alterations to those components might cause severe distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high-frequency coefficients aggressively. To obtain a balance between imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies [27]. Discrete Cosine Transform (DCT) and Fast Fourier Transform (FFT) frequency domain techniques are used in this thesis.

2.7.2.2.1 Discrete Cosine Transform

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform (DFT); it transforms a signal or image from the spatial domain to the frequency domain. It has been widely used because of its good capacity of energy compression and de-correlation. DCT is faster than DFT because its transform kernel is real cosine function while it is complex exponential in DFT [28].

2.7.2.2.2 Fast Fourier Transform

The Fast Fourier Transform (FFT) is commonly used to transform an image between the spatial and frequency domain. Unlike other domains such as Hough and Radon, the FFT method preserves all original data. Plus, FFT fully transforms images into the frequency domain, unlike time-frequency or wavelet transforms. The FFT decomposes an image into sines and cosines of varying amplitudes and phases, which reveals repeating patterns within the image [29].

2.7.3 Metrics for Evaluating Image Quality (Performance Evaluation Metrics)

To determine the quality of the watermarking techniques, some evaluating metrics are required that compares the watermarked image with the original image. Commonly used metrics are Peak Signal-to-Noise Ratio (PSNR), Normalized Cross Correlation (NCC) and Multi-scale structural similarity index measure (MSSIM) [30]. They are defined in the following:

2.7.3.1 Peak Signal-to-Noise Ratio (PSNR)

The PSNR is the most widely used metrics. It avoids the problem of image intensity by scaling the MSE according to the image range. Performance evaluation of PSNR between original image and watermarked image is calculated based on the formula:

$$PSNR = 10\log_{10}\frac{MAX}{\sqrt[2]{MSE}} \qquad \textbf{\textit{(2-2)}}$$

Where MAX refers to the maximum intensity of the given resolution of each pixel and the MAX value for gray scale image = 256, and in the audio is 1. On the other hand, the Mean Square Error (MSE) is defined as the square of the error between the cover without any hidden data and the watermarked cover after hiding the message [31]. The PSNR values are measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, however between images comparisons of PSNR, it is meaningless.

2.7.3.2 Multi-scale Structural Similarity Index Measure (MSSIM)

The MSSIM is designed by modeling any image distortion as a combination of three factors that are loss of correlation, luminance distortion and contrast distortion. The SSIM is defined as:

$$SSIM(f,g) = l(f,g)c(f,g)s(f,g) \tag{2-3}$$

$$\begin{cases} l(f,g) = \dfrac{2\mu_f\mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f,g) = \dfrac{2\sigma_f\sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f,g) = \dfrac{\sigma_{fg} + C_3}{\sigma_f\sigma_g + C_3} \end{cases} \tag{2-4}$$

The first term in (2-4) is the luminance comparison function which measures the closeness of the two images mean luminance (μ_f and μ_g). This factor is maximal and equal to 1 only if $\mu_f = \mu_g$. The second term is the contrast comparison function which measures the closeness of the contrast of the two images. Here the contrast is measured by the standard deviation σ_f and σ_g. This term is maximal and equal to 1 only if $\sigma_f = \sigma_g$. The third term is the structure comparison function which measures the correlation coefficient between the two images f and g [32]. Note that σ_{fg} is the covariance between f and g. The positive values of the SSIM index are in [0, 1]. A value of 0 means no correlation between images, and 1 means that f = g. The positive constants C1, C2 and C3 are used to avoid a null denominator.

2.7.3.3 Normalized Cross Correlation (NCC)

When the owner wants to check the watermark in a possibly attacked watermarked image; it's important that the extracted watermark be clear and easily recognized. The robustness is tested by comparing the original watermark with the extracted one using Correlation. Normalized Correlation (NC) is a measure of association (strength) of the relationship between two variables (images in this case). The values of NC are between 0 (random relationship) to 1 (perfect linear relationship) or -1 (perfect negative linear relationship). This extracted watermark may or may not resemble the original watermark because the image might have been attacked. The Normalized Correlation coefficient, used for similarity measurement is defined as:

$$NC = \frac{\sum W\widehat{W}}{\sum W^2 \sum \widehat{W}^2} \qquad \textbf{\textit{(2-4)}}$$

The normalized r* cross-correlation metric is based on the variance metrics of SSIM. It's defined as:

$$NNC = \sigma_{xy}/\boldsymbol{\sigma_x \sigma_y} \qquad \textbf{\textit{(2-5)}}$$

When $\sigma_{xy} \neq 0$, 1 when both standard deviations are zero, and 0 when only one is zero. It has found use in analyzing human response to contrast detail phantoms [33].

2.8 Related Works

A number of related works will be examined in this section. Since this research is concern with text watermarking, the following literature survey describes only the previous work done on digital watermarking in spatial domain on text watermarking in particular, apart from other studies that have been conducted on steganography and watermarking, in addition to go through different researches in touch with it.

- In [34] examined three important methods related for hiding digital data, depending on the psycho visual repetition in digital images of grey scale, using the neighborhood information. Their importance arises from the ability to know exactly the data included within the image input pixel, without making differences. The neighborhood connection sheds light on the smooth parts of an image that reflects the limited amount of unrevealed data, in addition to the complex parts of an image represented in the big amounts of hidden data. Smooth areas are less resistant to modification than edge parts. The greater number of image pixels were not contingent to the hidden information, as only three bits were approved to be kept secret in smooth areas, and other changing bit numbers were maintained concealed in the edge areas.

- In order to get color image modification from and into gray, according to [35], it was important to develop a method based on the direct and inverse alteration. Color image encryption/decryption could also benefit from this method. Achieving advanced real color image alternation, through the reduction of necessary time to manage inverse alteration by three and eight times for images. This improvement is achieved using R’G’I design instead of HSI design.
- In [36] presented a simple and robust watermarking algorithm using grayscale image, and concerning the concealment of data. They implement the third and the fourth least significant bits (LSB) for the digital watermark pattern. In their algorithm, two bits were embedded in the third and fourth LSB, and they claim that it is more robust than the traditional LSB technique in hiding the data inside the image by avoiding the watermarked image deformation, as the coordinates defined in the image after setting the hidden data inside the third and fourth LSB.
- A hash based LSB Techniques in spatial domain is reported by [37]. It is a utilization of an algorithm portrayed with audio video interleave (AVI) file as a cover medium. A video stream composed of collection of frames and the secret data is concealed in these frames as payload. The information of the cover video such as number of frames, frame speed, frame height, and frame width are extracted from the header. The cover video is then divided and separated into frames. The size of the embedded data is irrelevant when multimedia due to the fact that the data could be embedded in multiple frames. This technique conceals 8 bits of embedded data at a time in LSB of RGB pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight 8-bits of embedded 3-bits are inserted in R pixel, 3-bits in G pixel and remaining 2- bits are inserted in B pixel This distribution

pattern is applied because the chromatic influence of the blue pixel color component to the human eye is more than that of the red and green pixel components.

- As for [38], LSB pattern and Discrete Cosine Transform, including Gaussian noise represents the carrying out of the digital watermarking in spatial and frequency domains, respectively. The formation of Speckle as an example, representing the noise attacks, has been implemented, and the extraction of watermark played a role in gaining the results. Obviously, this method involves spatial and transformational techniques.
- A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code is proposed by [39]. It achieved more advanced and valid level of imperceptibility through the exploitation of the couple purpose robust algorithm, concerning image cryptography and digital watermarking.
- In [40] presented a new technique for image watermarking in the spatial domain utilizing the concept of information theory with LSB algorithm. The host image is segregated into blocks and the watermark is embedded into the block(s) with the maximum entropy value. They claim that their technique has performed reasonably well over a large varied datasets of host and watermark images and verified the perceptibility and the robustness.
- In [41] presented a spatial domain based image watermarking using shell based pixel selection. The importance of this algorithm arises from its ability to present an advanced degree of security, as well as, draw out the watermark. What distinguishes the algorithm is also its ability to make watermark locations unpredictable using pixel selection, which form the basis of the shell.
- In [42], presented a new digital watermarking method through bit replacement technology, which stores multiple copies of the same data that is to be hidden in a scrambled form in the cover image. In this paper an indigenous approach is described for recovering the data from the damaged copies of the data under attack by noise

salt and pepper with different density (0.01.0.02, 0.03 and 0.04) and quality of image is same with attack.

2.9 Summary

Digital watermarking is a very effective solution for authentication and copyright protection of digital contents. Image file gained very high importance for their security purpose. Digital watermarking is the solution for the protecting legal rights of digital content owner and the customer. The large need of networked multimedia system has created the need of copyright protection. The research in this thesis concentrates on gaining good performance for text watermarking into images. This will be achieved by suggesting an algorithm that performing the embedding of the text watermark in image in order to achieve intellectual properties protection of digital media and copyright protection.

Digital text watermarking is still under research and currently evolving. Some interesting research directions include Designing algorithms that recover reordering and retyping attacks, investigating the performance of polymorphism watermarking and designing algorithms that survive screen shots attacks and printing.

Chapter Three

Methodology

3.1 Introduction

In this chapter, the methodology followed in this thesis is described and presents the proposed watermarking algorithm for hiding text information (watermark) into images that is to be copyright protected and ownership proof. The methodology is divided into two main parts Techniques which are the spatial domain watermarking and frequency domain watermarking.

3.2 Proposed Method

The proposed watermarking algorithm in this thesis adopt the embedding of text watermarks or signatures information into still images. Where the two digital images watermarking domains techniques have been used for embedding text watermarking in image, they are Spatial Domain Techniques and Frequency Domain Techniques (explained in Chapter two). Each technique has a specific method for the image watermarking processes that is described in this chapter. In spatial domain technique, the least significant bit Technique (LSB) was used to embed the watermark bits in the least significant bits of image pixels (it will explain in the next section). In frequency domain technique, the discrete cosine transform technique (DCT) and Fast Fourier Transform technique (FFT) was used to embed the watermark into image (they were explained in the next section). After image watermarking (embedding and extraction) the performance metrics used for evaluation image quality are mathematically described, they are Peak Signal-to-Noise Ratio (PSNR), Normalized Cross Correlation (NCC) and Multi- scale structural similarity index measure (MSSIM), The way they work is explained in chapter two. The processes of embedding and extraction of text watermarks are shown in the flowchart in figure (3-1).

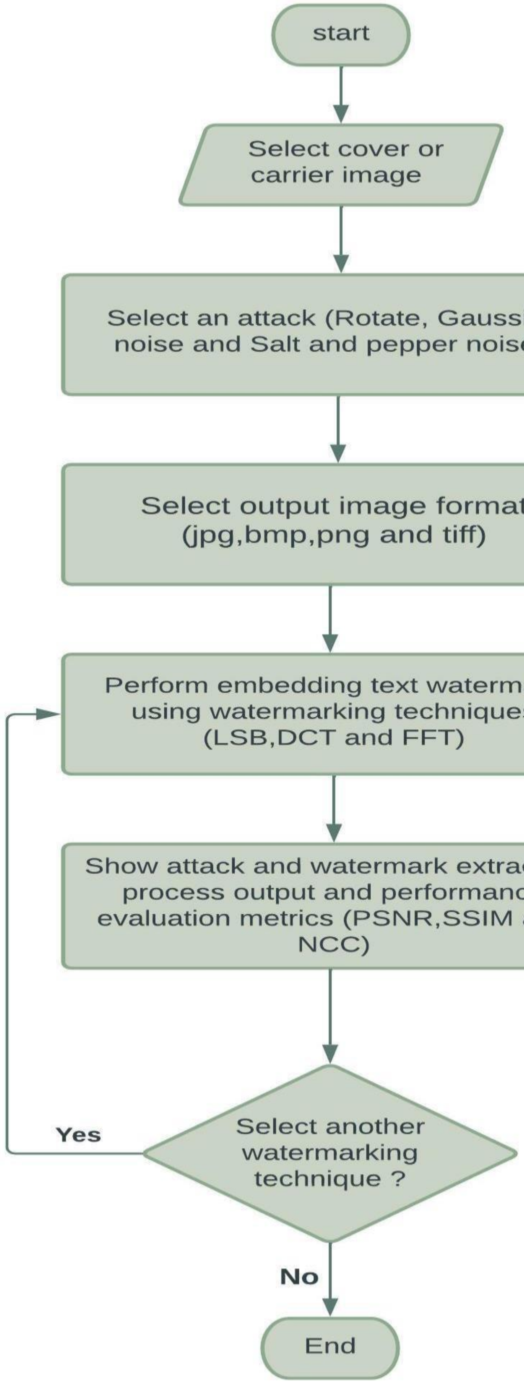
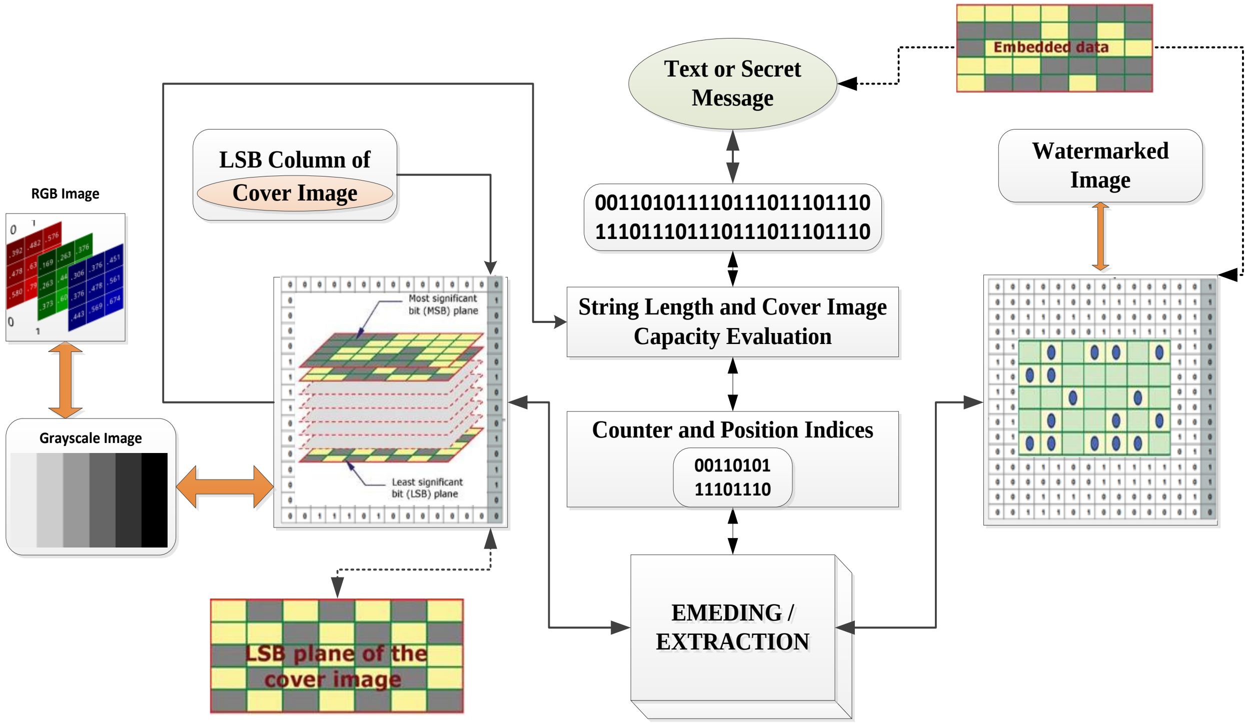

start
Select cover or carrier image
Select an attack (Rotate, Gaussian noise and Salt and pepper noise)
Select output image format (jpg,bmp,png and tiff)
Perform embedding text watermark using watermarking techniques (LSB,DCT and FFT)
Show attack and watermark extraction process output and performance evaluation metrics (PSNR,SSIM and NCC)
Select another watermarking technique ?
Yes
No
End

Figure 3-1: Proposed Method Flowchart

3.2.1 Least Significant Bit (LSB) Embedding

It is based on embedding the bits of message in the least significant bit of the cover which cause less effect in the cover signal value and less error compared with the original signal [43]. Figure (3-2), illustrates the LSB technique and how you can text embedding in the image cover using this technique. In the basic LSB approach shown, the bit-planes of a grayscale image are sketched on the left with most significant bit (MSB) on top (color image manipulation was explained in chapter two). Dark and light boxes represent binary values 0s and 1s, respectively, of the pixels on different bit-planes. The LSB-plane of the cover image on the top right is replaced with the hidden data in the middle, which becomes the LSB-plane of the watermarked image. The bottom-right map indicates differences between LSB planes of the cover and watermarked images. Circles represent the flipped bits; with an average of 50% bits in the LSB plane changed, the watermarked image is visually identical to the cover.


Embedded data
Text or Secret Message
LSB Column of Cover Image
Watermarked Image
RGB Image
0011010111101110111011101110
1110111011101110111011101110
Most significant bit (MSB) plane
String Length and Cover Image Capacity Evaluation
Counter and Position Indices
00110101
11101110
Grayscale Image
Least significant bit (LSB) plane
EMEDING / EXTRACTION
LSB plane of the cover image

.

Figure 3-2: LSB Embedding of text data in image file [44]

3.2.1.1 Watermark Embedding

In figure (3-2) displays the basic LSB watermarking technique that considered in this thesis to perform embedding of text or secret message (the watermark) into a colored RGB image after conversion to grayscale image and embedding of text binary representation into the LSB plane of the cover image, while that an evaluation of capacity of image for text handling is performed to make sure that the LSB plane of the cover image is enough for watermark and extraction information.

3.2.1.2 Watermark Extraction

The watermark extraction (extraction information) is represented by the counter of text characters and starting index of text data inside the watermarked image. The procedure is two directions functional, where reversing the embedding is actually performed for extraction.

3.2.2 Frequency Domain Techniques

Frequency domain transfers an image to its frequency representation and the image is segmented into multiple frequency bands. The embedded watermark in the frequency domain of a signal can provide more robustness than spatial domain. It is strong against attacks like compression, cropping where spatial domain is not. Several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) can be used. Each of these transforms has its own characteristics and represents the image in different ways. The procedure followed in frequency domain techniques considered in this study is show in Figure (3-3), where Discrete Cosine Transform (DCT) and Fast Fourier Transform (FFT) frequency domain techniques are used.

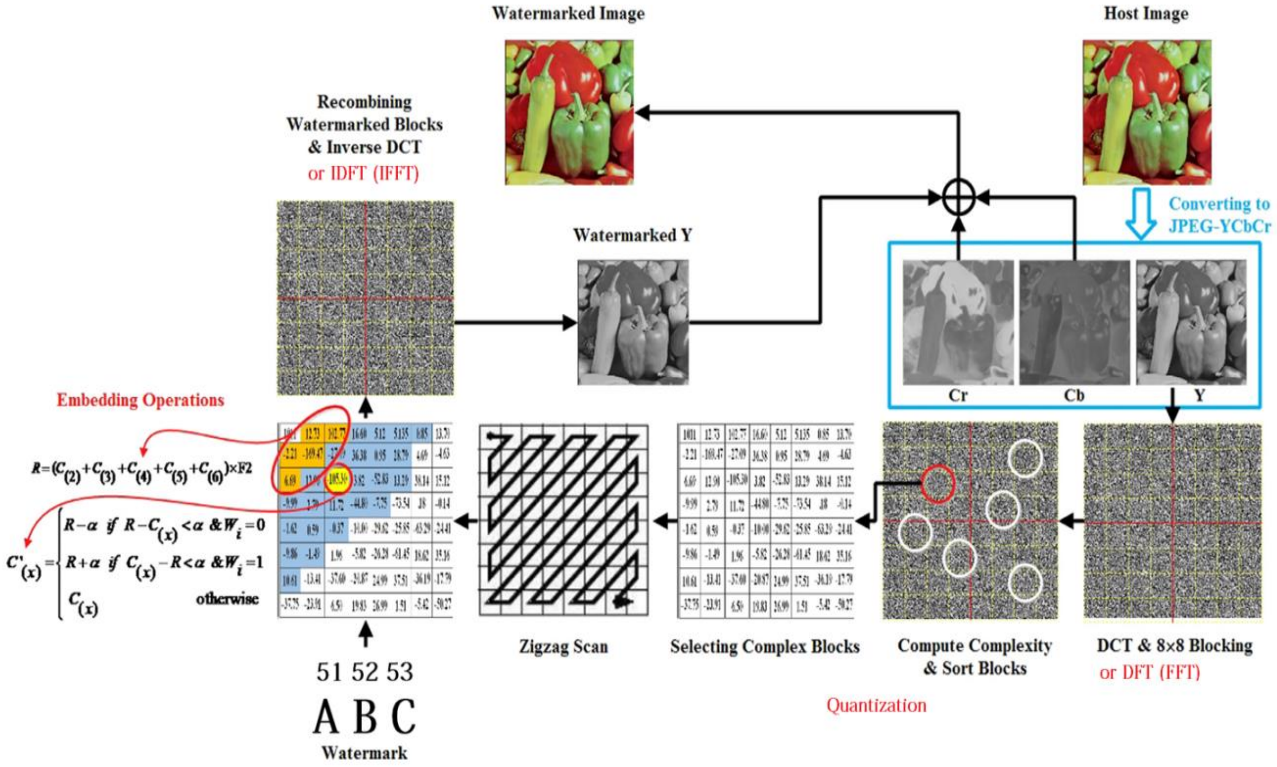

Watermarked Image
Host Image
Recombining Watermarked Blocks & Inverse DCT
or IDFT (IFFT)
Watermarked Y
Converting to JPEG-YCbCr
Cr
Cb
Y
Embedding Operations
$R=(C_{(2)}+C_{(3)}+C_{(4)}+C_{(5)}+C_{(6)})\times F2$
$C'_{(x)}=\begin{cases} R-\alpha \text{ if } R-C_{(x)}<\alpha \;\&W_i=0 \\ R+\alpha \text{ if } C_{(x)}-R<\alpha \;\&W_i=1 \\ C_{(x)} \quad \text{otherwise} \end{cases}$
51 52 53
A B C
Watermark
Zigzag Scan
Selecting Complex Blocks
Compute Complexity & Sort Blocks
DCT & 8×8 Blocking
or DFT (FFT)
Quantization

Figure 3-3: Frequency Domain Watermarking [45]

3.2.2.1 RGB to YCbCr Color Space Conversion

It has three components: the luminance Y, the blue difference Cb and the red difference Cr. One important task in image processing applications is the color space conversion. Real-time images are stored in RGB color space, because it is based on the sensitivity of color detection cells in the human visual system. In digital image processing the YCbCr color space is often used in order to take advantage of the lower resolution capability of the human visual system for color with respect to luminosity. Thus, RGB to YCbCr conversion is widely used in image processing [46].

Given a digital pixel represented in RGB format, 8 bits per sample, where 0 and 255 represents the black and white color, respectively, the YCbCr components can be obtained according to equation:

$$\begin{cases} Y = 16 + \frac{65.738R}{256} + \frac{129.057G}{256} + \frac{25.064B}{256} \\ Cb = 128 - \frac{37.945R}{256} - \frac{74.494G}{256} + \frac{112.439B}{256} \\ Cr = 128 + \frac{112.439R}{256} - \frac{94.154G}{256} - \frac{18.285B}{256} \end{cases} \qquad \textbf{\textit{(3-1)}}$$

Equation (3-1) represents the RGB to YCbCr conversion. Approximating the equations (3-1) to the nearest integer and replacing multiplication and division by shift registers, the equation (3-2) is obtained:

$$\begin{cases} Y = 16 + (((R << 6) + (R << 1) + (G << 7) + G + (B << 4) + (B << 3) + B) >> 8) \\ Cb = 128 + ((-((R << 5) + (R << 2) + (R << 1)) - ((G << 6) + (G << 3) + (G << 1)) + (B << 7) - (B << 4)) >> 8) \\ Cr = 128 + (((R << 7) - (R << 4) - ((G << 6) + (G << 5) - (G << 1)) - ((B << 4) + (B << 1))) >> 8) \end{cases} \qquad \textbf{\textit{(3-2)}}$$

Image consumes a lot of data. One of the reasons is because it is represented in the RGB format. However, is not worth to store or transmit information in this color space representation, once it has a large bandwidth. Thus, all the pixels should be converted to YCbCr to accomplish that. The converted image in the YCbCr space can be seen in Figure (3-4).

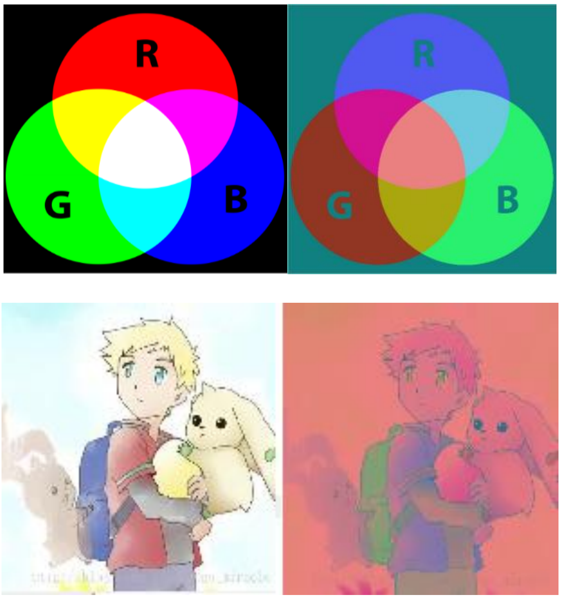


Figure 3-4: RGB to YCbCr Conversion

The Y component only filters the luminance (brightness) of the image, the Cb and Cr components subtract the red and blue colors, respectively, from the image (see Figure (3-5)).

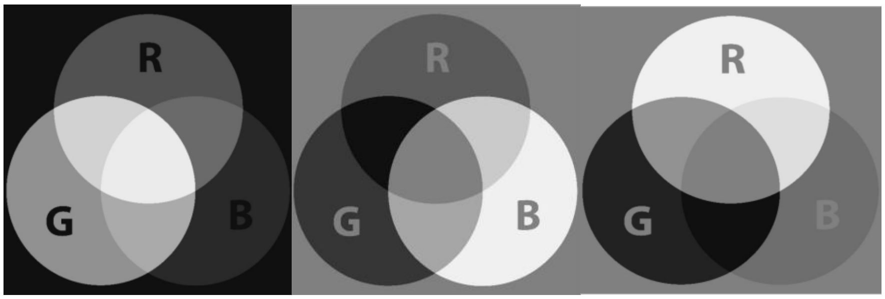


Figure 3-5: The Y, Cb and Cr component of YCbCr image

3.2.2.2 Discrete Cosine Transform (DCT)

DCT is powerful transformation technique. In DCT based compression scheme, source image samples are firstly grouped into non-overlapped and consecutive 8×8 blocks and each block is transformed by forward DCT into a set of 64 values referred to as DCT coefficients. The value located in the upper-left corner of the block is called Direct Current (DC) coefficients and the other 63 values are called Alternate Current (AC) coefficients.

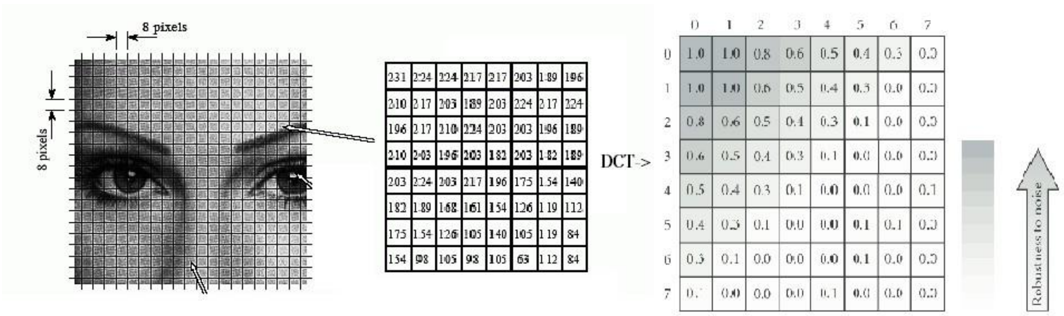
Technically, the discrete cosine transforms (DCT) is a technique for converting a signal into elementary frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image x, the coefficients for the output image y is [47]:

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} X(m,n) cos\frac{(2m+1)u\pi}{2M} cos\frac{(2n+1)v\pi}{2N} \qquad \textbf{\textit{(3-3)}}$$

$$\text{Where } \alpha_i = \begin{cases} \frac{1}{\sqrt{2}} & i = 0 \\ 1 & i = 1,2,\dots,N-1 \end{cases}$$

The input image x, is N pixels wide by M pixels high, $x(m,n)$ is the intensity of the pixel in row m and column n. $y(u,v)$ is the DCT coefficient in row u and column v of the DCT matrix.

DCT domain watermarking segments the image into non-overlapping blocks of 8x8 and applies DCT to each of the blocks which results with three frequency sub-bands: low, mid and high frequencies in each block as shown in Figure (3-6). Much of the signal energy lies at low frequencies which contain the most important visual parts of the image, and the high frequency components are easily removed through compression and noise attacks. The watermark is embedded by modifying the coefficients of the middle frequency bands so that the visibility of the image will not be affected and the watermark will not be removed by compression.



231	224	224	217	217	203	189	196
210	217	203	189	203	224	217	224
196	217	210	224	203	203	196	189
210	203	196	203	182	203	182	189
203	224	203	217	196	175	154	140
182	189	168	161	154	126	119	112
175	154	126	105	140	105	119	84
154	98	105	98	105	63	112	84

	0	1	2	3	4	5	6	7
0	1.0	1.0	0.8	0.6	0.5	0.4	0.3	0.0
1	1.0	1.0	0.6	0.5	0.4	0.3	0.0	0.0
2	0.8	0.6	0.5	0.4	0.3	0.1	0.0	0.0
3	0.6	0.5	0.4	0.3	0.1	0.0	0.0	0.0
4	0.5	0.4	0.3	0.1	0.0	0.0	0.0	0.1
5	0.4	0.3	0.1	0.0	0.0	0.1	0.1	0.0
6	0.3	0.1	0.0	0.0	0.0	0.1	0.0	0.0
7	0.1	0.0	0.0	0.0	0.1	0.0	0.0	0.0

Figure 3-6: DCT transformation of 8x8 blocks

The image is reconstructed by applying inverse DCT to each block using the three frequency sub-bands' coefficients including the modified coefficients according to Equation (3-4)

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v y(u,v)\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \qquad \textbf{\textit{(3-4)}}$$

When DCT is applied to a square block, it converts highly correlated data set in a relatively independent data set and results a dc coefficient, and a series of ac coefficients of zero values at high frequency and small values at low frequency. Since DCT is a lossless transformation, the function Inverse-DCT (IDCT) results original pixel value [48].

3.2.2.3 Fast Fourier Transform (FFT)

The FFT, forward and inverse, has found many applications in signal processing. The Fourier transform of a finite sequence is defined as:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi kn/N} = \sum_{n=0}^{N-1} x(n)\left(e^{-j2\pi/N}\right)^{nk} \qquad \textbf{\textit{(3-5)}}$$

Where, X[k]: Frequency sampled data; x[n]: Time sampled data; N: Total number of samples; n: Time index, n=0, 1, 2, 3,..., N-1; k: Freq index, k=0, 1, 2, 3, ., N-1.

3.2.2.4 Quantization

Quantization, involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible.

Quantization is the process of approximating the resultant DCT matrix into a small set of values, to determine what information can be discarded safely without a significant loss in visual fidelity. Consequently, that leads to the development of lossy compression [49]. The quantization is performed by using the following equation:

$$\boldsymbol{P_q(x,y) = Round(\frac{x(m,n)}{Q(x,y)})} \qquad \textbf{\textit{(3-6)}}$$

Where $\mathrm{Q(x,y)}$ is a common quantization matrix used to perform quantization as given below:

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

The quantization matrix assigns the larger quantization step size, usually, seen in the lower right region for the high frequency components to discard the redundant information, and smaller quantization step size for the low frequency components seen in the upper left region to preserve the significant information.

3.2.2.5 Zigzag Scan

Zigzag pattern (ZZ) is a common scanning pattern used in image compression, which is performed on the result of quantization process where the pixel values in a 2-D square matrix is reordered into a 1-D matrix [50]. Subsequently, a lossless encoding procedure called Run Length Encode (RLE) is applied to the result of Zigzag scan. During the scanning, we visit each cell exactly once in some order and bring into being a 1-D matrix. Zigzag pattern scans the 2-D square matrix in a horizontal diagonal vertical diagonal fashion starting from upper left to lower right as shown in Figure (3-7).

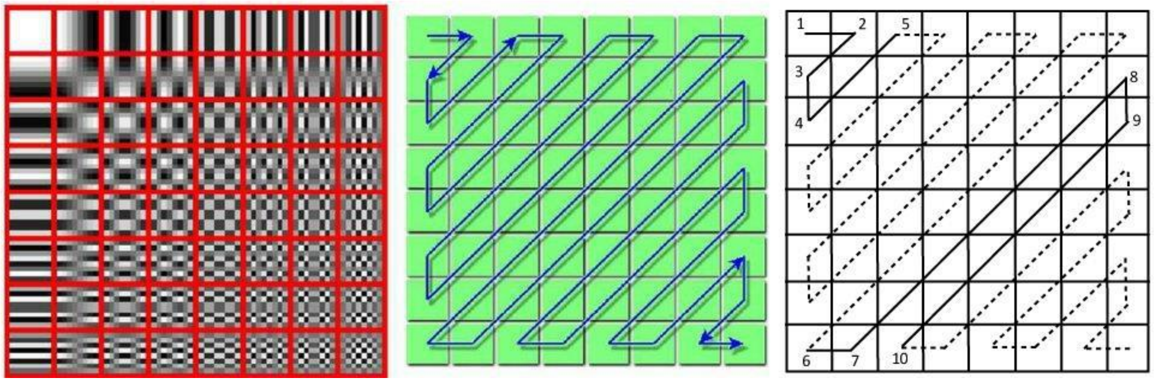


Figure 3-7: Zigzag Scan. The number indicates a shift in its procedure

The algorithm for ZZ is presented below:

Step 0: Initialize row =1 and column =1.

Step 1: Move right once by incrementing column by 1.

Step 2: Move to the bottom left by incrementing row by 1 and decrementing column by 1 until to reach the left side.

Step 2.1: Check if bottom most left is reached. If true, go to step 6 or else continue.

Step 3: Move to the bottom once by incrementing row by 1

Step 4: Move to the top right by decrementing row by 1 and incrementing column by 1 and continue this until to reach top side.

Step 5: Repeat step 1 to 4 until the condition specified at step 2.1 is satisfied.

Step 6: Do step 1.

Step 7: Move to the top right by decrementing row by 1 and incrementing column by 1 and continue this until to reach right side.

Step 8: Do step 3.

Step 9: Move to the bottom left by incrementing row by 1 and decrementing column by 1 until to reach the bottom side.

Step 10: Repeat step 6 to 9 until to reach the last cell.

3.2.2.6 Run Length Encode

The idea is to represent long repeated occurrences of a symbol with a pair called (n, symbol) where n is the total number of occurrences of a symbol. A version of Run Length Encode (RLE) called Zero Run Length Encoding is used in JPEG compression. In which ac coefficient is represented in (RUN, VALUE) format, where RUN is the total number of continuous zero ac coefficients preceding the nonzero ac coefficient and on the decoding side, the inverse process of zero run length encoding takes the zero run length encoded data as its input and produces the original ac coefficients as its output [51].

3.2.2.7 Watermark Embedding

In watermark embedding process the zigzag scan is used in order to dividing each block into low, middle and high frequency bands and then embedding operations is performed by modulating the relationship between the frequency coefficients according to:

$$R = (C_{(2)} + C_{(3)} + C_{(4)} + C_{(5)} + C_{(6)}) \times F \tag{3-7}$$

$$C'_{(x)} = \begin{cases} R - \alpha & if\ R - C_{(x)} < \alpha\ and\ W_i\ = 0 \\ R + \alpha & if\ C_{(x)} - R < \alpha\ and\ W_i\ = 1 \\ C_{(x)} & otherwise \end{cases} \tag{3-8}$$

In which $C_{(2)}, C_{(3)}, C_{(4)}, C_{(5)}$ and $C_{(6)}$ are the low frequency coefficients in position 2–6 in zigzag scan, R is the embedding threshold value of the host image coefficients, F is the impact factor of low frequency coefficients on determining the threshold, $C_{(x)}$ is the target coefficient for embedding, α is the embedding strength, W_i is the corresponding watermark bit and $C_{(x)}$ is the watermarked coefficients in the selected block.

After embedding all watermark bits, watermarked Y component is returned from frequency domain to spatial domain by inverse DCT or inverse FFT and watermarked Y component is combined with two other original components Cb and Cr. At the end, the image is transformed from YCbCr to RGB color space and the watermarked bits are obtained.

3.2.2.8 Watermark Extraction

In watermark extraction process the zigzag scan is used in order to dividing each block into low, middle and high frequency bands and then extraction operations are performed by investigating the relationship between the frequency coefficients according to:

$$R' = (C'_{(2)} + C'_{(3)} + C'_{(4)} + C'_{(5)} + C'_{(6)}) \times F \qquad \textbf{\textit{(3-9)}}$$

Where $W_i' = \begin{cases} 1 & if\ C'_{(x)} > R' \\ 0 & otherwise \end{cases}$

In which $C'_{(2)}, C'_{(3)}, C'_{(4)}, C'_{(5)}$ and $C'_{(6)}$ are the low frequency coefficients in position 2–6 in zigzag scan, R' is the embedding threshold value of the host image coefficients, F is the impact factor of low frequency coefficients on determining the threshold, $C'_{(x)}$ marked coefficient, W_i' is the extracted watermark bit in the selected block. Finally, the extracted watermark is obtained.

3.3 Summary

In this chapter an evaluation of both spatial and frequency domain watermarking techniques is introduced by comparing three different watermarking techniques which are the LSB, DCT, and FFT. The LSB is considered the basic and traditional technique which is a special domain watermarking, while DCT and FFT are the frequency domain watermarking and are more widely applied Compared to spatial domain.

Chapter Four

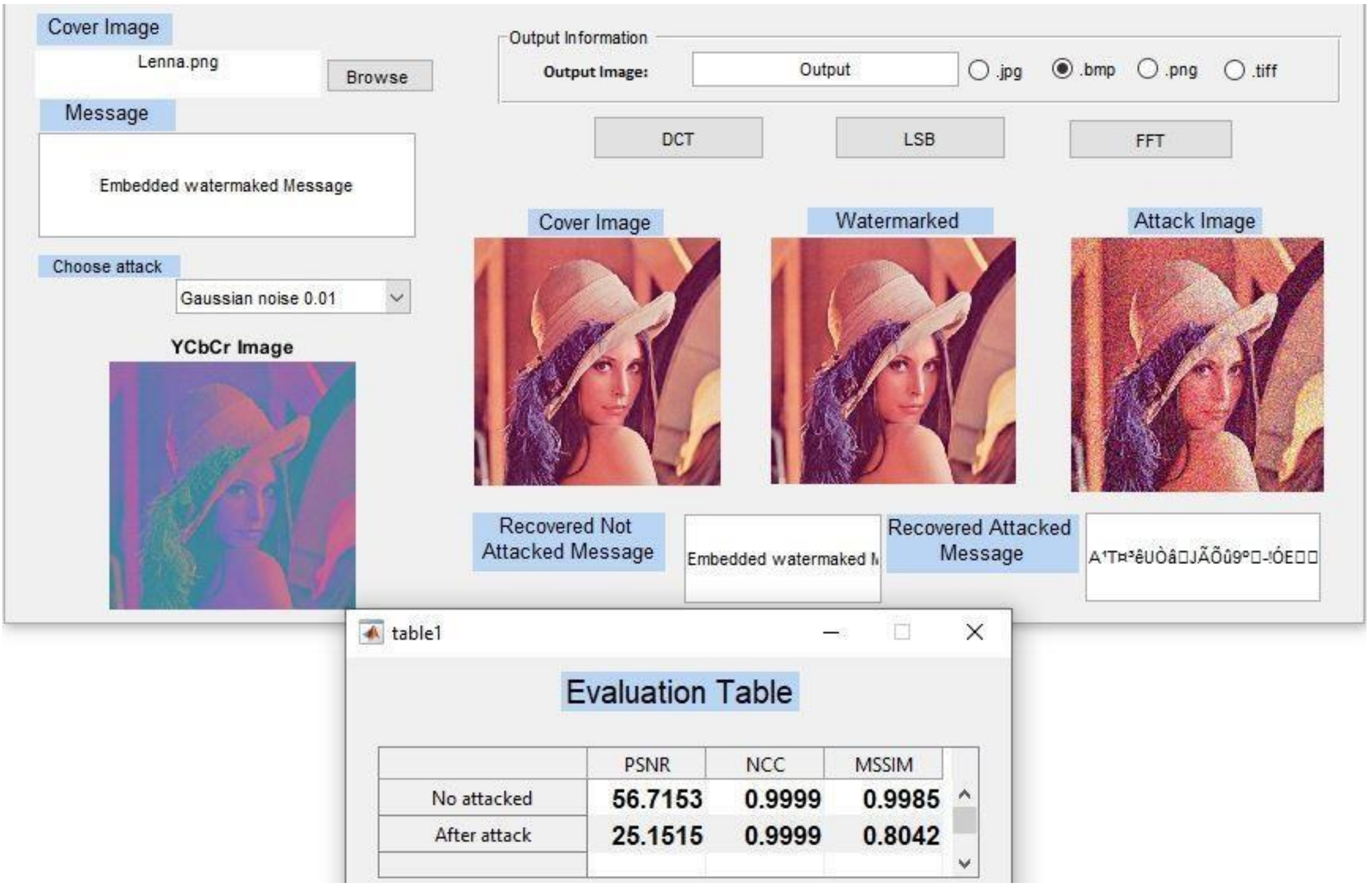
Implementation and Results

4.1 Introduction

This chapter includes implementation and testing of the proposed method for text watermarking into digital images. The implementation and evaluation of the performance is performed by testing the MATLAB application developed using Graphical User Interface (GUI) functionality, with testing image sample and text through pushbuttons and edit text boxes, for more interactive deployment and evaluation.

4.2 The Proposed Method Implementation

The proposed text watermarking method is tested for embedding and extraction of different embedded text watermark sizes into various sizes of host images. One image was selected as example to be listed in this thesis, namely; Lenna with size 512*512 pixels, respectively. Different options are performed for attack type which are: Gaussian noise (0.01 and 0.05), Rotate (10° and 30°), Salt and pepper noise (0.05 and 0.15). Also, Different options are performed for image format (jpg, png, bmp and tiff), watermark embedding mechanism or technique, (DCT, LSB and FFT), and finally watermark extraction results and image performance evaluation metrics (PSNR, NCC and MSSIM), which are shown as in Figure (4-1).



Cover Image: Lenna.png

Message: Embedded watermaked Message

Choose attack: Gaussian noise 0.01

Output Information

Output Image: Output ○ .jpg ● .bmp ○ .png ○ .tiff

Recovered Not Attacked Message: Embedded watermaked M

Recovered Attacked Message: A¹T¤³êUÒâ□JÃÕû9º□-¦ÓE□□

Evaluation Table

	PSNR	NCC	MSSIM
No attacked	56.7153	0.9999	0.9985
After attack	25.1515	0.9999	0.8042

Figure 4-1: Main GUI application interface and performance evaluation metrics table

The evaluation procedure followed in this thesis finds that all types of attacks tested are not recoverable for the tested procedure, while evaluation also considers the effects of embedding and extraction without attacks as shown in the following sections. The definition of each option in figure (4-1) is as follows:

- **Cover image:** Browse the image we want to embed the text watermark in it.
- **Message:** the text watermark we want to hided or embedded in image.
- **Choose Attack:** Choose the type of attack to be embedded into image.
- **Recovered Not Attacked Message:** Extracting the text watermark that was embedded into image that did not get attacked.

- **Recovered Attacked Message:** Extracting the text watermark that was embedded in the image that was attacked.
- **Cover Image:** The original image.
- **Watermarked Image:** The image after embedding the watermark in it.
- **Attacked Image:** The image after it was attacked.
- **Output image:** Saving the output watermarked image in a different format.
- **Evaluation Table:** Shows the results of performance evaluation metrics.

4.2.1 Attacks Evaluation

In this scenario, six attacks effects are evaluated (Gaussian noise 0.01, Gaussian noise 0.05, Rotate 10°, Rotate 30°, Salt and pepper noise 0.05 and Salt and pepper noise 0.15) for the same image and watermark text, shown as in figure (4-1). And will see the effect of each attack on performance evaluation metrics (PSNR, NCC and MSSIM).

4.2.1.1 Normalized Cross Correlation (NCC) Evaluation

The evaluation shows that without attacks the NCC remains high, while attacks perform degradation on the NCC. The result show that the worst case attack can occur in rotation attack an as rotation angle increase the NCC degraded reversely, also in noise addition the as variance of noise increases the NCC degraded, this for the two noise considered which are the Salt and Pepper (S&P) and the Gaussian noise, where generally S&P noise has more effect in image watermark extraction probability as in NCC metric when compared to Gaussian noise. See figure (4-2).

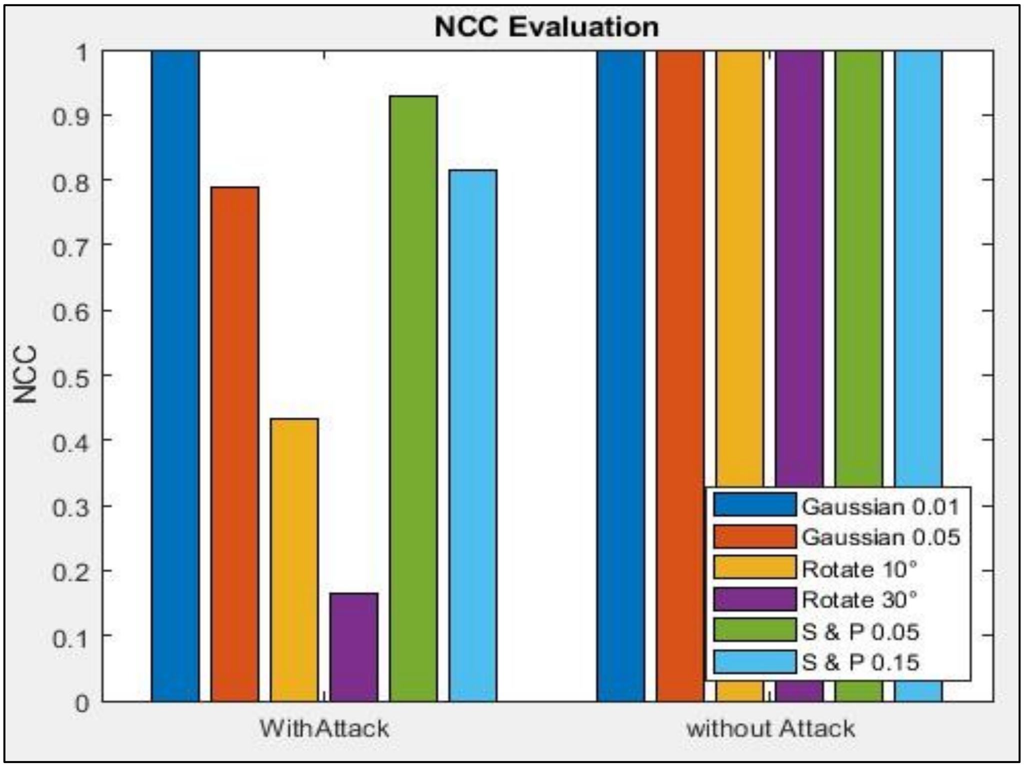


Figure 4-2: NCC evaluation for different types of Attacks

4.2.1.2 Peak Signal-to-Noise Ratio (PSNR) Evaluation

The PSNR also measures the quality of the image which also refers to watermark extraction probability and they are proportional to each other; when PSNR increases the probability of watermark extraction increases, here the results in (4-3) shows that when no attacks were applied the PSNR remains high, while attacks scenarios cause degradation in PSNR with similar corresponding behavior on NCC result before.

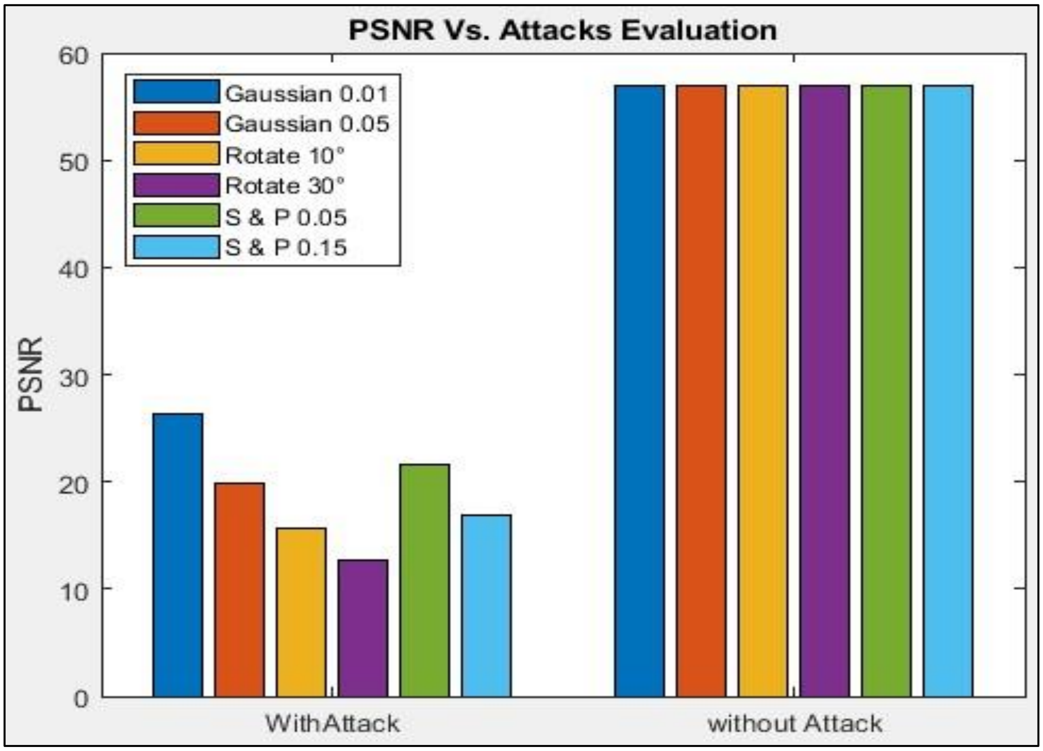


Figure 4-3: PSNR evaluation for different types of Attacks

4.2.1.3 Multi-Scale Structural Similarity Index Measure (MSSIM) Evaluation

The MSSIM represents the number of changes happens in image structure which is less sensitive to geometrical attacks as in rotation as shown in Figure (4-4), while in noise attacks more degradation of MSSIM occur.

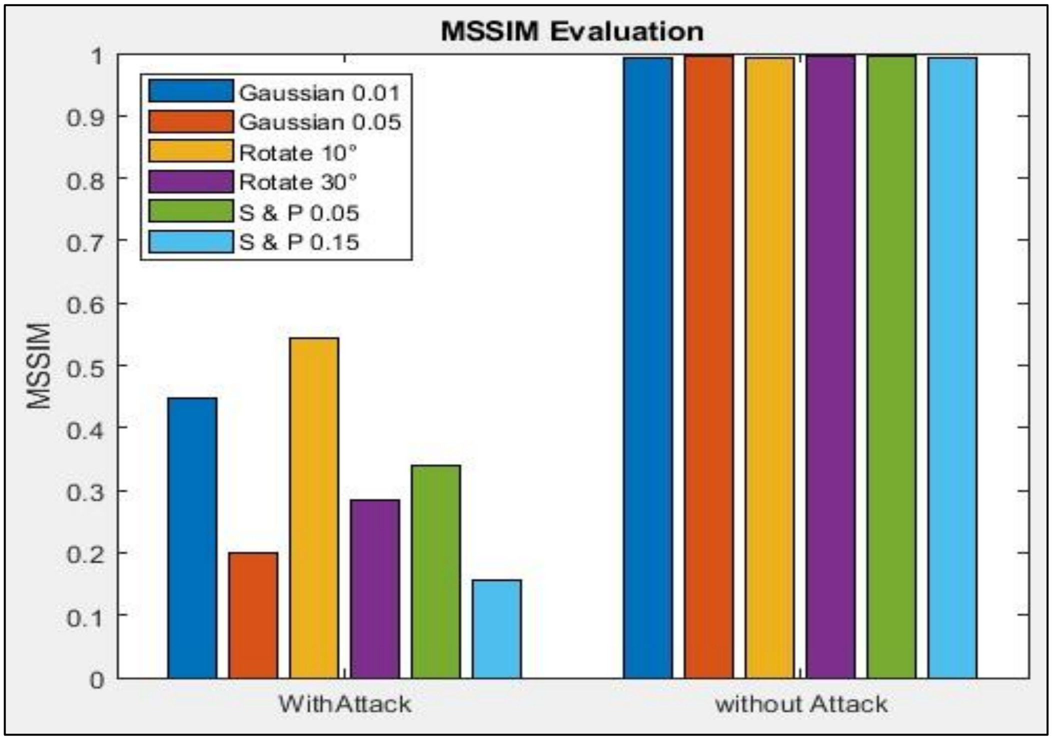


Figure 4-4: MSSIM evaluation for different types of Attacks

4.2.2 Image Formats Evaluation

In image formats evaluation, four different types are tested; BMP, JPG, PNG, and TIFF. We'll see how the image format effects on performance evaluation metrics.

4.2.2.1 Multi-Scale Structural Similarity Index Measure (MSSIM) Evaluation

The evaluation generally shows that in attacks scenarios the MSSIM degraded constantly in all types of attacks, while highest MSSIM can be only achieved when no attack was applied as shown in Figure (4-5).

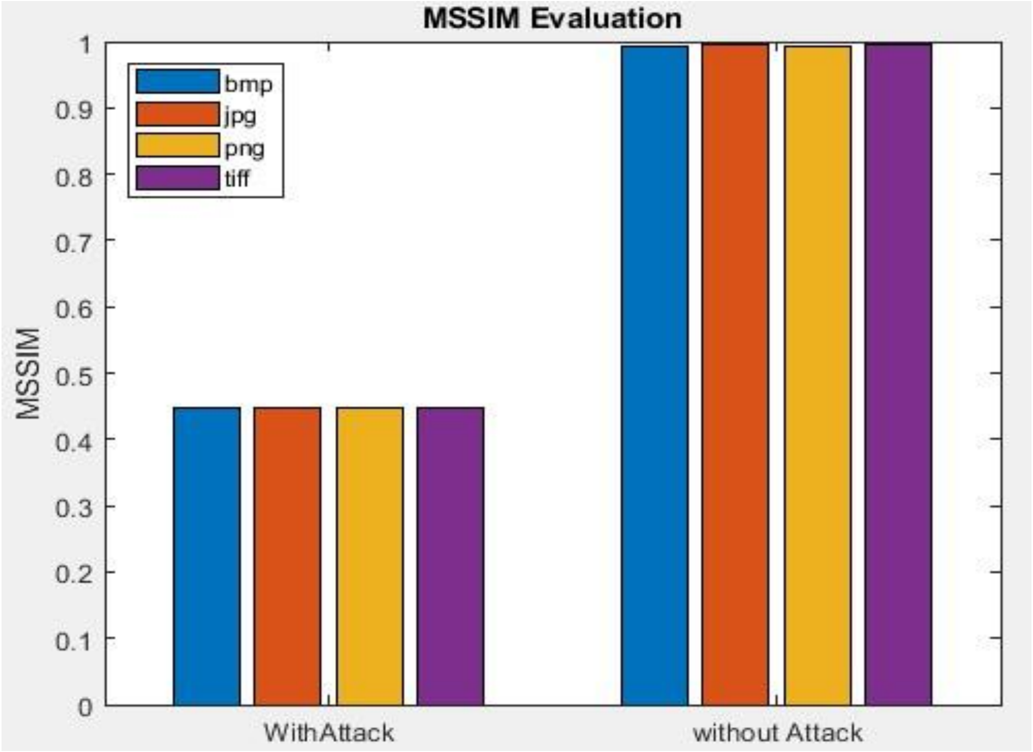


Figure 4-5: MSSIM evaluation for different types of image formats

4.2.2.2 Normalized Cross Correlation (NCC) Evaluation

In NCC evaluation for different image formats, the NCC remains high in all cases even with attacks but only the TIFF format has reduction of NCC as shown in Figure (4-6), which means that the TIFF is the most unsuitable image type that can be used in watermarking.

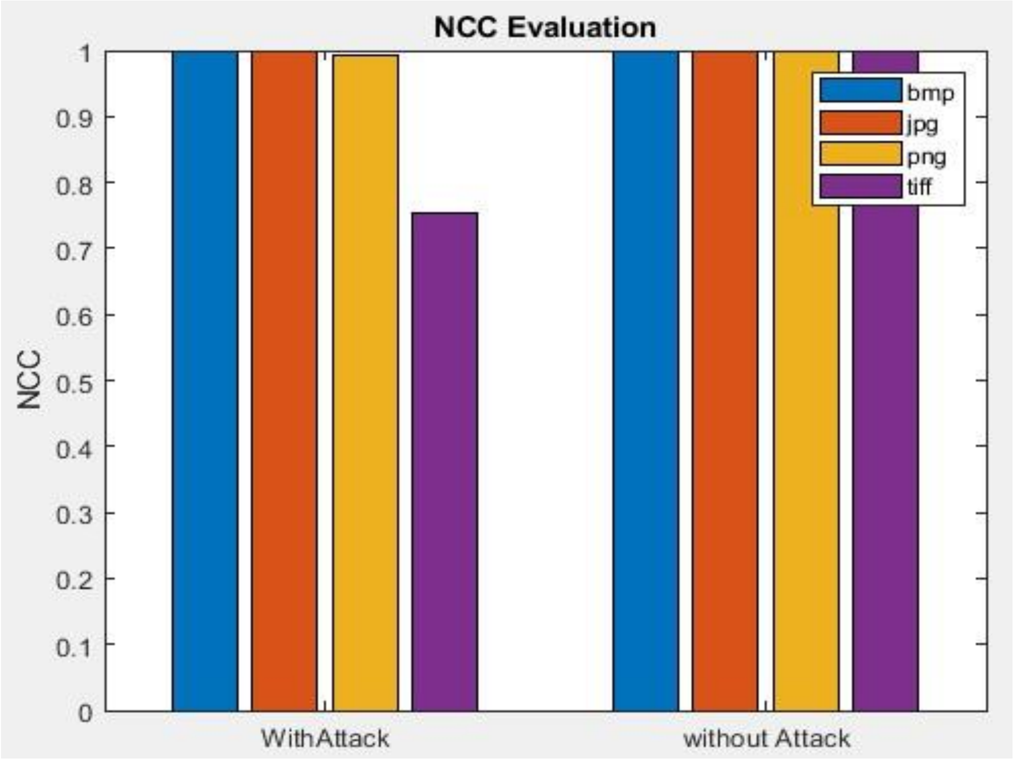


Figure 4-6: NCC evaluation for different types of image formats

4.2.2.3 Peak Signal-to-Noise Ratio (PSNR) Evaluation

In PSNR similar behavior of MSSIM in Figure (4-5) is introduced in Figure (4-7) which confirms the relationship between the MSSIM and PSNR, and degradation is only occur due to the attacks, while highest PSNR can be only achieved when no attack where applied.

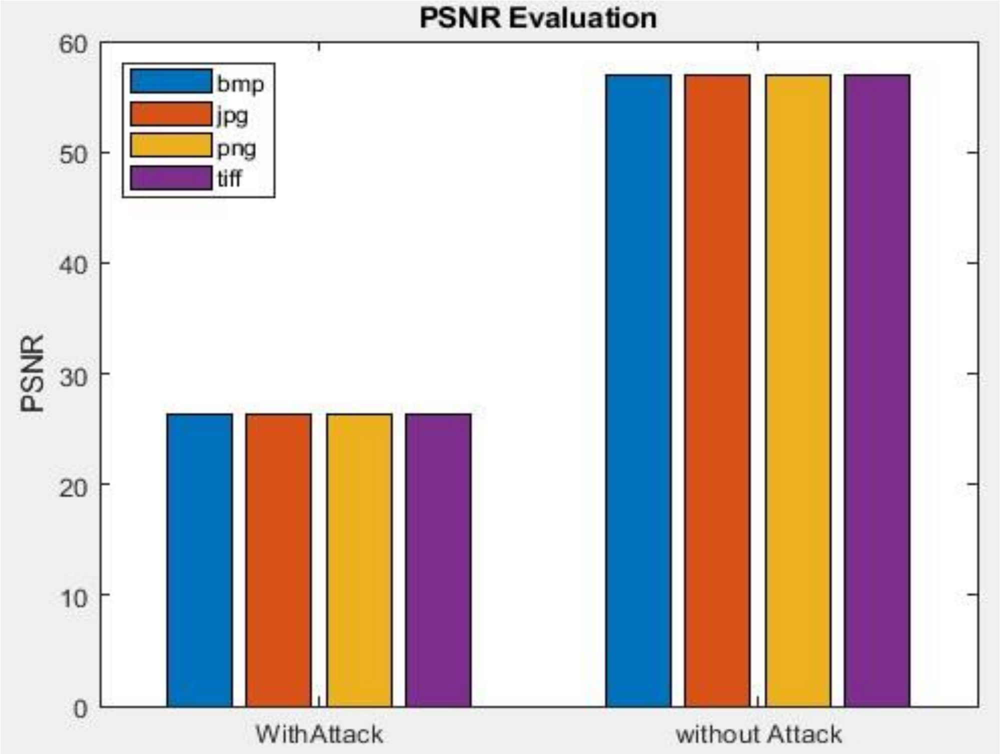


Figure 4-7: PSNR evaluation for different types of image formats

4.2.3 Watermarking Mechanisms or Techniques Evaluation

The evaluation of watermarking mechanism is performed for the three most common watermarking techniques which are the Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT) and Least Significant Bit (LSB). We'll see how different types of watermarking techniques effects on performance evaluation metrics.

4.2.3.1 Multi-Scale Structural Similarity Index Measure (MSSIM) Evaluation

The performance of MSSIM in Figure (4-8) shows there is no a difference between the mechanism except the attack effect. In other words, the evaluation generally shows that in attacks scenarios the MSSIM degraded constantly in all types of attacks, while highest MSSIM can be only achieved when no attack where applied.

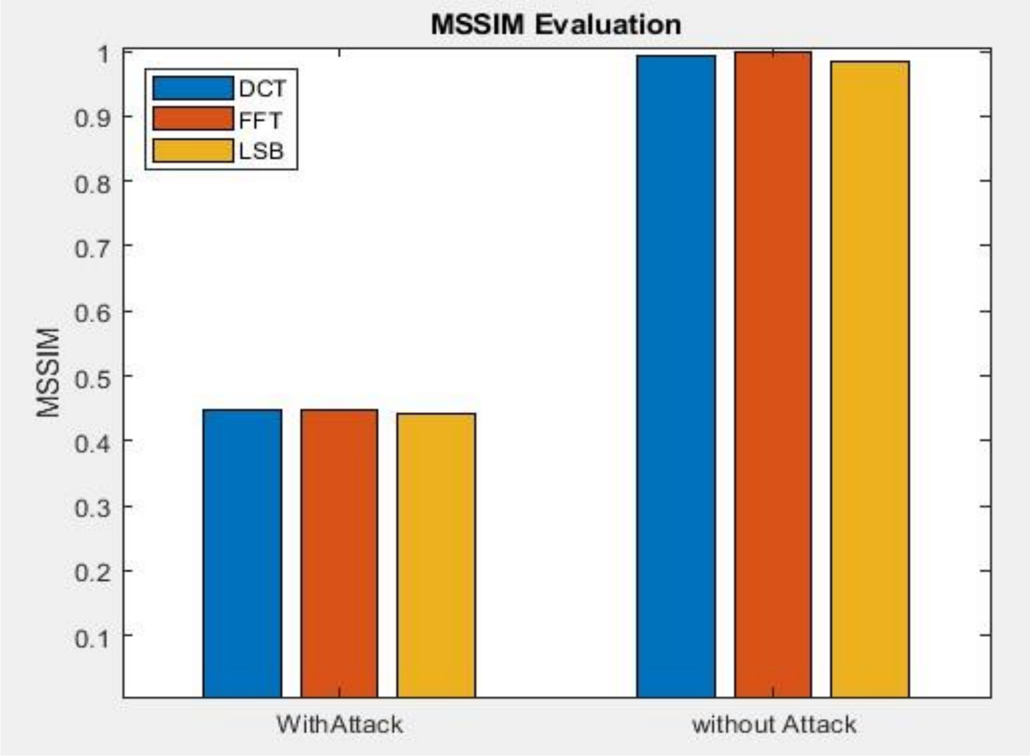


Figure 4-8: MSSIM evaluation for different types of watermarking mechanisms

4.2.3.2 Normalized Cross Correlation (NCC) Evaluation

In NCC evaluation of different mechanism different behavior is introduced, where without attacks the LSB shows the lowest NCC. While with attacks performance differs, where LSB also has the lowest NCC and DCT has the highest NCC, while FFT has an average NCC between other mechanisms. This means that with attacks scenario the best mechanism can be the DCT. See figure (4-9).

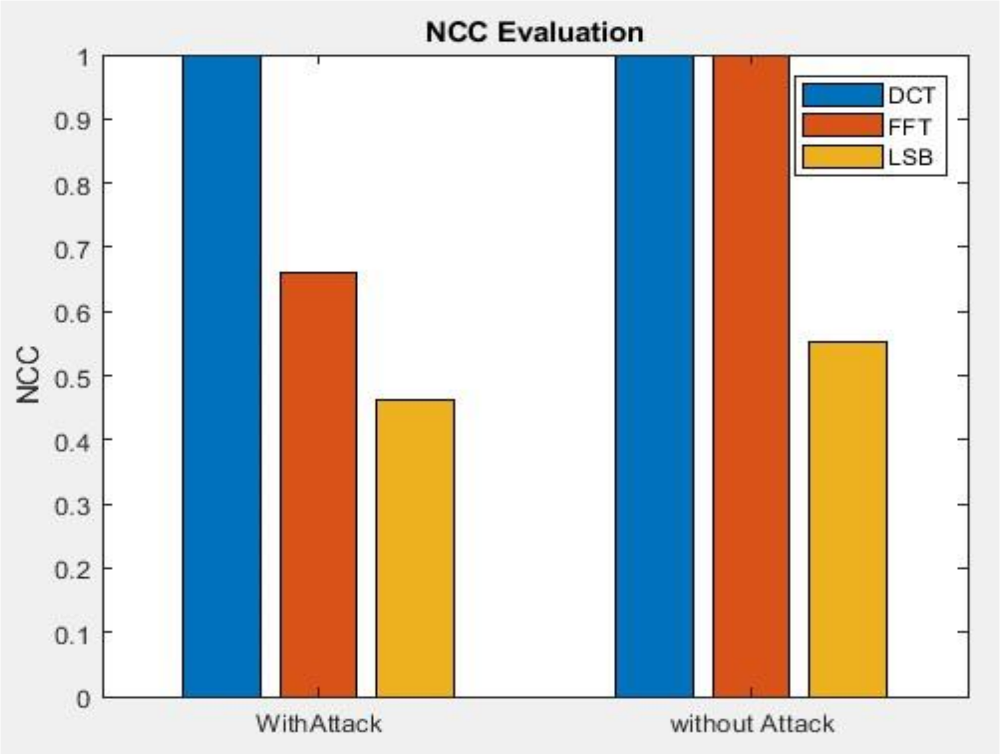


Figure 4-9: NCC evaluation for different types of watermarking mechanisms

4.2.3.3 Peak Signal-to-Noise Ratio (PSNR) Evaluation

In PSNR different behavior has occurred, where with attack scenario the PSNR degraded constantly in all types of attacks and the performance of the three mechanism remains constant. In without attack scenario, FFT has the best PSNR result and LSB has the lowest PSNR, while DCT has an average PSNR performance between others as shown in figure (4-10).

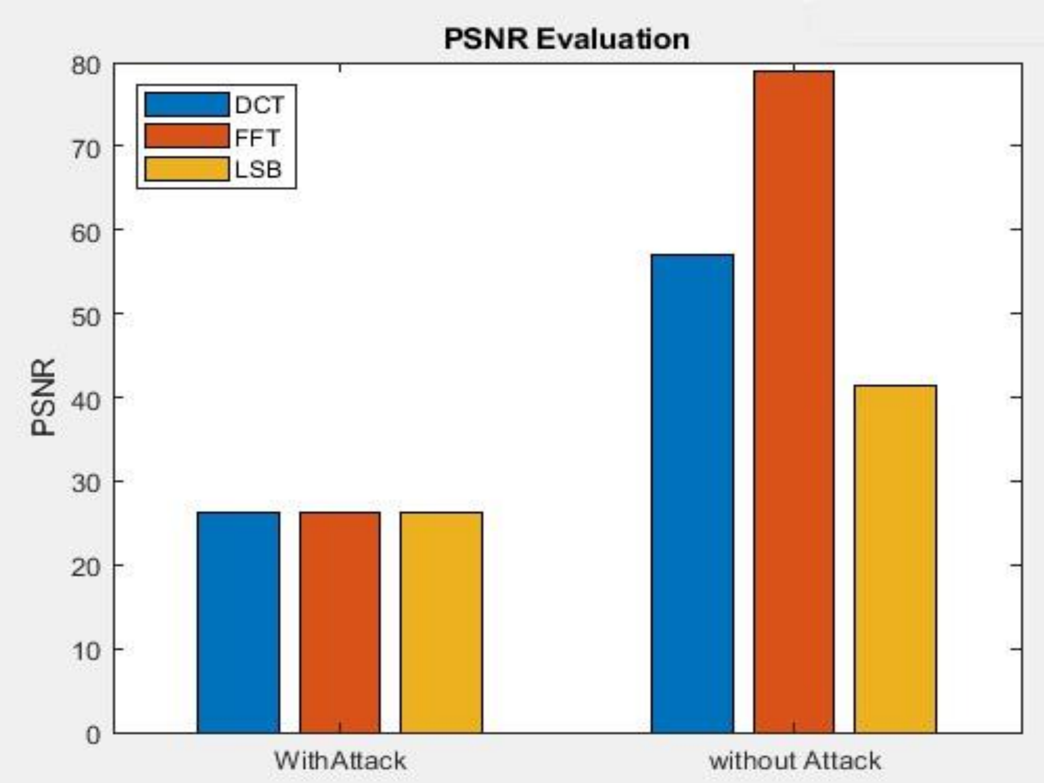


Figure 4-10: PSNR evaluation for different types of watermarking mechanisms

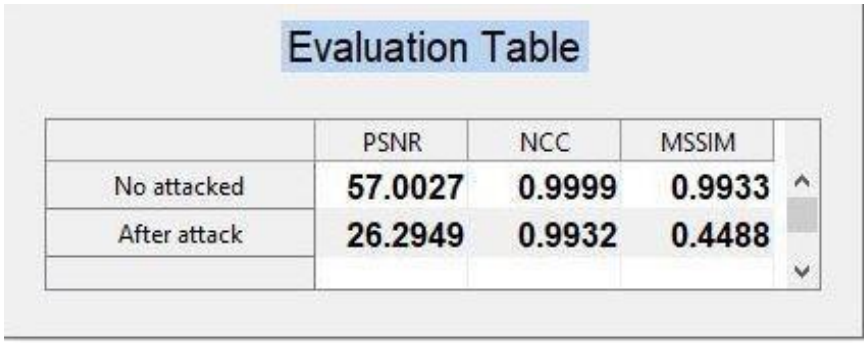
4.3 Discussion of Analysis and Results

In this section the results and the impact of each type of attack on performance evaluation metrics are discussed. And also, the effect of image format and watermarking techniques on performance evaluation metrics.

The results show (in Evaluation Table) that without attacks (no attacks were applied) the performance evaluation metrics (NCC, PSNR and MSSIM) remain high which means a high probability for successful extraction, while attacks perform degradation on them which makes the extraction process hard to be accomplished successfully (This is about attacks evaluation and image formats evaluation).

4.3.1 Gaussian Noise Attack Evaluation

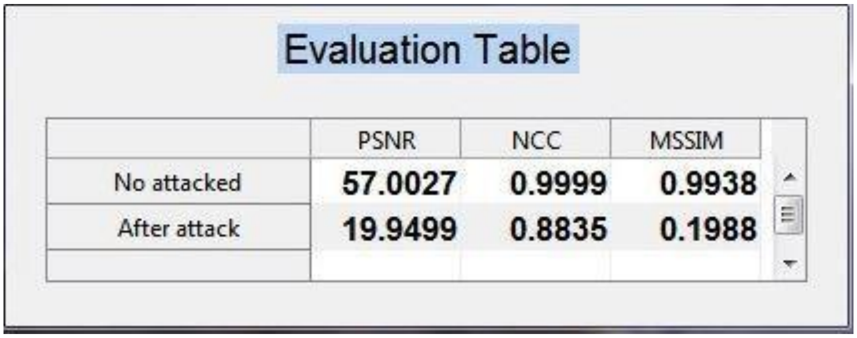
In **NCC**, the Gaussian noise 0.05 attack increases the NCC degraded, while in the Gaussian noise 0.01 attack the NCC remains high. In **PSNR**, the Gaussian noise 0.05 and 0.01 attack increases the PSNR degraded. Where Gaussian noise 0.05 has more effect extraction probability compared to Gaussian noise 0.01. In **MSSIM** more degradation occur when the Gaussian noise 0.05 attack were applied compared to Gaussian noise 0.01. See tables (4-1) and (4-2).



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9933
After attack	26.2949	0.9932	0.4488

Table 4-1: Gaussian noise 0.01 attack evaluation



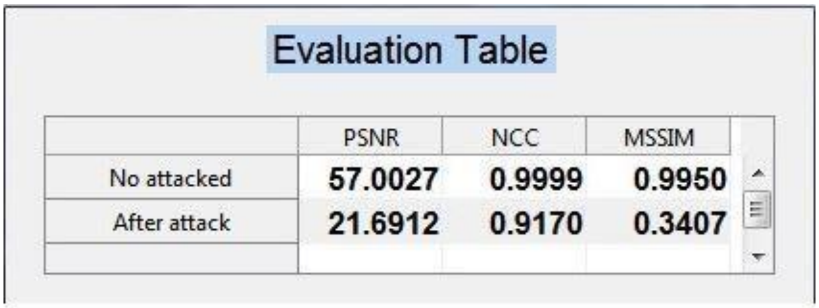
Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9938
After attack	19.9499	0.8835	0.1988

Table 4-2: Gaussian noise 0.05 attack evaluation

4.3.2 Salt and Pepper Noise Attack Evaluation (S&P)

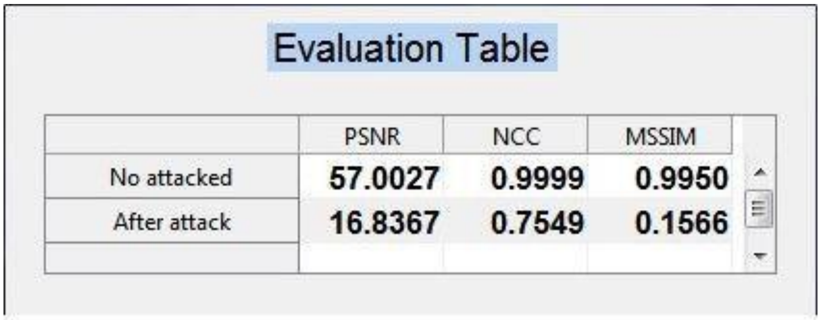
In **NCC**, more degradation occurs when the S&P 0.15 noise attack were applied compared to S&P 0.05 noise attack. In **PSNR**, attacks scenarios causes degradation in PSNR with similar corresponding behavior on NCC result before. In **MSSIM**, the S&P 0.05 and S&P 0.15 noise attack occur more degradation in MSSIM. See tables (4-3) and (4-4).



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9950
After attack	21.6912	0.9170	0.3407

Table 4-3: Salt and Pepper noise 0.05 attack evaluation



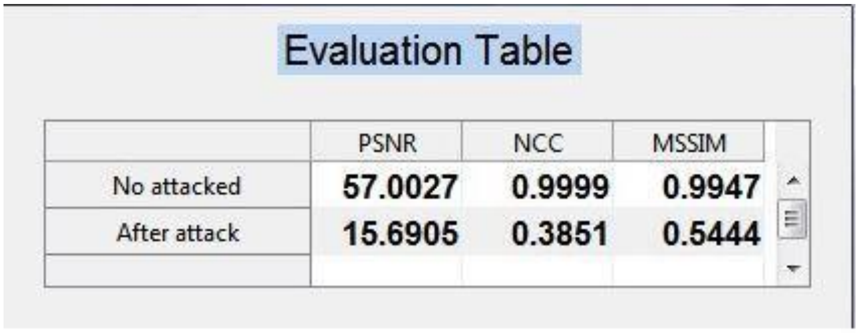
Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9950
After attack	16.8367	0.7549	0.1566

Table 4-4: Salt and Pepper noise 0.15 attack evaluation

4.3.3 Rotation Attack Evaluation

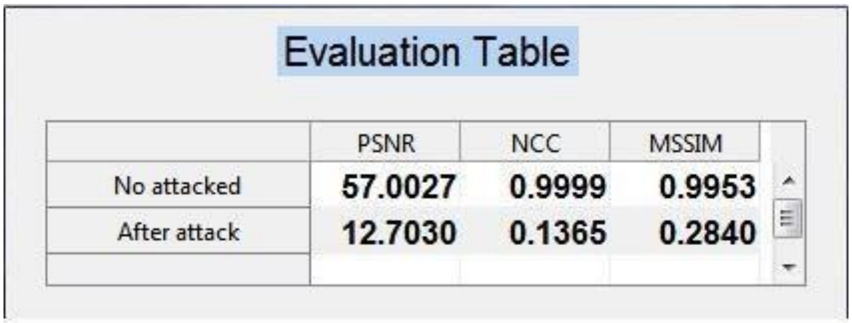
In **NCC**, the result show that the worst case attack can occur in rotation 10° and 30° attack increase the NCC degraded reversely. In **PSNR**, also attacks scenarios causes degradation in PSNR with similar corresponding behavior on NCC result. The **MSSIM** is less sensitive to rotation 10° and 30° attack compared to NCC and PSNR. See tables (4-5) and (4-6).



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9947
After attack	15.6905	0.3851	0.5444

Table 4-5: Rotation 10° attack evaluation



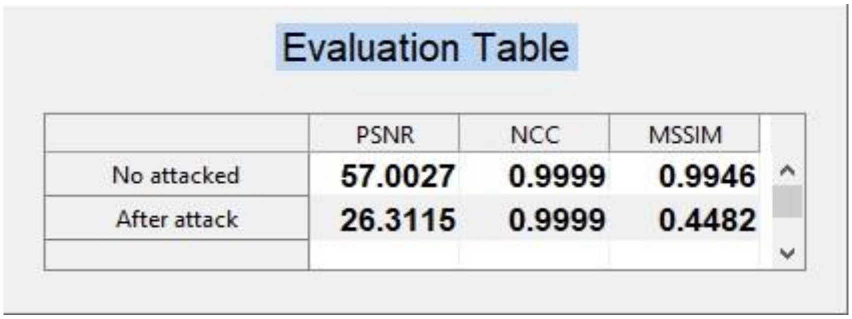
Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9953
After attack	12.7030	0.1365	0.2840

Table 4-6: Rotation 30° attack evaluation

4.3.4 Image Formats Evaluation (JPG, BMP, PNG and TIFF)

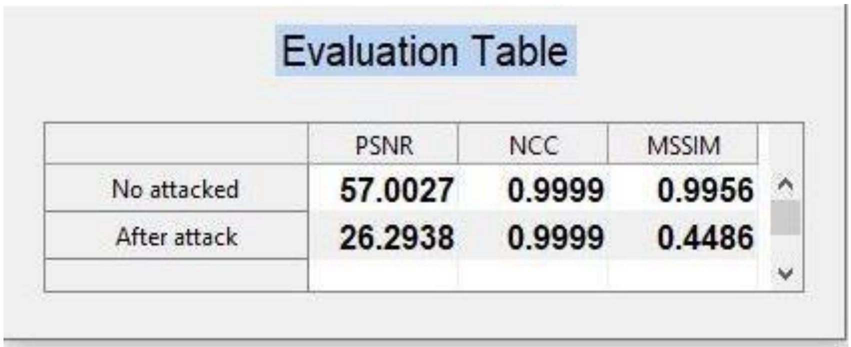
The **NCC** remains high in jpg, bmp and png formats even with attacks but only the tiff format has reduction of NCC. In **PSNR**, in attacks scenarios the PSNR degraded constantly in all types of attacks. The **MSSIM** has similar behavior to PSNR, where only degradation occurs due to attacks. See tables (4-7), (4-8), (4-9) and (4-10).



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9946
After attack	26.3115	0.9999	0.4482

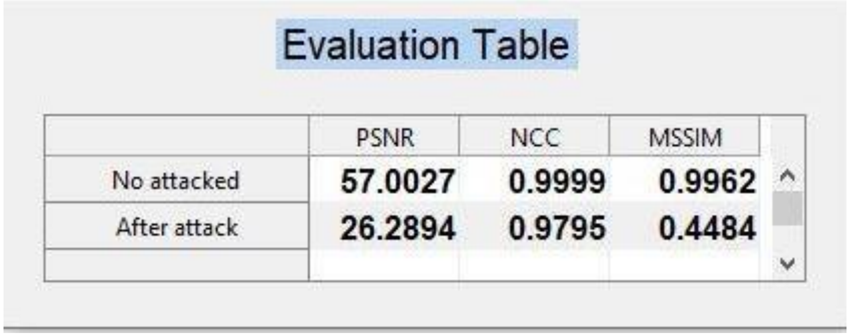
Table 4-7: JPG image format evaluation



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9956
After attack	26.2938	0.9999	0.4486

Table 4-8: BMP image format evaluation



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9962
After attack	26.2894	0.9795	0.4484

Table 4-9: PNG image format evaluation

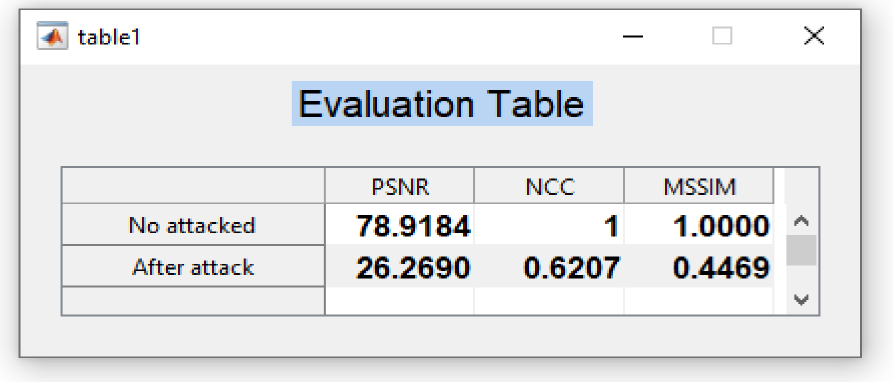


table1

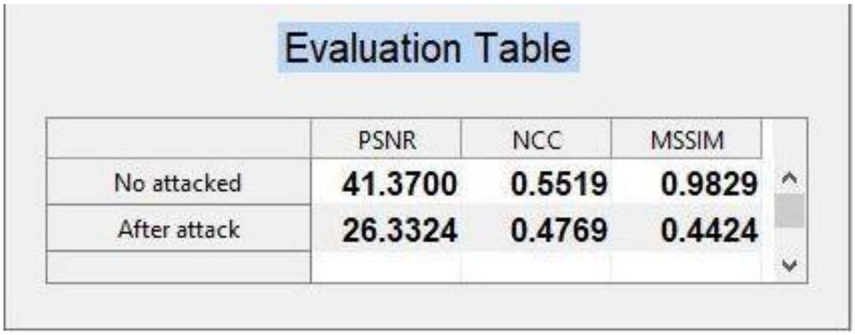
Evaluation Table

	PSNR	NCC	MSSIM
No attacked	78.9184	1	1.0000
After attack	26.2690	0.6207	0.4469

Table 4-10: TIFF image format evaluation

4.3.5 Watermarking Techniques Evaluation (LSB, DCT and FFT)

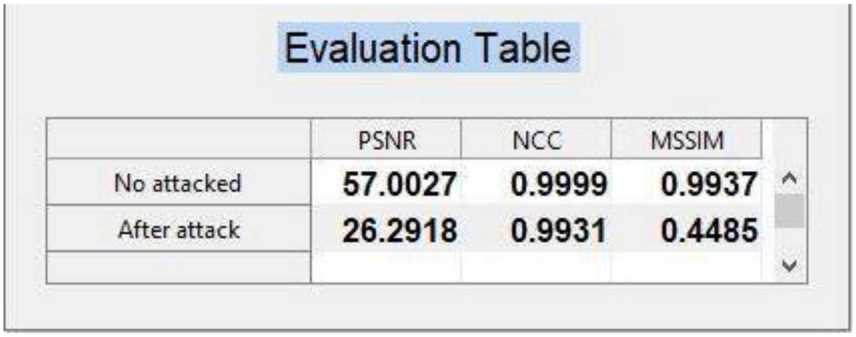
In **NCC,** with no attack applied the LSB shows the lowest NCC. While with attacks DCT has the highest NCC, LSB also has the lowest NCC and FFT has an average NCC between DCT and LSB. In **PSNR,** with attack scenario the PSNR degraded constantly in all types of attacks. While without attack scenario, FFT has the best PSNR result and LSB has the lowest PSNR, while DCT has an average PSNR performance between other mechanisms. In **MSSIM**, the highest of the MSSIM can be only achieved when no attack where applied, while in attacks scenarios the MSSIM degraded constantly in all types of attacks. See tables (4-11), (4-12) and (4-13).



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	41.3700	0.5519	0.9829
After attack	26.3324	0.4769	0.4424

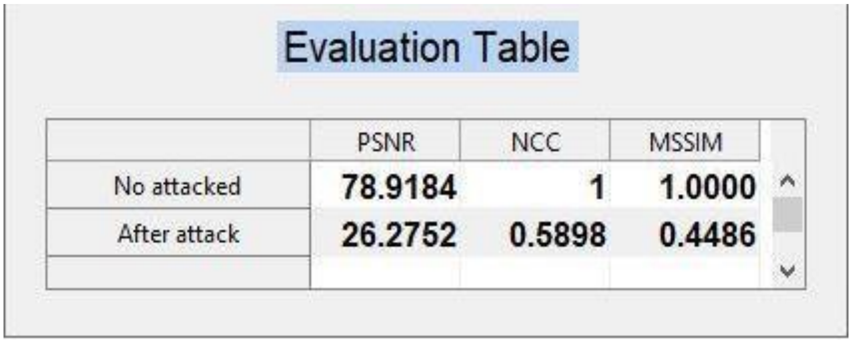
Table 4-11: LSB technique evaluation



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	57.0027	0.9999	0.9937
After attack	26.2918	0.9931	0.4485

Table 4-12: DCT technique evaluation



Evaluation Table

	PSNR	NCC	MSSIM
No attacked	78.9184	1	1.0000
After attack	26.2752	0.5898	0.4486

Table 4-13: FFT technique evaluation

4.4 Table of Summary

In Table (4-14) all the results and impact of each type of attack on performance evaluation measures and also the effect of image format and watermark techniques on it, are summarized.

#	NCC	PSNR	MSSIM
Gaussian noise attack	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
Salt and Pepper noise attack	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
Rotation attack	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
JPG image format	With attack: **high** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
BMP image format	With attack: **high** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
PNG image format	With attack: **high** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
TIFF image format	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**
LSB technique	With attack: **degraded** Without attack: **degraded**	With attack: **degraded** Without attack: **degraded**	With attack: **degraded** Without attack: **high**
DCT technique	With attack: **high** Without attack: **high**	With attack: **degraded** Without attack: **degraded**	With attack: **degraded** Without attack: **high**
FFT technique	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**	With attack: **degraded** Without attack: **high**

Table 4-14: Summary table of results

4.5 Summary

In this chapter the methodology is implemented and evaluation extended to include investigation of different types of watermarking attacks namely geometrical (Rotation) and noise attacks (Gaussian Noise and Salt and pepper noise). Where these types of attack were applied on the watermarked image, and how much they effect on performance evaluation metrics. In addition to the extent to which different watermarking techniques and different types of images format (In case of being attacked or not being attacked) effect on performance evaluation metrics. And then the results are shown for each.

Chapter Five

Conclusion and Recommendations

5.1 Conclusion

Watermarking had found a lot of attention lately, especially with the huge digital information propagation and transactions, and it's considered as a formal copyright process in digital media. This thesis included the development, design, implementation, and testing of text watermarking algorithm into digital images. Embedding of the text contents was investigated for various sizes of images and different length of texts. The proposed method produces watermarks that are imperceptible by visual inspection and was implemented and tested for copyright protection and ownership judgment.

In this study an evaluation of both spatial domain and frequency domain watermarking techniques are introduced by comparing three different watermarking techniques which are the Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Fast Fourier Transform (FFT). The LSB is considered the basic and traditional technique which is a special domain watermarking technique, while DCT and FFT are the frequency domain watermarking technique. The methodology is implemented using MATLAB and evaluation extended to include investigation of different types of watermarking attacks namely geometrical attacks (Rotation) and noise attacks (Gaussian Noise and Salt and pepper noise). Also, different types of image formats are evaluated which are the BMP, JPG, PNG, and TIFF. Finally watermark extraction results and image evaluation performance metrics (PSNR, NCC and MSSIM) are mathematically described. The results show that generally the spatial domain technique LSB is more sensitive to geometrical attacks such as rotation, while frequency domain techniques are more sensitive to noise attacks such as Gaussian Noise and Salt and pepper noise. The DCT mechanism introduces good behavior in attack scenario as shown in NCC result chapter four, while FFT has the best performance in without attack scenario. Degradation of PSNR and MSSIM is introduced with all attack scenarios which is an expected behavior and represents a further study challenge. In image formats evaluation different types of image extension shows no difference except the attack effect, but the TIFF format introduced a low NCC value in attack scenario which makes it not suitable for such watermarking application.

5.2 Recommendations

Finally, it's recommended for such projects researchers to have a good background on basic Digital Image Processing (DIP) Techniques and media data domain transformation for descriptive compression and clean watermarking such as DCT and FFT technique which are very basic in Digital Signal Processing (DSP). The recommendations and improvement or evaluation to the proposed method would include the following:

1. Trying the possibility of coupling this method with other watermarking methods. i.e., working on hybrids watermarking methods in order to get more satisfactory results.
2. Using this method for short message exchange or emails over smart telephones.
3. Design, test and implement online chat system with text watermarking capabilities.
4. Develop the method in order to use Arabic text watermarking.
5. Improve system that can use a watermarking on 3D images.
6. Evaluation of image size, text (watermark) length, capacity of watermark and image compression techniques such as JPEG and Wavelet compression technique.
7. Support of JPG formats for better watermark extraction.
8. Support of successful text watermark extraction for noise and geometrical attacks scenarios.

References

1. Hebah H.O. Nasereddin, (2011), “Digital Watermarking a Technology Overview”. www.arpapress.com, Volume 6, Issue 1.
2. Jobin Abraham, (2011), “Digital Image Watermarking Overview”. National Seminar on Modern Trends in EC&SP.
3. Shraddha S. Katariya, “Digital Watermarking: Review”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 1, Issue 2, February 2012.
4. Chugh, Gunjan, “Information Hiding - Steganography & Watermarking”, International Journal of Advanced Research in Computer Science. Mar/Apr2013, Vol. 4 Issue 2, p165-171. 7p.
5. Provos Niels, (2009), "Hide and Seek: Introduction to steganography". IEEE Computer society.
6. Cox Ingemar J., Matthew L. Miller and Jeffrey A. Bloom, (2008), "Handbook of Digital Watermarking". Morgan Kaufmann Publishers, Inc., San Francisco.
7. 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.
8. Petitcolas, Fabien A. P., (2002), (Ed.), “Proceedings of the 5th International Workshop on Information Hiding”, Lecture Notes in Computer Science (LNCS) by Springer Verlag, vol. 2578, The Netherlands.
9. Gaurav Chawla, Ravi Saini, Rajkumar Yadav, and Kamaldeep, (2012), “Classification of Watermarking Based upon Various Parameters”. International Journal of Computer Applications & Information Technology, Vol. I, Issue II, (ISSN: 2278-7720).
10. Jonathan k. su, Frank hartung and Bernd girod, (2000), “Digital Watermarking of Text, Image, and Video Documents”, Comput. & Graphics, Vol. 22, No. 6, pp. 687-695.
11. Hyoung Joong Kim, (2004), “Audio Watermarking Techniques”. Department of Control and Instrumentation Engineering, Kangwon National University, Korea.
12. Swati Dhiman and Onkar Singh, (2016), “Analysis of Visible and Invisible Image Watermarking – A Review”. International Journal of Computer Applications (0975 – 8887). Volume 147 – No.3.

13. Shruti Sharma and Asst. Prof. Vivek Kumar, “A Survey of Blind & Non-Blind Watermarking Techniques”, International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016.

14. Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and Vineeth Sarma Venugopala Sarma, (2010), “Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques”, International Conference on Signal Acquisition and Processing.

15. Chih-Hung Lin, “Multi-purpose Digital Watermarking Method – Integrating Robust, Fragile and Semi-fragile Watermarking”, International Journal of Innovative Computing, Information and Control, Volume 6, Number 7, July 2010.

16. Yukti Varshney, (2017), “Attacks on Digital Watermarks: Classification, Implications, and Benchmarks”. International Journal on Emerging Technologies (Special Issue NCETST-2017) 8(1): 229-235.

17. Vinicius Licks and Ramiro Jordan, “Geometric Attacks on Image Watermarking Systems”, IEEE Computer Society August 2015.

18. Harsh K Verma, Abhishek Narain Singh and Raman Kumar, International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

19. Eduardo Fragoso, Kevin Rangel, Mariko Nakano, Manuel Cedillo and Hector Perez, (2021), “Seam Carving based visible watermarking robust to removal attacks”. Journal of King Saud University - Computer and Information Sciences.

20. Mohammad Rizwan Khan, Ankur Goyal, “Gaussian Noise attack Analysis of Non-Blind Multiplicative Watermarking using 2D-DWT”. International Journal of Computer Science and Information Technologies, Vol. 7 (6), 2016.

21. Hilario Moreno, Pedro Gil, Sergio Arroyo, Roberto Sastre and Saturnino Maldonado, “A Salt and Pepper Noise Reduction Scheme for Digital Images Based on Support Vector Machines Classification and Regression”. The Scientific World Journal Volume 7, July 2014.

22. Begum, M. Sharma and Mohammad Shorif Uddin,"Digital Image Watermarking Techniques". Information 2020, 11, 110; doi: 10.3390/info11020110.

23. Chetna and Krishan Kumar, “Data and Information Hiding on Color Images Using Digital Watermarking”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014.
24. Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen and Tao Ya, “New Rapid and Robust Color Image Watermarking Technique in Spatial Domain”, IEEE. Translations and content mining are permitted for academic research only. Volume 7, 2019.
25. V. Jain, L. Kumar, M. Sharma, M. Sadiq, and K. Rastogi, (2017). "Image Watermarking based on modified LSB method," J Glob Res Comput Sci, vol. 3.
26. Andreja Samcovic and Jan Turan, “Digital Image Watermarking by Spread Spectrum”, International Conference on Communications, July 2014.
27. Khaled Mahmoud, Sekharjit Datta and James Flint, (2005). “Frequency Domain Watermarking”. The International Arab Journal of Information Technology, Vol. 2, No. 1.
28. Mohamed A. Suhail and Mohammad S. Obaidat, “Digital Watermarking-Based DCT and JPEG Model”, IEEE Transactions on Instrumentation and Measurement, Vol. 52, No. 5, October 2003.
29. Shelvie Nidya Neyman, I Nyoman Prama Pradnyana and Benhard Sitohang, “A New Copyright rotection for Vector Map using FFT-based Watermarking”, TELKOMNIKA, Vol.12, No.2, June 2014.
30. André Rodrigues, Fabiana Fernandes and Zélia Peixoto e Flávia Freitas, (2013). “Evaluation of Image Color Metrics for Watermarked Color Images”. Xxxi brazilian telecommunication symposium – sbrt'13, fortaleza, ce.
31. Asim Naveed, Yasir Saleem, Nisar Ahmed, Aasia Rafiq, (2015) “Performance Evaluation and Watermark Security Assessment of Digital Watermarking Techniques”, Int. (Lahore), 27(2), 1271-1276.
32. M. Cadik and P. Slavik, (2004). “Evaluation of two principal approaches to objective image quality assessment”, 8th International Conference on Information Visualisation, IEEE Computer Society Press, pp. 513-551.
33. P. Gabriel, Guibelalde, Eduardo, Chevalier, Margarita, Turrero and Agustin, (2011). "Use of the cross-correlation component of the multiscale structural similarity metric (R* metric) for

the evaluation of medical images: R* metric for the evaluation of medical images". Medical Physics. 38 (8): 4512–4517.

34. Hossain M., S. Al Haque, and F. Sharmin, (2010), Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information. The International Arab Journal of Information Technology (IAJIT), Vol. 7, No. 1, PP34-38.
35. Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A. AbuJazar and Rushdi Abu Zneit, (2010), Optimized TrueColor Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952.
36. Bamatraf, A., Ibrahim, R., &Salleh, M. N. B. M. (2010). Digital watermarking algorithm using LSB. In Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference (pp. 155-159).
37. Dasgupta K., J.K. Mandal and P.Dutta, (2012) Hash Based Least Significant Bit Technique for Video Steganography (HLSB). International Journal of Security. Privacy and Trust Management (IJSPTM), Vol. 1, No. 2.
38. Sruthi, N., Sheetal, A. V., &Elamaran, V. (2014, April). Spatial and spectral digital watermarking with robustness evaluation. In Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on (pp. 500-505). IEEE.
39. Ghosh, S., De, S., Maity, S. P., &Rahaman, H. (2015). A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using Extended Hamming Code. In Electrical Information and Communication Technology (EICT), 2015 2nd International Conference on (pp. 167-172). IEEE.
40. Kumar, S., &Dutta, A. (2016). A novel spatial domain technique for digital image watermarking using block entropy. In Recent Trends in Information Technology (ICRTIT), 2016 International Conference on (pp. 1-4). IEEE.
41. Mathur, S., Dhingra, A., Prabukumar, M., Agilandeeswari, L., &Muralibabu, K. (2016). An efficient spatial domain based image watermarking using shell based pixel selection. In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 2696-2702). IEEE.
42. Karan Singh Rajawat, Deepak Chaudhary and Dr. Amit Kumar, (2014). Watermarking Text and Image with Encryption. International Journal of Scientific & Engineering Research, Volume 5, Issue 5, ISSN 2229-5518.

43. Preeti Gaur, Neeraj Manglani, “Image Watermarking Using LSB Technique”, International Journal of Engineering Research and General Science Volume 3, Issue 3, June 2015.

44. Rajni Verma and Archana Tiwari, “Copyright Protection for Watermark Image Using LSB Algorithm in Colored Image”. Advance in Electronic and Electric Engineering, ISSN 2231-1297, Volume 4, Number 5 (2014), pp. 499-506.

45. Mahdieh Ghazvini, Elham Mohamadi Hachrood and Mojdeh Mirzadi, (2017), “An Improved Image Watermarking Method in Frequency Domain”. Journal of Applied Security Research,ISSN 1936-1610, VOL. 12, NO. 2, 260–275.

46. Hui Yong Li, Hong Xu Jiang, Ping Zhang, Han Qing Li and Qian Cao, (2014). Efficient RGB to YCbCr Color Space Conversion for embedded application. Applied Mechanics and Materials Vols 543-547 (2014) pp 2873-2878 Trans Tech Publications, Switzerland.

47. Reem A.Alotaibi and Lamiaa A.Elrefaei, “Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)”. Applied Computing and Informatics,Volume 15, Issue 2, July 2019.

48. Chia-Chen Lin and Pei-Feng Shiu, “High Capacity Data Hiding Scheme for DCT- based Images”, Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, No. 3, pp. 220-240, July 2010.

49. Viraktamath S. V., Dr. Girish V. Attimarad, (2011), “Impact of Quantization Matrix on the Performance of JPEG”. International Journal of Future Generation Communication and Networking, Vol. 4, No. 3.

50. Walaa M. Abd-Elhafiez, Wajeb Gharibi, (2012), “Color Image Compression Algorithm Based on the DCT Blocks”. International Journal of Computer Science Issues, Vol. 9, Issue 4, No. 3.

51. S Sankar and Dr. S Nagarajan, (2014), “ZZRD and ZZSW: Novel Hybrid Scanning Paths for Squared Blocks”. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, pp. 10567-10582.