جـامـعـة الـشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

An Improved Text Watermarking Algorithm for Color Images

خوارزمية محسنة للعلامات المائية النصية في الصور الملونة

Prepared by

Akram Naser Al-Dakari

Supervisor

Prof. Hamza Abbass Al-Sewadi

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

Department of Computer Science

Faculty of Information Technology

Middle East University

May, 2017


بسم الله الرحمن الرحيم
وَقُلِ اعْمَلُوا
فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ
سورة التوبه

Authorization statement

I, Akram Naser Adam Al-Dakari, authorize the Middle East University to provide hard copies or soft copies of my Thesis to libraries, institutions or individuals upon their request.

Name: Akram Naser Adam Al-Dakari

Date: 12 / 08 / 2017

Signature: 

اقرار تفويض

انا أكرم ناصر الدغاري افوض جامعة الشرق الاوسط بتزويد نسخ من رسالتي ورقياً و الكترونياً للمكتبات، او المنظمات، او الهيئات و المؤسسات المعنية بالابحاث و الدراسات العلمية عند طلبها.

الاسم : أكرم ناصر ادم الدغاري

التاريخ :2017/08/12

التوقيع:

Examination Committee Members: Signature

Prof. Hamza Abbass Al-Sewadi (Supervisor & Chairman)

Computer Information System Department,

Middle East University (MEU)

Hamza A-Ali

12-8-2017

Dr. Ahmad Adel Ahmad Abu- Shareha (Internal examiner)

Computer Information System Department,

Middle East University (MEU)

Prof. Wesam Abdel Rahman Moh'd Al-Mobaideen (External examiner)

Computer Science Department,

The University of Jordan

2017/8/16

Acknowledgement

First of all, thanks to his almighty God for his blessing and support for giving the opportunity of this achievement, despite various difficulties and frustrations.

I would like to express my thanks and gratitude to my supervisor, prof. Hamza Abbass Al-Sewadi for his continuous scientific support, suggestions, guidance, and patience throughout the project progress, besides his fatherly care.

My deep gratitude to prof. Ziad Al-Qadhi for his valuable support and suggestions.

Thanks are also due to the Middle East University and all its Faculty members and staff members who were generous in their teaching and academic services.

Finally, my deepest thanks and unlimited love to my wife and son who were so helpful and patience in supporting me throughout the completion of thesis with pleasant time.

Dedication

To the beloved lady who suffered, cared, and prayed for my success, my mother.

To the great man who taught me honesty, humbleness with dignity, my father.

To the sole which I loved and never forget, my mother in law.

To the candles of my life; my wife, my son, my brothers & sisters, and all the faithful friends for their unlimited love and support,

For them all, I dedicate this humble work

Table of Content

List Of Tables

List of Figures

List of Symbols

Symbol	Description
M*N	The Number of Rows and Columns in the Input Images
I (m, n)	The Value of the Pixel Located at m and n Position in the Image
R	The Maximum Possible Pixel Value of the Image
Y	The Luminance of the Image
U, V	Consists of the Color Information
A	Original Text Message after Vectoriztion
E_t	Encrypted Text
D_t	Decrypted Text
PK	Private Key
PK^{-1}	Inverse Private Key

List of Abbreviations

Abbreviations	Meaning
LSB	Least Significant Bit
DWT	Discrete Wavelet Transform
SVD	Singular Value Decomposition
DCT	Discrete Cosine Transform
IHW	Information Hiding Workshop
SPIE	Society of Photo-optical Instrumentation Engineers
CPTWG	The Copy Protection Technical Working Group
SDMI	The Secure Digital Music Initiative
BSS	Blind Source Separation
VQ	Vector Quantization
HWT	Haar Wavelet Transformation
DFT	Discrete Fourier Transform
DLT	Discrete Laguerre Transform
DHT	Discrete Hadamard Transform
HVS	The Human Visual System
MSE	The Mean-Squared Error
PSNR	Peak Signal-to-Noise Ratio
ASCII	The American Standard Code for Information Interchange
ANSI	The American National Standards Institute
YUV	YUV Color Model
YIQ	YIQ Color Model

IS	**Image Size**
S	**Secret message Size**
SK	**Secret Key**
NI	**Noisy Image**
PK	**Private Key**
ET	**Encryption Time**
DT	**Decryption Time**

An Improved Text Watermarking Algorithm for Color Images

Prepared By

Akram Naser Al-Dakari

Supervisor

Prof. Hamza Abbass Al-Sewadi

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, proposes a text watermarking algorithm 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 color images. The embedding process relies on the insertion of the texts elements randomly into the color image as noise, where the randomness is achieved by the use of random number generator that is arranged to be influenced by the image size as well as the text watermark length. Initially, three color image processing methods; separate color channels, direct conversion to grey and YIQ model, were studied and compared with each other for processing speed first, and the YIQ model was found the fastest, and hence it is adopted for the embedding process. An optional choice of encrypting the text watermark before embedding is also suggested (in case required by some applications), where, the text can is encrypted using a matrix manipulation method before embedding into images is executed, adding more difficulty to hackers.

Experimental results of applying the proposed algorithm for embedding and extraction of text watermarks of various content combinations and sizes into vast number of images were satisfactory, as they resulted into an improvement of more than double in speed of embedding and extraction than other systems (such as least significant bit method, LSB) and fairly acceptable level of peak signal to noise ratio (PSNR) with low mean square error values, however PSNR deteriorates faster than LBS technique with the watermark text size increases, therefore it is found more suitable for watermarking application, rather than for steganography that is used for secure information exchange purposes.

Keywords: Digital watermarking, Copyright protection, Ownership judgment, Cryptography, Steganography.

خوارزمية محسنة للعلامات المائية النصية في الصور الملونة

إعداد

أكرم ناصر الدغاري

إشراف

أ.د. حمزة عباس السوادي

المُلخص

تتم حماية حقوق الطبع وأحكام الملكية للوسائط المتعددة الرقمية (كالنصوص والصوت والصور الثابتة والمتحركة) هذه الايام باستخدام العلامات المائية الرقمية. تقدم هذه الرسالة خوارزمية للعلامات المائية النصية لحماية حقوق وأحكام الملكية للوسائط المتعددة. وهي تركز على عملية الاخفاء لنصوص صغيرة او معلومات المالك في الصور الملونة. وتعتمد عملية الاخفاء على ادخال اجزاء النصوص عشوائيا كضوضاءً في الصورة الملونة. حيث يتم الحصول على العشوائية باستخدام مولد ارقام عشوائية تتأثر قيمها بحجم الصورة المستخدمة وطول النص للعلامة المائية.

درست ثلاثة طرق معالجة الصور في البداية وهي طريقة قنوات الالوان المنفصلة وطريقة التحويل المباشر للون الرمادي ونموذج YIQ للصور, وقورنت سرعة المعالجة لها مع بعضها, وقد كانت سرعة المعالجة لنموذج YIQ هي الاسرع وعندئذ تم اختيارها لعملية الاخفاء. كما طرح اقتراح اضافة خطوة اختيارية بتشفير النصوص قبل الاخفاء (في حالة الحاجة اليها في بعض التطبيقات), حيث يمكن تشفير النصوص بطريقة المناورة بالمصفوفات قبل تنفيذ الاخفاء في الصورة مما يزيد الصعوبة على القراصنة.

كانت النتائج التجريبية لتطبيق الخوارزمية المقترحة لإخفاء واستخراج العلامات المائية ولاطوال مختلفة و محتويات مختلفة للنصوص مقنعة, حيث نتج عنها تحسن في سرعة الاخفاء والاستخراج بأكثر من ضعف سرعة النظم الاخرى (مثل طريقة المرتبة الاقل اهمية) وكذلك مستوى مقبول جداً من نسبة الاشارة الى الضوضاء (PSNR) مع معدل مربع الخطأ منخفض , إلا

انه تبين بان PSNR يتناقص اسرع من تقنية المرتبة الاقل اهمية مع زيادة حجم نصوص العلامة المائية, ولهذا وجد بان الخوارزمية المقترحة اكثر مناسبة لتطبيقات العلامات المائية منها لعمليات الاخفاء بهدف تبادل المعلومات السرية.

الكلمات المفتاحية: العلامات المائية ,حماية حقوق الطبع, احكام الملكية, التشفير, اخفاء المعلومات

Chapter one

Introduction

1.1 Introduction

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).

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. This

modified schema relies on a random number generator for the embedding and extracting processes of text watermarks into images that works faster than LSB technique. It relies on pixel replacement presented as noise rather than bits replacement. Moreover, an encryption stage of the text watermark is added before embedding with the intention of thwarting the original owner of the watermarked image.

1.2 History of Watermarking

Although the art of papermaking was invented in China over one thousand years ago, paper watermarks did not appear until about 1282AD, in Italy. The marks were made by adding thin wire patterns to the paper moulds. The paper would be slightly thinner where the wire was and hence more transparent **(**Yusof, and Khalifa, 2007**).**

By the 18th century, watermarks began to be used as anti-counterfeiting measures on money and other documents.

The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term wassermarke **(**Simpson and Weiner, 2000**).**

The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hembrooke for identifying music works. However, it was Komatsu and Tominaga **(**Komatsu, and Tominaga, 1988**),** who appears to be the first to use the term digital watermark. Still, it was probably not until early 1990s that the term digital watermarking really came into vogue.

Around1995, interest in digital watermarking began to mushroom. The first Information Hiding Workshop (IHW),which included Digital Watermarking as one of its primary topics, was held in 1996,**(**Anderson, 1996**)**.

As from1999, the Society of Photo-optical Instrumentation Engineers (SPIE) started devoting a conference specifically to Security and Watermarking of Multimedia Contents **(**Wong and Delp, 1999**)** and **(**Wong and Delp, 2000**)**. In addition, about this time, several organizations began considering watermarking technology for inclusion in various standards. The Copy Protection Technical Working Group (CPTWG) tested watermarking systems for protection of video on DVD disks **(**Bell, 1999**)**. The Secure Digital Music Initiative (SDMI) made watermarking a central component of their system for protecting music. Watermarking is used by the European Union, VIVA and Talisman, for broadcast monitoring **(**Depovere. et.al., 1999**)**.

The International Organization for Standardization (ISO) took an interest in the technology in the context of designing advanced MPEG standards.

In the late 1990s several companies were established to market watermarking products. Technology from the Variance Corporation was adopted into the first phase of SDMI and was used by internet music distributors such as Liquid Audio. In the area of image watermarking, Digimarc bundled its watermark embedders and detectors with Adobe's Photoshop **(**Depovere. et.al., 1999**).**

1.3 Information Hiding, Steganography, and Watermarking

1.3.1 Definitions

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. 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 insures 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 **(**Provos Niels, 2009**).**

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. **(**Niels, 2009**).**

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 **(**Ingemar. et. al., 2008**)**.

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.

1.3.2 How does Steganography and Watermarking Work?

in steganography, let the message M be the data that the sender wishes to keep confidential. It can be plaintext, cipher text, image or anything that need to be embedded into a cover media C, and then stored or sent to a recipient over a communication channel.

A secret password or a key K is selected and used to embed the message M into the cover object using certain algorithm of coding function f(M,C,K) in order to

produce a stego-media Z. This media is sought to be similar to the original media in order not to raise any suspicion, as shown in the block diagram of Figure 1.1.

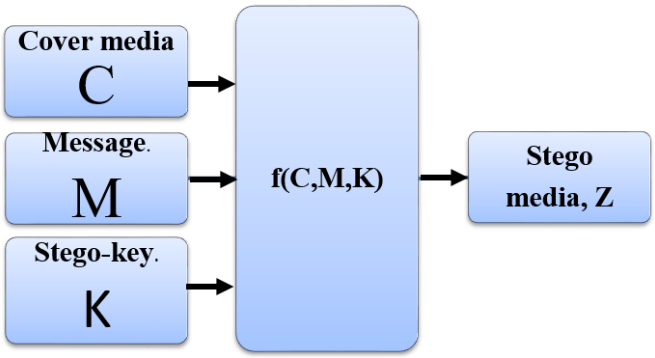


Fig 1.1 Block diagram for steganography embedding process

The secret password K, which is known as stego-key is shared with the recipient ensures that only recipient who knows the corresponding decoding function will be able to extract the message from a cover-media C. Figure 1.2 shows an example of a cover image before and after the embedding process. The embedding process is performed by the function f, which follows an algorithm that plant the contents of M into the content of C with the use of the key K.

Fig 1.2 Cover Image Before and After Message Embedding (Kumar and Gupta,2012)

Watermarking is similar to steganography as shown in a general watermarking process diagram illustrated in Figure 1.3. Digital Watermark is embedded in the original

media using a certain key through an embedding algorithm in order to produce the watermarked media. There are few differences between the two hiding techniques as will be seen in the next section.

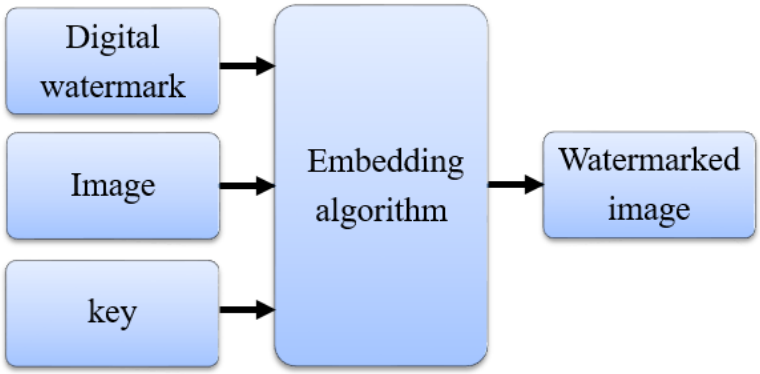


Fig 1.3 Block diagram of the watermarking process

It must be stated that the extraction process of the secret message from the stego-media and the watermark from the watermarked media are the exact inverse of the embedding processes shown in Figure 1.1 and Figure 1.3, respectively.

1.3.3 Steganography vs. Digital Watermarking

In order to outline the differences between steganography and digital watermarking techniques, their various features are summarized in Table 1.1 (Chen and Shen, 2009).

Table 1.1 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
Steganographic communication are 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.

1.3.4 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 1.4.

Information hiding covers covert channels, anonymity, steganography, and copyright watermarking techniques. Detailed definitions and descriptions of all these terms can be found in **(**Petitcolas and Fabien, 2002**)**. However, the work in this thesis will be confined to the field of watermarking and steganography, which are defined in section 1.3.1.

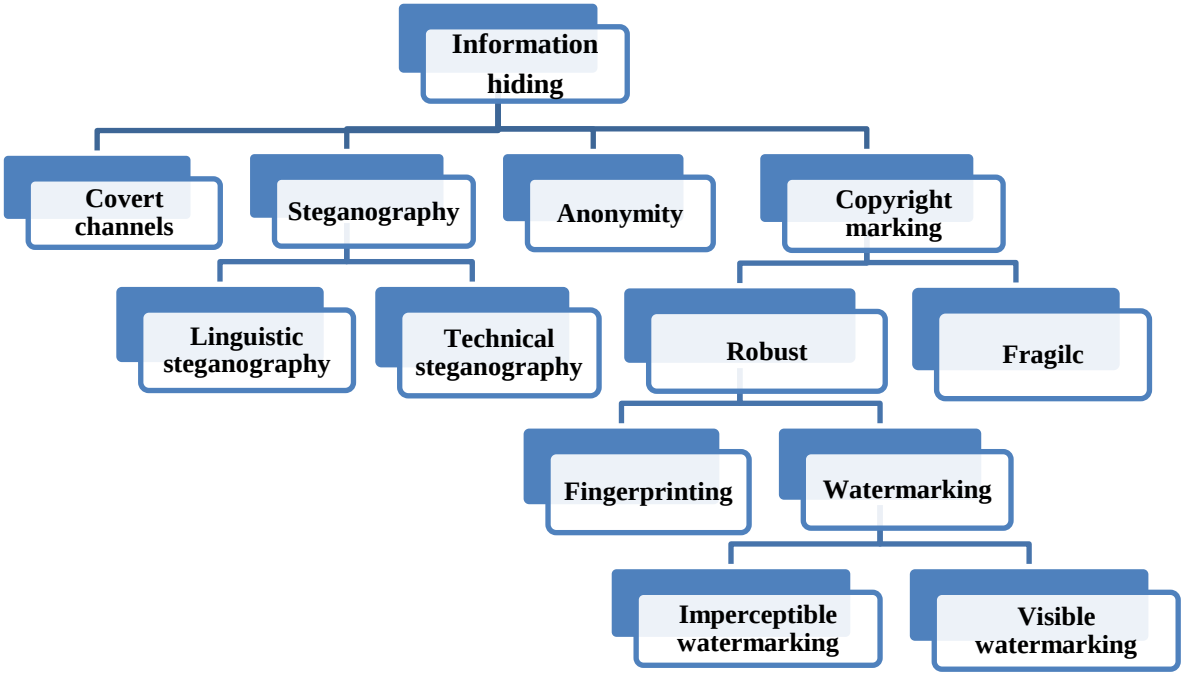


Fig 1.4 : A classification of Information-Hiding Techniques (Petitcolas, Anderson and Kuhn, 1999).

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). The following lists a brief description of these two types **(**Petitcolas and Fabien, 2002**)**.

Time Domain: This type of data hiding is related to the replacement (or modification) of image content itself with minimum noticeable effect. An example of this type is the Least Significant Bit (LSB) technique. LSB is the technique that works by replacing some of the information in particular pixels with the information from the data in the image. LSB is performed by modulating the slightly less significant bit(s). However, this modulation reduces the contrast in colors or intensity of the image. Due to the changes in the LSB bits (Yousof, and Khalifa, 2007). The work in this thesis is concerned with this domain but differs from LSB technique by replacing pixels in the cover image as noise rather than bits..

Frequency Domain: In this type of data hiding the carrier multimedia is converted into another form and then modified according to the data to be hidden. This type includes many techniques, such as Discrete Wavelet Transform (DWT) (Provos and Niels, 2009), Discrete Cosine Transform (DCT).(Malik, Khokhar and Ansari, 2004), Singular Value Decomposition (SVD) (Muntean, Grivel, and Najim, 2002) , and Discrete Fourier Transform (DFT).

1.4 Importance of Digital Watermarking

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 with the introduction of Marc Andreessen's Mosaic web browser in November 1993 **(**Bors and Pitas, 1996**)**, 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 (for example large Hollywood studios and music labels) also see a high risk of piracy **(**Bors and Pitas, 1996**)**. 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.

1.5 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 (Sun Y. et.al, 2015). This problem have 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. Vast number of digital image watermarking schemes were developed with different levels of

imperceptibility, content authentication, and security. For example, spatial domain schemes are fast and simple but have good imperceptibility, on the other hand transformation domain schemes are complicated but give better robustness. Hence, more research interest in developing watermarking systems that have better performance is needed. The aim of this thesis is to develop and test a watermarking technique that is fast and secure. A preprocess of text encryption is performed using matrix manipulation method before embedding the watermark in order to achieve content authentication and then randomly embedding the encrypted text pixels into digital image that is intended to be protected. Hence, multiple hiding technique is adopted in order to produce a high level of imperceptibility and content authentication. The resulting scheme will be tested for various environmental disturbances such as compression, addition of noise, filtering, rotation, etc.

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

1- Does impressibility increase if watermark content authentication or text encryption is implemented before embedding? and what is the improvement obtained?
2- What would be the improvements in the embedding and extraction speed when the random pixel replacement method implemented?
3- What would be the effectiveness of the environment effects such as noise and deformation on the watermark?
4- What is the effect of different noise and external factors on the thesis embedding technique ?And what is its added value?
5- What are the main enhancements and weaknesses of the proposed watermarking scheme compared with other spatial schemes, such as LSB

technique in terms of efficiency and security? And what are the most important suggestions that we may recommend?

1.6 Objective of the Study

The objective of the study in this thesis can be summarized as follows:

1- Establishing a fast text watermark embedding scheme as notes or signature to be used for protecting the property rights and support ownership judgment of images or paintings using spatial domain watermarking.

2- Comparing the proposed watermarking scheme results with the traditional spatial domain techniques such as LSB in order to determine its feasibility and efficiency.

3. Testing the resulting proposed scheme under various environmental disturbances and the effects of noise addition, filtering, rotation, skewing, etc.

1.7 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 main significance of the proposed watermarking scheme is to decrease embedding and extracting processes time, and at the same time look for increase imperceptibility and robustness of watermarking technique using a spatial domain which is less complex than other techniques. The short text information or signature are to be encrypted first for content authentication purposes, then it is randomly embedded as noise into the images. The proposed system

introduces an improved approach to protect the image for the purposes of copyright, ownership and intellectual property.

1.8 Scope and Limitations

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 still images, and will be involved with spatial domain. I will also cover some kind of encryption to the text information which is intended to be embedded in the images. Some limitations are expected when different image formats are involved, hence this thesis will also be limited to bitmap (bmp) digital color images.

1.9 Organization of Thesis

The thesis contains five chapters. They are organized as follows:

- Chapter One: It include an introduction, Information Hiding, History of Watermarking, How does Steganography and Watermarking work, the problem statement, objective of the study in the thesis, motivation and the scope and limitations.

- Chapter Two: It includes digital watermarking classification, properties, application, attacks, image processing techniques, image watermarking techniques, evaluation of image quality, properties and techniques used for watermarking, and literature review.

- Chapter Three: This chapter considers many algorithms to design the thesis. Component (RGB) values, The thesis method and The matrix cryptographic method,

- Chapter Four: It presents the implementation and results.

- Chapter Five: It presents conclusions and suggestions for future works.

Chapter Two

Theoretical Background and Literature Review

2.1Overview

This Chapter covers the theoretical background of watermarking techniques in general and the related work. It includes digital watermarks calcification, properties, and application of watermarking first, then describes important watermarking techniques, and attacks. As the research work in this thesis will be compared with LSB technique for image watermarking, a brief explanation of LSB is included, too. Finally, a literature survey of the related works is included.

2.2 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 intended for, that includes copyright protection, multi-media authenticity, and ownership proof, preventing misuse of sensitive information, and hiding crime traces (Al-Rashied, 2006).

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:

- According to host type: The watermarked multimedia host can be text, still 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 (Kumar, 2008). Watermarking of the still 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 (Hyoung, 2004).

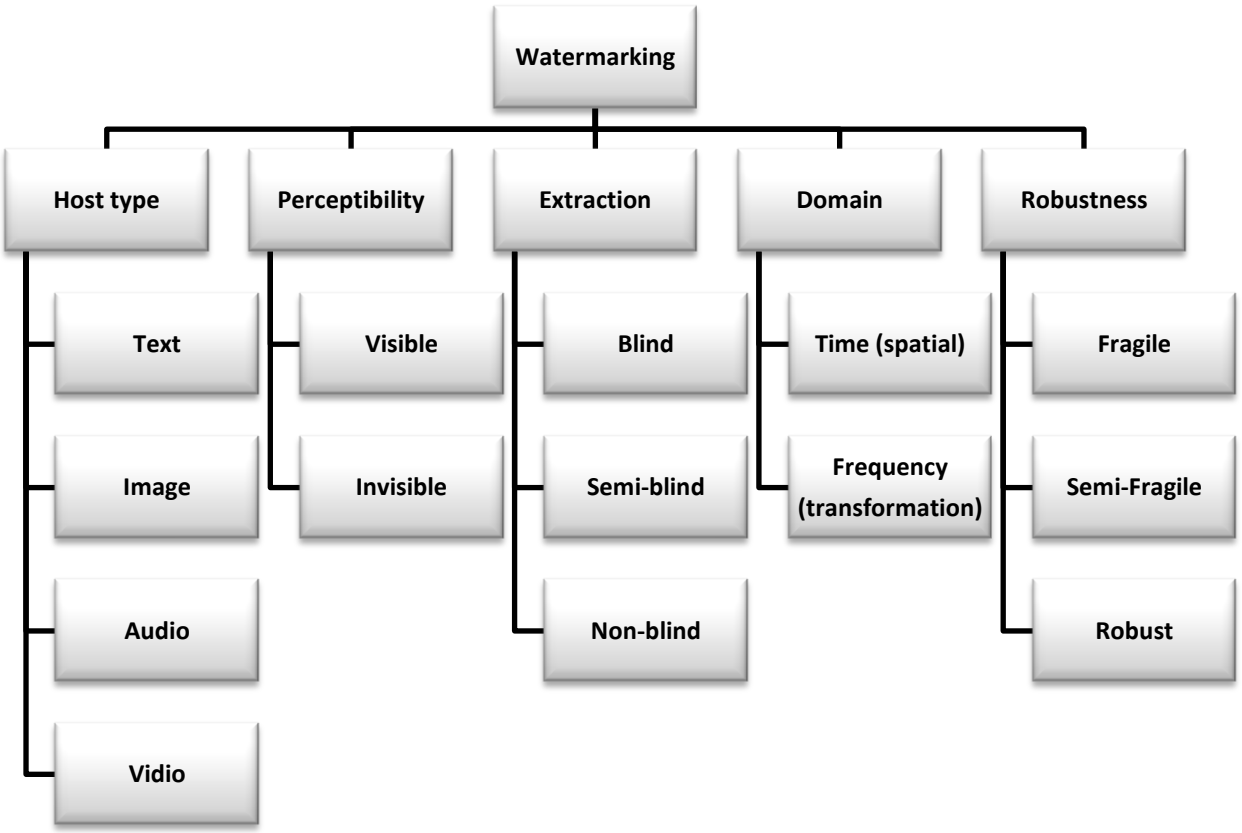


Fig 2.1: Watermarks Classification

- ***According to the watermark type*:** 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. publically 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.

- ***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 (Qasim, 2005). 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.

- ***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 (Prasad, 1999). 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.

- ***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 (Jonathan, Hartung and Girod, 1999), they are commonly used and acceptable.

2.3 Watermarking Properties

Properties of digital watermarking (or expected requirements) include imperceptibility, robustness, security, tamper resistance, embedding effectiveness, fidelity, data payload, blind or informed detection, False Positive Rate, embedding and retrieval process, cost of watermark. One of the challenges for researchers in the watermarking field is that these requirements compete with each other (Emek, & Pazarci, 2005). In the following, these requirements are briefly defined

- ***Imperceptibility*****:** An embedded watermark is truly imperceptible if a user cannot distinguish the original multimedia from its watermarked version.

- ***Robustness:*** Robustness means that it should not be possible to remove or alter the watermark without sufficient degradation of the perceptual quality of the host multimedia.

-***Security:*** Security of watermark means how safe is the watermark and cover multimedia against unauthorized users. According to Kirchhoff's assumption, the security of the encryption techniques must lie in the choice of key. This assumption is also valid for watermark techniques (Ingemar, 2000).

- ***Tamper Resistance:*** Tamper resistance refers to watermarking system’s resistance to hostile attacks. There are several types of tamper resistance depending on

the application. Certain types of attacks are more important than others, in fact there are several applications in which the watermark has no hostile enemies, and tamper resistance is irrelevant.

- ***Embedding Effectiveness:*** Watermarking requires that when a watermarked multimedia is input to a detector, it results into a positive detection. With this definition of watermarking, the effectiveness of a watermarking system is the probability that the output of the embedding algorithm will be watermarked multimedia (AL-Rashied, 2006).

-***Fidelity:*** The fidelity of a watermarking system refers to the perceptual similarity between the original and watermarked versions of the cover multimedia (Ingemar, 2000).

- ***Data Payload:*** Data payload refers to the number of bits a watermark encodes within a unit of time or within a multimedia.

-***Blind or Informed Detection:*** In some applications, the original, un-watermarked multimedia must be available during detection (or extraction). For example, in a transaction-tracking application, it is usually the owner of the original multimedia who runs the extraction in order to discover who illegally distributed a given copy. The owner, of course, should still have an un-watermarked version of the multimedia and can thus provide it to the extractor along with the illegal copy (Ingemar, 2000).

-***False Positive Rate:*** A false positive is a detection of a watermark in a piece of multimedia that does not actually contain that watermark. When one talks of the false positive rate, he/she refers to the number of false positives expected to occur in a given number of runs of the extractor.

- ***Cost of Watermark:*** The economics of deploying watermark embedders and extractors can be extremely complicated and depend on the business models involved. From a technical point of view, the two principal issues of concern are the speed with which embedding and extraction must be performed and the number of embedders and extractors that must be deployed.

2.4 Watermarking Applications

Watermarking methods are often evaluated based on common properties of robustness, imperceptibility, and security. However, focusing solely on compliance of these properties, without careful consideration of the intended application is often misleading. For examples, a watermark designed to serve ownership proof must be meeting different requirements than the one designed for copy control. Thus, it is inappropriate to evaluate these watermarking properties without considering their application domain and use. This section describes most applications of watermarking, such as authentication, copyright protection, copy control, fingerprinting, broadcast monitoring, covert communication, and others (Bouhlel, Trlchlll, Derbel and EamoNn, 2002).

- **Broadcast Monitoring*:*** Watermarking can be used for broadcast monitoring which refers to verifying whether the content that supposed to be broadcasted (on TV or Radio) has really been broadcasted or not (Bender et al, 2000).

- **Owner Identification*:*** A digital watermark can be used to provide complementary copyright marking functionality because it becomes an integral part of the content, for example, the copyright information is embedded in the music to supplement the text notice printed on the packaging (Ingemar, Miller and Bloom, 2001).

The Digimarc Corporation has marketed a watermarking system designed for this application. Their watermark embedders and detectors are bundled with Adobe's popular image processing program, i.e. Photoshop. When a detector finds a watermark, it contacts a central database to identify the watermark's owner (who must have paid the correct fee in order to keep the information in the database).

- **Tamper Proofing:** It helps to prevent unauthorized modifications to watermarked contents. If an attacker attempts to tamper with the watermarked contents, the watermark also gets modified. The major goal of tamper proofing is to detect alterations made in the watermarked contents and to make the contents useless if the attacker tampers with it. Tamper proofing is considered as a challenging domain in digital watermarking community.

- **Authentication (content verification*):*** The content of digital image/audio/video can easily be modified so that it is very difficult to detect what has changed. In the case of sensitive legal documents and medical images, this becomes increasingly important in order to verify the authenticity of original content. For authentication, a watermark is embedded into the original content which is used to evaluate the strength of such content. If the content is altered by an attacker maliciously, the watermark gets changed and therefore the content will be considered non-genuine. Watermark in this case is considered less robust or fragile (Thapa and Sharma, 2011).

- **Transactional Watermarks (Fingerprinting):** Associating unique information about each distributed copy of digital content is called fingerprinting. Watermarking is an appropriate solution for fingerprinting application because it can be invisible and inseparable from the content. This type of application is useful for monitoring or tracing illegally produced copies of digital work.

- **Copyright Protection***:* Copyright protection is considered as the most important application of digital watermarking. For copyright protection of digital content, copyright information, such as signature, copyright message, or logo image are inserted or embedded in digital content to be protected. The embedding algorithm incorporates copyright message which can then be extracted by the extraction algorithm in order to prove ownership.

Although copyright notice does not guarantee the protection of copyright but still it is used. Generally, books, images, audio, and videos contain copyright notices, sometimes visible and sometimes invisible. It is necessary to achieve very high level of robustness when embedding watermark for copyright protection. Attackers can remove the copyright information through intelligent manipulation of the contents such as image cropping, segmentation of videos, modifications in audio, and rephrasing the text. Hence, it is necessary to embed copyright information in each and every piece of copyrighted material or multimedia. (Bender, Butera, Gruhl, Hwang, Paiz, and Pogreb, 2000).

- **Copy Control*:*** Copy control falls into a broader category of applications, which we refer to as device control. There are several other applications in which devices react to watermarks they detect in content.

- **Medical Application*:*** For security reasons of the patient, digital watermarks can also create hidden labels and annotations in medical applications, and for multimedia indexing and content-based retrieval applications. In the medical application, watermarks might be used for identifying patient records, as well as the physician and the medical asset.

In addition to the application areas mentioned above, there are some other application areas of watermarking, such as access control, traitor tracing, transaction tracking, etc.

2.5 Digital Watermarking Attacks

Watermarking techniques should be tamper resistant to hostile attacks. Depending on the application, the watermarked content encounters certain types of attacks. In the following, a definition of some basic types of attacks are briefly explained.

- **Active Attacks***:* 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 (Cox and Linnartz, 1998).

- **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. Most of the scenarios above are not concerned with this type of attack. In fact, one might even advertise the presence of the mark so that it can serve as a deterrent. But for covert communication, our primary interest is to prevent the watermark from being observed. (Craver, Memon, Yeo, and Yeung, 1998).

- **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 (Cox, Kilian, Leighton, and Shamoon, 1997).

- **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.

- **Fragility:** 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. (Craver, Memon, Yeo and Yeung, 1998)

2.6 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 the mean square error (MSE) and the peak -signal-to-noise ratio (PSNR) are defined.

2.6.1 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 2.2, 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 r referred to as RGB.

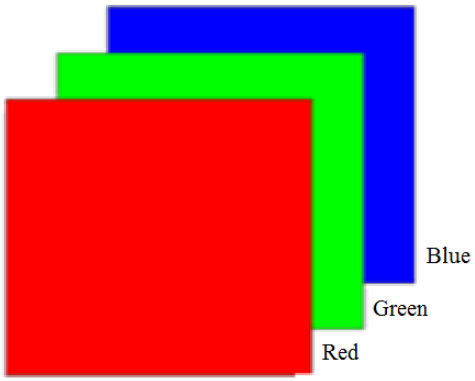


Fig 2.2 Digital Color Image Channels

Digital color image can be manipulated as a 3 separate pixel arrays of similar dimensions as shown in Figure 2.3. Each color component pixel is represented by 8 bits, therefore each image pixel consists of 24 bits length. Where $I_R(u,v)$, $I_G(u,v)$, and $I_B(u,v)$ are the intensity of the red, green, and blue pixel at the point with (u,v) coordinate, respectively.

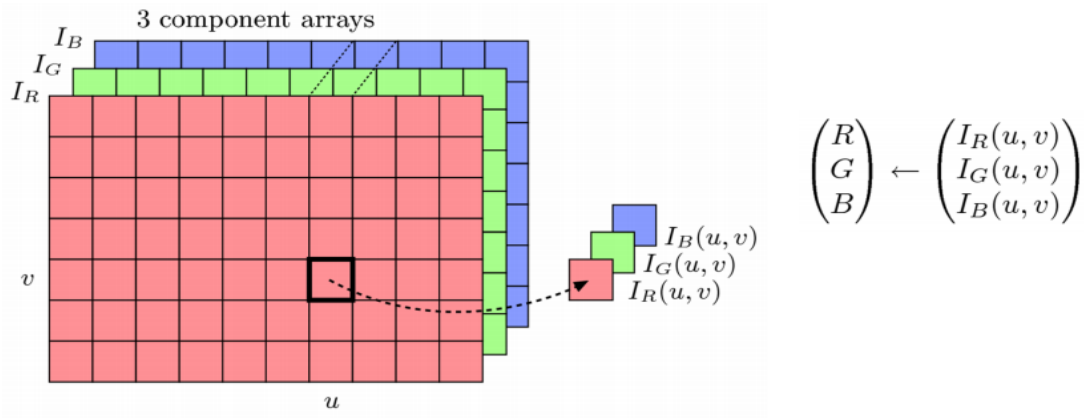


Fig 2.3: Color Image as a 3 Arrays

The RGB component intensity values representing pixel's colors are packed together into single element as shown in Figure 2.4. However for gray images only one array of pixels represents the image pixels intensities (each of 8 bits length) are used.

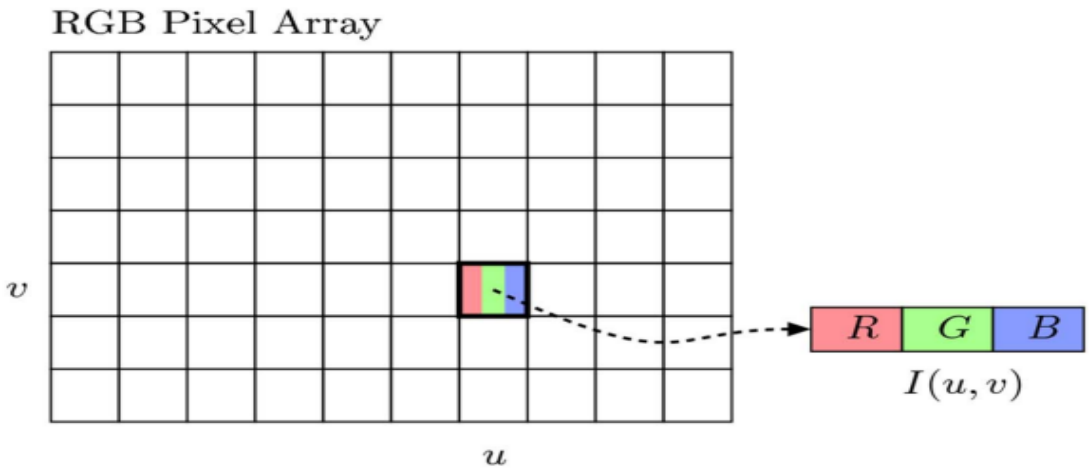


Fig 2.4 RGB Component intensity values

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.

2.6.2 Color image processing techniques

Three type of color processing techniques were considered and studied in this thesis first in order to select the fastest one to be adopted in the proposed embedding algorithm. They are briefly outlined in the following:

1. **Separate color channels:**

The RGB color image components are separated into three channels, then each channel. Each of the three color components (i.e. R, G, and B) is handled or treated separately,

then they are recombined together in order to produce the resulting processed color image, as illustrated in Figure 2.5 (Gonzalez and Woods, 2002).

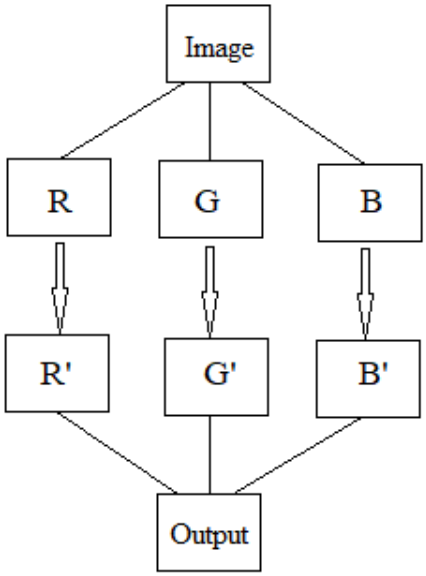


Fig 2.5: Separating color image to 3 Arrays (Ramos and Rezaei, 2010).

2. Direct conversion to gray color:

The RGB color image is converted directly to gray image first, then the gray image is handled for any purpose such as embedding, and then it is converted back to color image. The direct conversion method to gray color adopts the conversion to three components; two of them for chrominance (Rd and Gd) and one for intensity (I),(Chowdhury, Banerjee and Bhattacharjee, 2010) and are given by equation 2.1 below.

$$Rd = (R*256) / (R+G+B)$$

$$Gd = (G*256) / (R+G+B) \quad . \ . \ . \ . \ . \quad (2.1)$$

$$I = (R+G+B) / 3$$

Then after handling or treating these components, the invers conversions is performed to recover the color image (RI,GI, and BI), as given by equation 2.2 below.

$$RI = (3*Rd*I) / 256$$
$$GI = (3*Gd*I) / 256 \quad \ldots\ldots (2.2)$$
$$BI = (3*(256-Rd-Gd)*I) / 256$$

3. YIQ Model:

Deferent methods are now available to convert color image to gray and vise versa such as **YUV**, YIQ conversions, (for more details, see Al-Dwairi, Alqadi, AbuJazar and Abu Zneit, 2010). In these models, color information is separated from brightness information. YIQ model is mainly used in North American television systems and it is slightly different version of YUV. Y is the luminance component while I and Q consist of the color information (chrominance). YIQ model has the following advantages over RGB.

- The brightness information is separated from the color information.
- The correlations between the color components are reduced.
- Most of the information is collected to the Y component, while the information content in I and Q is less.

YIQ will considered in this thesis, and the conversion from RGB is achieved using equation 2.3.

$$Y = 0.299.\ R + 0.587.\ G + 0.114.\ B$$
$$I = 0.596.\ R-0.275.\ G-0.321.\ B \quad \ldots\ldots (2.3)$$
$$Q= 0.212.\ R-0.523.\ G + 0.311.\ B$$

Converting an RGB color image to YIQ color model and back to RGB is shown diagrammatically in Figure 2.6. Therefore embedding can be done after the conversion to gray, then convert back to color image.

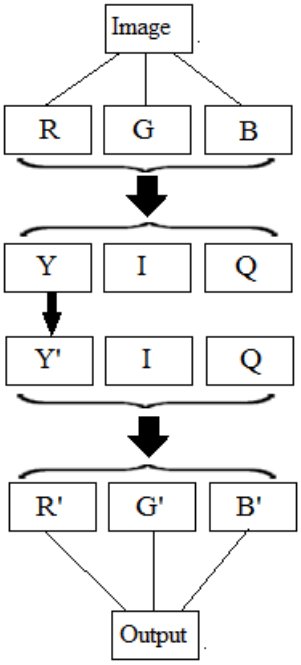


Fig 2.6: Image conversion between RGB and YIQ (Naik and Murthy, 2003)

It was shown in **(**Al-Dwairi, 2010**)** that the direct and inverse conversions require a minimum time of conversion. This method of conversion will be used in the proposed methodology of data hiding.

2.6.3 Spatial Domain Techniques

This watermark technique is based on insertion of watermark data directly into pixels of a host image. This approach produces minor changes in the pixel intensity value, which are supposed to be imperceptible. The simplest example of the previous technique is to embed the watermark bits in the least significant bits (LSB) of image pixels. In other words, 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. (Abbasfard, M. 2009) It should be noted that the research work in this thesis will be involved in the development of an improved embedding scheme in spatial domain for embedding text data into images. 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 less robust against the attacks.

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:

- **Least-Significant Bit (LSB)**

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Each image consist 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:

(10100001 10001000 00110011)
(01011111 11001111 11110000)
(10101101 10101010 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. (Abbasfard, M. 2009)

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

- **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.

2.6.4 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), 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 (Johnson, Duric and Jojodia, 2000).

2.6.5 Metrics for Evaluating Image Quality

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 Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio(PSNR) (Forouzan, 2011).They are defined in the following:

- **The Mean-Squared Error**

The mean squared error (MSE) between two images $\mathbf{I_1}$(m, n) and $\mathbf{I_2}$(m, n) can be calculated by equation 2.1.

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad . \ . \ . \ . \ . \ . \ . \ (2.1)$$

where M and N are the number of rows and columns in the input image patterns, respectively, $\mathbf{I_1}$(m, n) is the intensity or the value of the pixel located at (m, n) position in the watermarked image and $\mathbf{I_2}$(m, n) is intensity of the corresponding pixel in the original image. The mean-squared error depends strongly on the image intensity scaling.

- **Peak Signal-to-Noise Ratio**

The Peak Signal-to-Noise Ratio (PSNR) is the most widely used metrics. It avoids the problem of image intensity by scaling the MSE according to the image range, and it is given by equation 2.2.

$$\text{PSNR} = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad . \ . \ . \ . \ . \ . \ . \ (2.2)$$

Where R is the maximum possible pixel value of the image, which is for gray scale image = 256.

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 (Forouzan, 2011).

2.7 Literature Review

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 their study (Hossain M., S. Al Haque, and F. Sharmin, 2010) examined three important methods related for hiding digital data, depending on the psycho visual repetition in digital images of grey scale, using the neighbourhood information. Their importance arises from the ability to know exactly the data included within the image input pixel, without making differences. The neighbourhood 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 (Al-Dwairi, Alqadi, AbuJazar, and Abu Zneit, 2010), 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.

(Bamatraf, Ibrahim, and Salah, 2010) 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 (Dasgupta, Mandal, and Dutta, 2012). 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 (Sruthi, N., Sheetal, and et.al, 2014), 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 (Ghosh, Maity, and Rahaman, 2015). It achieved more advanced and valid level of imperceptibility through the exploitation of the couple purpose robust algorithm, concerning image cryptography and digital watermarking.

(Kumar & Dutta, 2016) 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 a 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.

(Mathur, Dhingra, Prabukumar, Agilandeeswari, and Muralibabu, 2016) 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.

The research in this thesis concentrates on gaining good performance for text watermarking into still images. This will be achieved by suggesting an algorithm that depends on the random determination of host image locations and performing the embedding of the text watermark in these locations as noise rather than as bits in the

pixels as the case of LSB. The proposed algorithm will tested and compared with the traditional LSB technique for embedding and extraction speed of text messages.

Chapter Three

The Text Watermarking Algorithm

3.1 Overview

This chapter presents the proposed watermarking algorithm for hiding text information (watermark) into the host color images that is to be copyright protected and ownership proof. The embedding and extraction phases of this algorithm will be outline first, then the adopted color image processing model and vectorization process are described. Furthermore, the adopted method for encrypting and decrypting the text watermark is explained at the end of the chapter.

3.2 The Proposed Method.

The proposed watermarking algorithm in this thesis adopt the embedding of text watermarks or signatures information into still color images. The watermarking process is performed into the host images as noise insertion after they have been converted to grey scale in YIQ format, then the watermarked images are converted back to RGB. The YIQ format is chosen for the embedding process as it is found to give the shorter processing time in comparison with the separate color channels and the direct conversion method outlined in chapter 2. The embedding of water mark as noise into the images is adopted due to the fact that text watermarks are usually short messages and hence, their existence in color images, which are normally much greater in size, is tolerated and the hardly noticed. To increase the owner authenticity, an extra stage may be added to the watermarking by encrypting the text watermark using any encryption technique. In this thesis, matrix manipulation method is suggested (analogous to Hill cipher technique) to use optionally if watermark encryption is required, as will be outlined later in this chapter.

In the following a detailed description of the proposed watermarking algorithm. It consists of two phases; embedding phase and extraction (or detection phase) as

outlined in the following subsections, and their flow charts are illustrated in Figure 3.1 and Figure 3.2, respectively.

3.2.1 Watermark embedding

The embedding process starts by inputting the color image that need to be protected (host), then input the text watermark, vectorize and find the size of both the watermark and the image. Generate random position matrix to be used as the secret key (SK). Use this secret key for embedding the watermark data into the vectorized image as noise. The resulting watermarked image is a noisy image. The embedding process is explained in the following steps as illustrated in Figure 3.1.

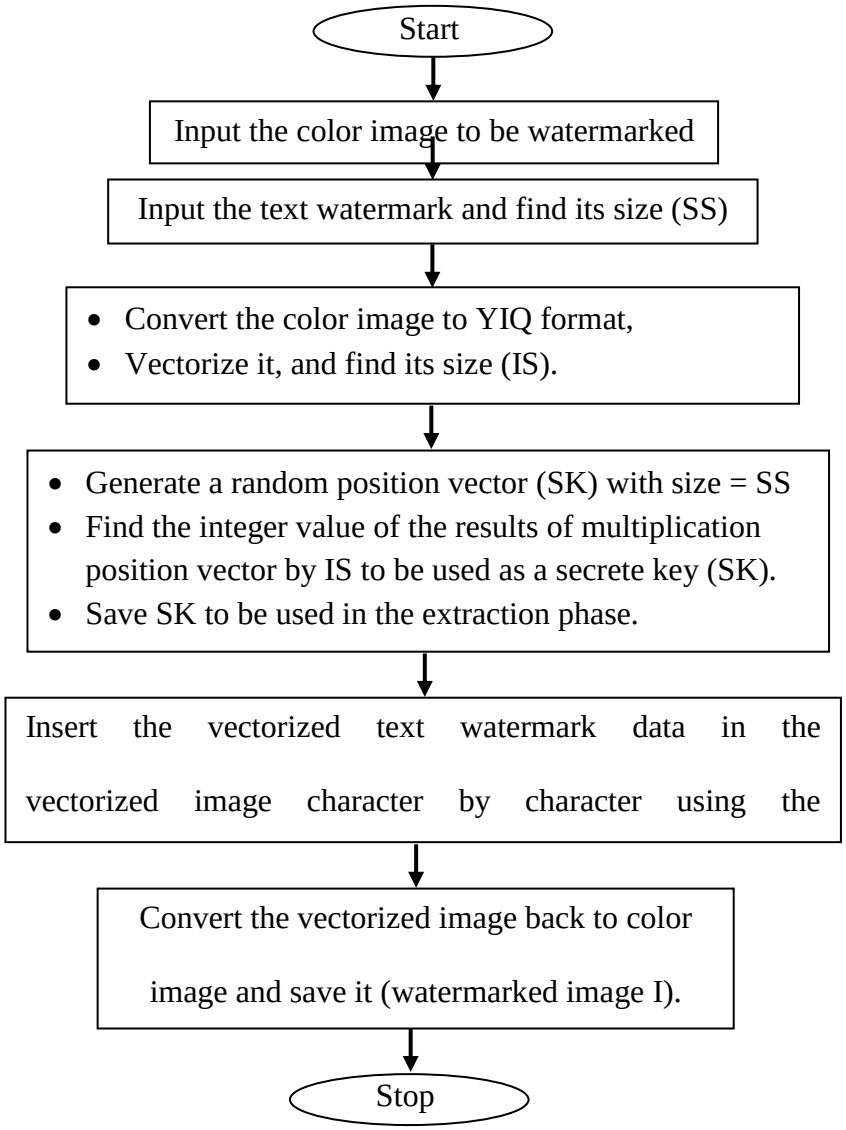


Fig 3.1: Flow chart of the embedding process

To hide the text watermark into an image using the proposed algorithm, the following steps are applied:

1. Get the host image: Input the original host image which is to be watermarked. This image can be gray image or color image (in this thesis, RGB color images are chosen in order to have a source image with large sizes and high resolution).

Let the input RGB image be of ***r*c*** size, where ***r*** is the number of rows and ***c*** is the number of columns. Hence it can be represented by three ***r*c*** arrays of 8-bits pixels, i.e. one array for each color component, Red, Green, and Blue. Therefore the total size of the image array equals: **IS = 3 * *r* * *c***

2. Get the watermark: Input the watermark data, which is a text data of any number of characters (referred to as watermark key size, KS) in the form of ASCII code, and arrange them a vector, whose elements are the binary representations of the characters.
3. Process the host image: The RGB image array values obtained in step 1, which consists of three matrices, each having a size of ***r * c*** pixels is converted into three matrices in YIQ format as explained in chapter 2. These three matrices are vectorized, i.e. rearrange into one vector or one dimensional array having a size of 3* ***r * c*** elements, which is the same as IS, ready to be used for watermark embedding. The vectorization process means converting 3 matrices into one vector as explained in the next section.
4. Key generation: Randomly generate a vector of size equal to the number of characters in the text watermark (KS) and values in the range 0 to 1. The elements values in the random position vector are be obtained by taking the integer value of the result of multiplication of the random value by the size of the image vector, hence resulting into position values in the range from 1 to IS. Therefore, this generated key vector is to be used for hiding the text watermark and it must be privately saved to be used for the extraction process. [Note: It must be noted that the same key is save and used with LSB method, for the purpose of comparison that is reported in chapter 4].

5. The insertion step: Successively use the elements of the generated key of step 4 to locate elements of the host image vector of step 3, and replace them by the watermark vector elements of step 2, such that the 1st watermark element value replaces the value of the position determined by the 1st key element, the 2nd watermark element value replaces the value of the position determined by the 2nd key element, etc. message into the image vector using the generated secrete key.
6. Rearranging the resulting watermarked image vector in order to get the in YIQ format, then converting it back to RGB produces the final watermarked color image.

   The watermarked image may be referred to as the noisy image (NI) due to the fact that the embedded text watermark can be considered just like noise. The proposed embedding process of text or signature watermark hiding is highly secure due to the difficulty of guessing the key by unauthorized user, as will be explained later.
7. Optional: To increase the difficulty for hacker or thieves, and thwarting them from knowing the original owner of the protected image with a watermark, an encryption stage is added before the insertion step (step 4 above). This measure increases the watermark authenticity by hiding the identity of the image owner. The text watermark can be encrypted using any encryption technique before it is inserted into the image. In this thesis, a matric manipulation process is adopted, as described later in this chapter.

3.2.2 Watermark extraction

To detect the hidden watermark in the watermarked image, the watermarking extraction or process is performed. It is exactly the inverse of the watermark embedding

process. The extraction algorithm starts by accepting the watermarked image, convert it to YIQ format, vectorize it, then use the same key that is randomly generated and used for the embedding process (SK) to retrieve the watermark text from the vectorized image watermark. The extraction process is briefly explained in the following steps as illustrated in Figure 3.2.

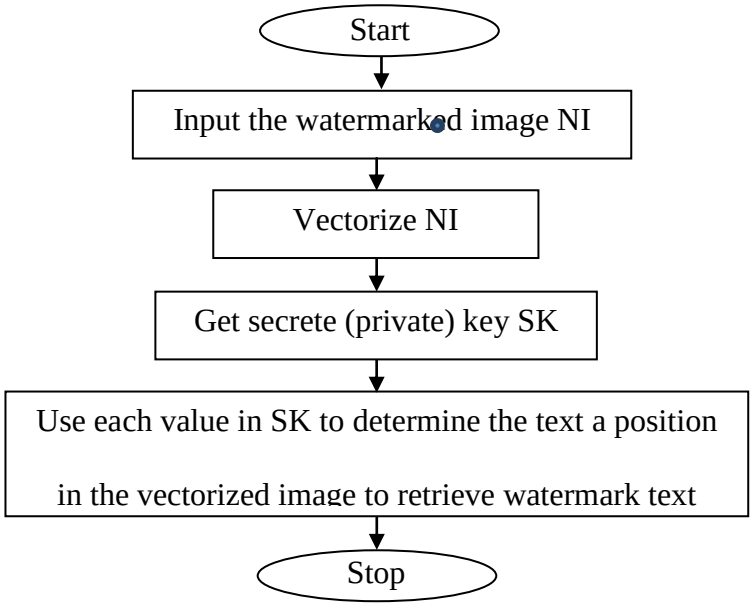


Fig 3.2 Flow Chart of the Extracting Process.

The extracting process of the proposed algorithm can be implemented applying the following steps:

1- Get the watermarked color image (NI) and convert it into YIQ format.

2- Vectorize the obtained image by changing it from three matrices with ***r*c*** pixels size to one vector with 3****r*c*** elements.

3- Get the secrete key which used for the embedding process and use it to retrieve the embedded data from the vectorized image, which is the text watermark.

However, if the optional encryption stage was included in the embedding process, then the next step performed.

4- Optional: If the text watermark was encrypted during the embedding process, then to recover the plaintext watermark, a decryption stage is performed on the obtained output in step 3 above.

3.3 Vectorization Process

The vectorization process means converting many matrices into one vector matrix. Hence, vectorization of the three matrices representing the pixel values for RGB components of the color image means rearranging these elements into one image vector. This is achieved by successively writing the columns elements after each other for the first followed by the columns elements of the second matrix, then followed by the columns elements of the third matrix.

To illustrate the vecorization process of three matrices, a simple example is shown in Figure 3.3. Each matrix consists of 3x3 elements. The vectorization process results into a vector consisting of 3x3x3 elements.

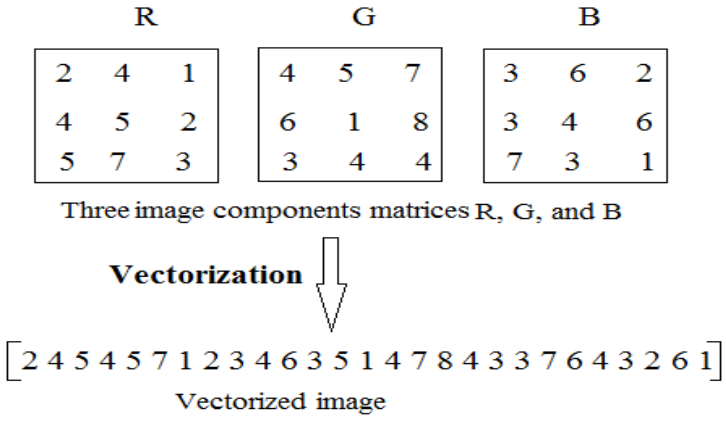


Fig. 3.3 Simple example of vectorization process

3.4 The Matrix Cryptographic Method.

To increase the secrecy of embedded text watermark, it is recommended that it is encrypted. This section suggests an encryption method that relay on matrix manipulation, which is similar to Hill cipher. It can be summarized as follows.

Consider a text watermark of size W characters. The watermark text characters are converted to decimal values using the ASCII code table. These decimal values of the resulting watermark text decimal are vectorized into vectors, each of dimension N. [note: if there is a shortage in the last vector, it is filled with spaces]. Then an N*N matrix is chosen randomly to be used as an encryption key [**K]**. The text encryption/decryption processes can be summarized as follows.

The original text or signature watermark after vectorization is [**W**], the two dimensional square matrix which is to be used as a private key [**K**], the inverse of the key matrix is [$\mathbf{K^{-1}}$] let the encrypted text be [$\mathbf{E_t}$], and the decrypted text be [$\mathbf{D_t}$], then mathematically the encryption and decryption processes can be expressed as below:

The encrypted watermark is: $\mathbf{[E_t] = [K] * [W]}$ . . . . . (1)

And the decrypted watermark is: $\mathbf{[D_t] = [K^{-1}] * [E_t]}$ . . . . . (2)

Now substituting equation 1 into equation 2, gives

$$\mathbf{[D_t] = [K^{-1}] * [K] * [W] = [W]} \quad . \ . \ . \ . \ . \ (3)$$

Which means that decrypted text watermark is the same as original text.

The above method of encryption/decryption using the matrix technique can be clarified as in the following example.

Example. Let the message be W = "NASER AKRAM NASER", and the encoding matrix or the encryption key [**K**] be

$$\mathbf{[K]} = \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix} \quad . \ . \ . \ . \ . \ (4)$$

Using the number representation for each letter of the alphabet. For simplicity, let us associate each letter with its position in the alphabet: A is **1**; **B** is **2**, and so on. Also, assign the number **27** (remember we have only **26** letters in the alphabet) to a space between two words. Thus the watermark text becomes:

N	A	S	E	R	*	A	K	R	A	M	*	N	A	S	E	R
14	1	19	5	18	27	1	11	18	1	13	27	14	1	19	5	18

Since a **3** by **3** matrix is used as the encryption key, the above enumerated watermark is broken into a sequence of **3** by **1** vectors, as follows

$$\mathbf{[W]} = \begin{bmatrix}14\\1\\19\end{bmatrix}\begin{bmatrix}5\\18\\27\end{bmatrix}\begin{bmatrix}1\\11\\18\end{bmatrix}\begin{bmatrix}1\\13\\27\end{bmatrix}\begin{bmatrix}14\\1\\19\end{bmatrix}\begin{bmatrix}5\\18\\27\end{bmatrix} \quad \ldots\ldots (5)$$

Note that it was necessary to add a space at the end of the message to complete the last vector. We now encode the watermark by multiplying each of the above vectors by the encoding matrix according to equation 1. This can be done by writing the above vectors as columns of a matrix and perform the matrix multiplication of that matrix with the encoding matrix as follows:

$$\mathbf{[E_t] = [K] * [W]} = \begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}14 & 5 & 1 & 1 & 14 & 5\\1 & 18 & 11 & 13 & 1 & 18\\19 & 27 & 18 & 27 & 19 & 27\end{bmatrix} \quad \ldots (6)$$

Which produce the following matrix

$$\mathbf{[E_t]} = \begin{bmatrix}-121 & -177 & -108 & -150 & -121 & -177\\20 & 45 & 29 & 40 & 20 & 45\\135 & 182 & 109 & 151 & 135 & 182\end{bmatrix} \quad \ldots\ldots (7)$$

The columns of this matrix give the encoded watermark. The message is transmitted in the following linear form:

$\mathbf{E_t}$ = "-121 20 135 -177 45 182 -108 29 109 -150 40 151 -121 20 135 -177 45 182"

This is the encrypted watermark that will be embedded into the color image.

To decode the ciphered watermark, the receiver writes this string as a sequence of 3 by 1 column matrices and repeats the above technique using the inverse of the encoding matrix, i.e. $[K^{-1}]$. The inverse of this encoding matrix, i.e. the decoding matrix, is:

$$\mathbf{[K^{-1}]} = \begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \quad \ldots\ldots (8)$$

Thus, to decode the message, perform the matrix multiplication

$$\mathbf{[D_t] = [K^{-1}]*[E_t]}$$

$$\mathbf{[D_t]} = \begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -121 & -177 & -108 & -150 & -121 & -177 \\ 1 & 18 & 11 & 13 & 1 & 18 \\ 19 & 27 & 18 & 27 & 19 & 27 \end{bmatrix}$$

Evaluating this matrix multiplication produce the following matrix

$$\mathbf{[W]} = \begin{bmatrix} 14 & 5 & 1 & 1 & 14 & 5 \\ 1 & 18 & 11 & 13 & 1 & 18 \\ 19 & 27 & 18 & 27 & 19 & 27 \end{bmatrix} \quad \ldots\ldots (9)$$

When the columns of this matrix rearranged and written in linear form, then replacing the numerals by the corresponding characters gives the followings

14	1	19	5	18	27	1	11	18	1	13	27	14	1	19	5	1
N	A	S	E	R	*	A	K	R	A	M	*	N	A	S	E	R

Which is the original text watermark.

Chapter Four

Implementation and Results

4.1 Introduction

This chapter includes implementation and testing of the proposed algorithm for text watermarking into color images. The implementation is done using MATLAB codes which run on i7 PC with 4G bytes RAM. It starts with the testing of three image processing types under consideration in order to choose the more suitable method for the hiding method. Then the testing of embedding and extraction processes for speed of processing and the effects of noise and other external disturbances.

4.2 The Image Processing Methods

This section is included to test image processing speed for the three methods described in section 2.6.2, namely; the separate color channels, the direct conversion to gray, and the YIQ model, in order to choose the fastest method to be adopted in the proposed algorithm. MATLAB13a application platform is used as the programming tool.

4.2.1 Processing tests

For each of three methods under consideration, a color image is taken in, separate its RGB components, determine and plot the histogram for each color component, and encrypt the image using the matrix manipulation technique described in section 3.4. Then it is decrypted and plotted together with the histograms for its three R, G, and B color components. The steps for these processes together with the images and histograms are shown in the following.

- ***Method 1 (Separate color channels)***: The three color components R, G, and B are separated first, processed for encryption or decryption, and combined back to produce color image. This method is summarized in the following steps for image encryption:

1- Get the original color image.
2- Retrieve each of the red, green and blue channels.
3- Determine the size of the color channel.
4- For each channel generate a 2 dimensional square matrix key.
5- Apply matrix multiplication encryption for each channel using its key to get the encrypted channel.
6- Combine the three encrypted channels to form the encrypted color image, and plot it.
7- Now to decrypt this image, get its three R`, G`, and B` channel components.
8- Apply matrix multiplication to each channel by using the inverse of its matrix key to get the original color channel.
9- Combine the three decrypted channels to recover the original image.

The image and the components histograms before the encryption and decryption processes and after these processes are shown in Figure 4.1 and Figure 4.2. The processing times of encryption and decryption are determined and will be listed later in this section.

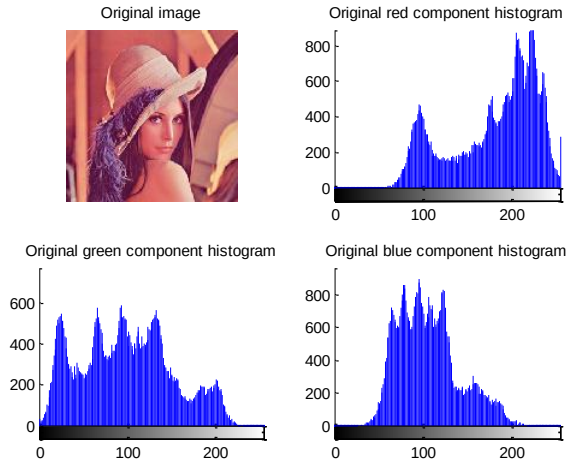


Fig 4.1 Separate color channels original image with R, G, and B histograms

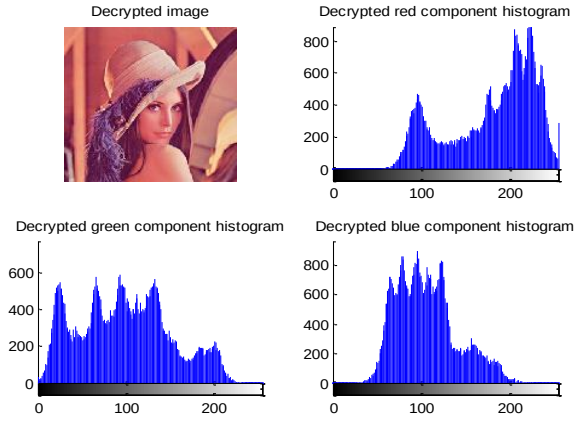


Fig 4.2 Separate color channels - after encryption/decryption processes

- ***Method 2 (Direct conversion to grey image):*** In this method, the color component are modified, processes for encryption or decryption, and then recombined to recover the color image. This method is summarized in the following steps:

  1- Get the original color image, and convert it to gray.

2- Determine the size of the gray image, and generate a 2 dimensional square matrix key.

3- Apply matrix multiplication of gray image and matrix key to get the encrypted gray image.

4- Convert the gray image back to color using inverse conversion.

5- Now to decrypt this image, convert it to gray image.

6- Apply matrix multiplication of grey image and use the inverse of its matrix key to get the original color channel.

7- Convert the decrypted gray image back to color using inverse conversion.

The image and the components histograms before and after the encryption and decryption processes, and the grey image are shown in Figures 4.3 - 4.5. The processing times of encryption and decryption are recorded and will be listed later in this section.

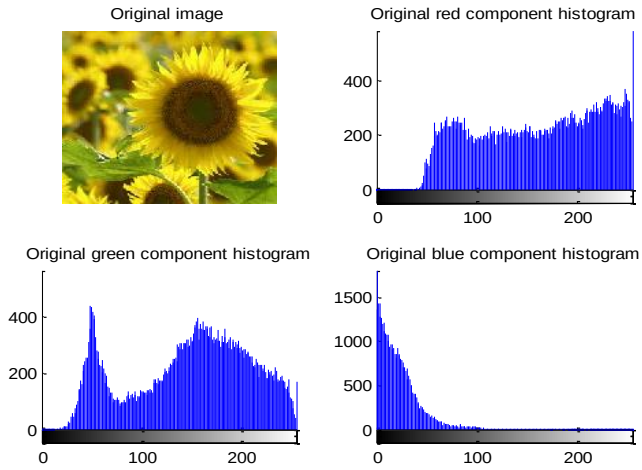


Fig 4.3: Original image for direct conversion to grey with color components histograms

Fig 4.4: Grey image

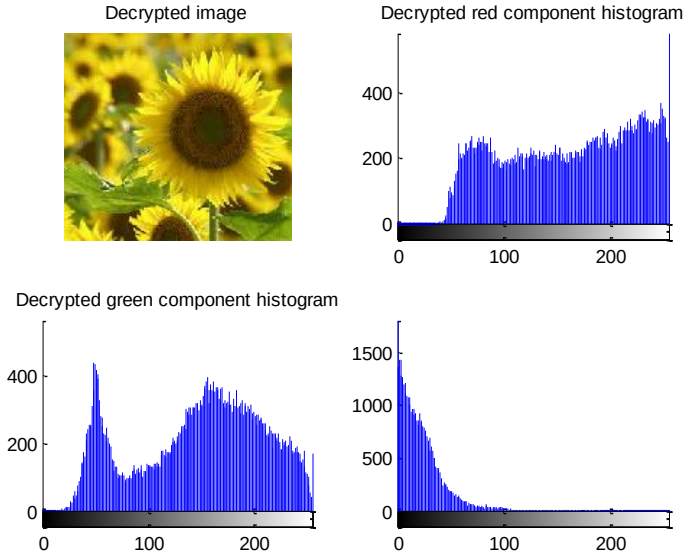


Figure 4.5: Direct conversion to grey image after encryption/decryption processes

- ***Method 3 (YIQ Model):*** In this method, the RGB color component are converted to YIQ components first, processes for encryption or decryption, and then recombined to recover the color image. This method is summarized in the following steps:

  1- Get the RGB color image, get its R, G, and B channels, and determine the YIQ components.

2- Convert from 3D matrix (row, column, 3) to 2D matrix ((row, column)*3).
3- Generate a 2D square matrix key and apply matrix multiplication on the image with the 2D matrix key to get 2D encrypted matrix.
4- Covert the 2D encrypted matrix to 3D encrypted matrix, then convert back to RGB color image.
5- Now to decrypt this image, get its R, G, and B channels, and determine the YIQ components, then convert it from 3D matrix 2D matrix.
6- Apply matrix multiplication on the resulting grey image using the inverse of its matrix key.
7- Convert this decrypted gray image back to color using inverse conversion.

The image and the components histograms before and after the encryption and decryption processes and the grey image are shown in Figures 4.6 - 4.8. The processing times of encryption and decryption are determined and will be listed later in this section.

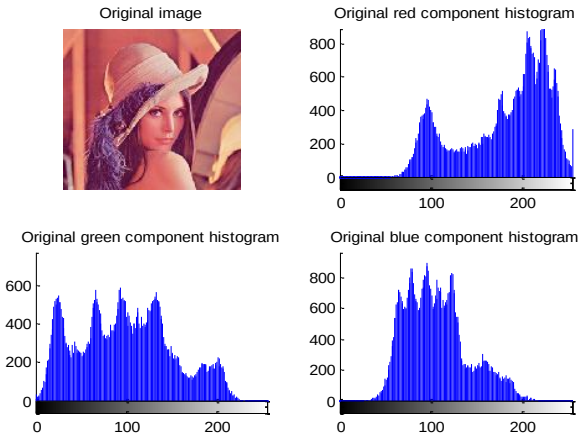


Fig 4.6: Original image for YIQ model with color components histograms

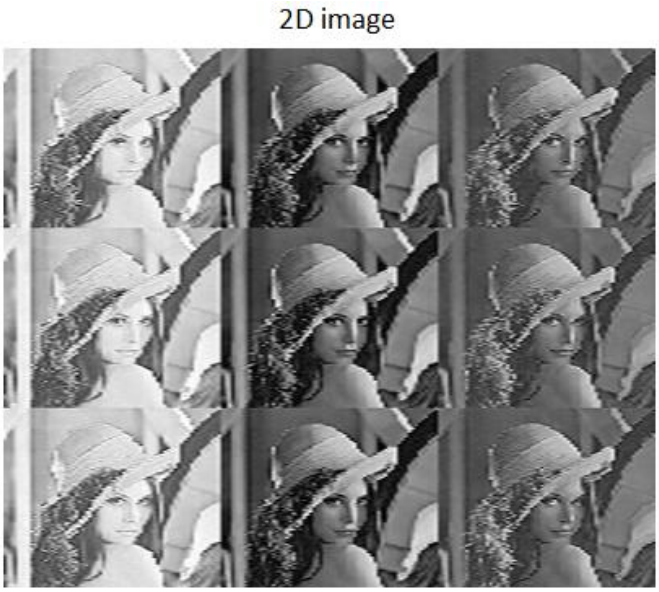


Fig 4.7: YIQ model 2D Image

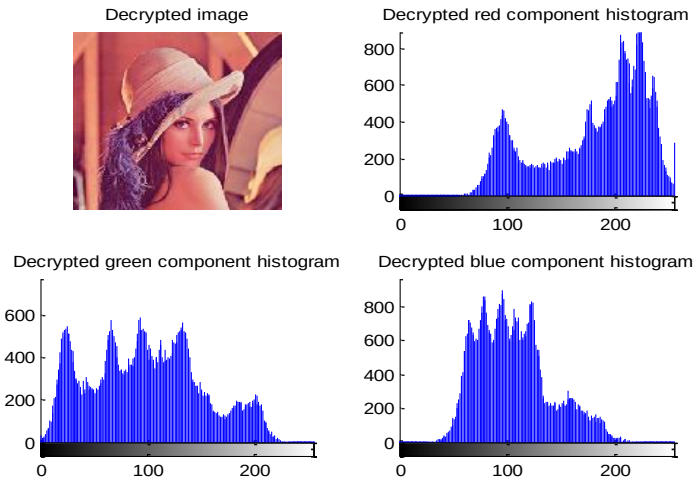


Fig 4.8: YIQ model image after encryption/decryption processes

4.2.2 Methods comparison

A selected message was chosen and 200 color images were processes with the three image processing methods described above. The processing time is measured (in seconds) for each process and recorded as encryption time (E.T.), decryption time (D.T.), and total time (T.T.). A sample of these measurements are listed in table 4.1, and 4.2, together with calculated average for each.

Table 4.1: Encryption/decryption processing time for the three methods

Image name	Image size	Method 1 *Separate color channels*		Method 2 *LSB*		Method 3 *Proposed*	
		E.T (sec)	D.T (sec)	E.T (sec)	D.T (sec)	E.T (sec)	D.T (sec)
peppers.png	384*512*3	0.089	0.339	0.566	0.222	0.073	0.168
autumn.tif	206*345*3	0.263	0.272	0.544	0.192	0.063	0.124
board.tif	648*306*3	1	0.253	0.839	0.204	0.079	0.135
coloredChips.png	391*518*3	0.326	0.32	0.907	0.225	0.114	0.178
concordaerial.png	2036*3060*3	5.19	12.69	2.722	4.702	4.552	6.194
fabric.png	480*640*3	0.344	0.321	0.599	0.272	0.141	0.224
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
hestain.png	227*303*3	0.293	0.164	0.549	0.172	0.056	0.128
office_5.jpg	600*903*3	0.445	0.5904	0.635	0.393	0.202	0.366
pears.png	486*732*3	0.38	0.36	0.613	0.283	0.139	0.285
pillsetc.png	384*512*3	0.317	0.249	0.594	0.232	0.112	0.169
Average Time		**0.8647**	**1.55584**	**0.8658**	**0.6897**	**0.5531**	**0.7971**

Table 4.2: Total processing time for the three methods

Image name	Total time (sec)		
	Method 1 ***LSB***	**Method 2** ***Separate color channels***	**Method 3** ***Proposed***
peppers.png	0.4280	0.7880	0.2410
autumn.tif	0.5350	0.7360	0.1870
board.tif	1.2530	1.0430	0.2140
coloredChips.png	0.6460	1.1320	0.2920
concordaerial.png	17.8800	7.4240	10.7460
fabric.png	0.6650	0.8710	0.3650
.	.	.	.
.	.	.	.
.	.	.	.
hestain.png	0.4570	0.7210	0.1840
office_5.jpg	1.0354	1.0280	0.5680
pears.png	0.7400	0.8960	0.4240
pillsetc.png	0.5660	0.8260	0.2810
Average Time	**2.42054**	**1.5465**	**1.3502**

As can be seen from the results presented in tables 4.1 and table 4.2 that the image encryption and decryption processing time for time is much shorter in the case of method 3 which corresponds to the image processing using YIQ model as compared with the separate color channels and the direct grey image processing methods, for example the average total time for processing using the YIQ model is (1.3502), while that for method 1 and method 2 are (2.42054)_and (1.5465), respectively. Therefore, the YIQ model for color image processing is chosen to be adopted for the text watermark embedding in color images as it is more than twice faster than any of the two other methods.

4.3 The Proposed Algorithm Implementation

The proposed text watermarking algorithm is tested for embedding and extraction of different embedded text watermark sizes into various sizes of host color images. The test covered the text lengths 100, 250, 750, 1250, and 2000 characters, and hundreds of color images with different sizes. However, three images were selected as example to be listed in this thesis, namely; Jarash, Einstein, and Lena profile with sizes 800*469, 337*268, and 225*225 pixels, respectively. First examples of watermark hiding will be listed, then embedding and extraction processing time, and finally, the peak signal to noise ratio PSNR are included.

4.3.1 Embedding imperceptibility

The proposed hiding technique is tested for different embedded watermark text size together with variation in image size. The test covered the text lengths 100, 250, 750, 1250, and 2000 characters, and the images sizes used were 800*469, 337*268, and 225*225.

The images before and after embedding of the text watermark of size 2000 bytes for three examples, namely. Jarash, Einstein, and Lena profile are listed here. These images were processed for embedding and shown in Figure 4.9 to Figure 4.11 using the proposed algorithm, Figure 4.12 to Figure 4.14 using the LSB technique offered by MATLAB, and Figure 4.15 to Figure 4.17 using the separate color channel method.

Fig 4.9 Jarash.bmp (800*469) using the proposed algorithm

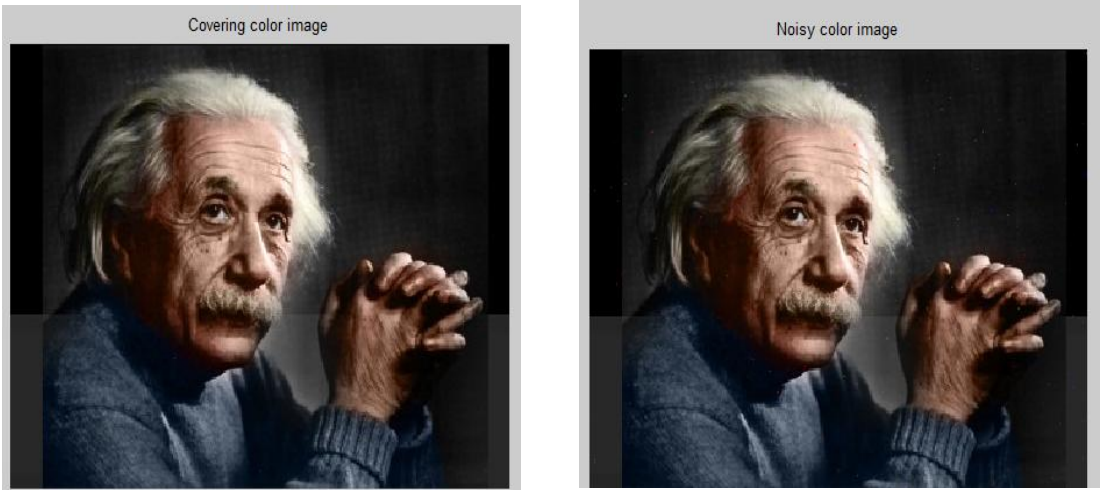


Fig 4.10 Einstein.bmp (337*268) using the proposed algorithm

Fig 4.11 Lena.bmp (225*225) using the proposed algorithm

Fig 4.12 Jarash.bmp (800*469) using LSB algorithm

Fig 4.13 Einstein.bmp (337*268) using LSB algorithm

Fig 4.14 Lena.bmp (225*225) using LSB algorithm

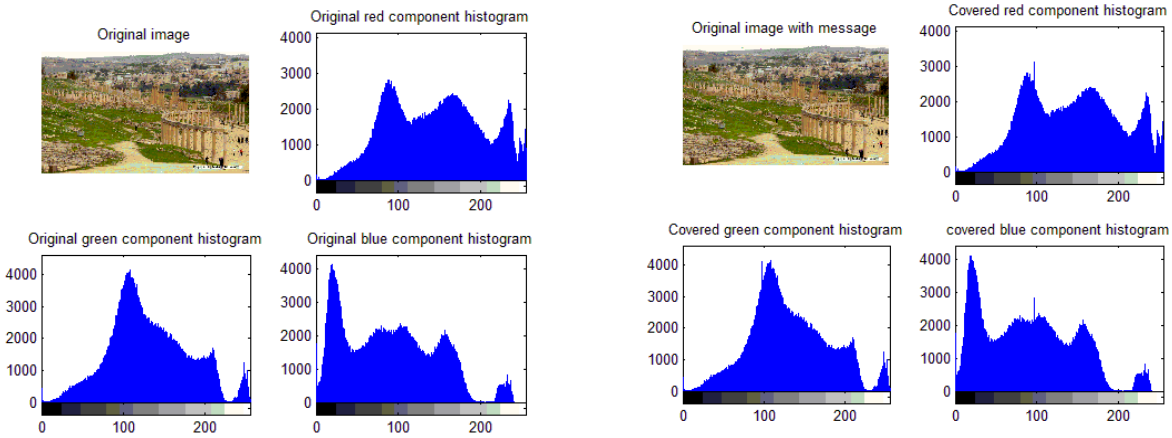


Fig 4.15 Jarash.bmp (800*469) using Separate color channels mothod

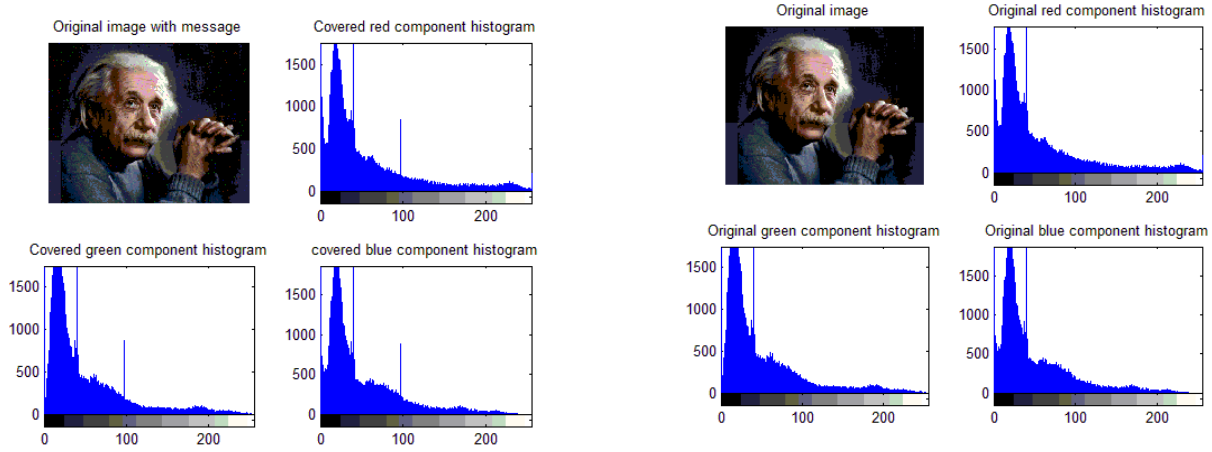


Fig 4.16 Einstein.bmp (800*469) using Separate color channels method

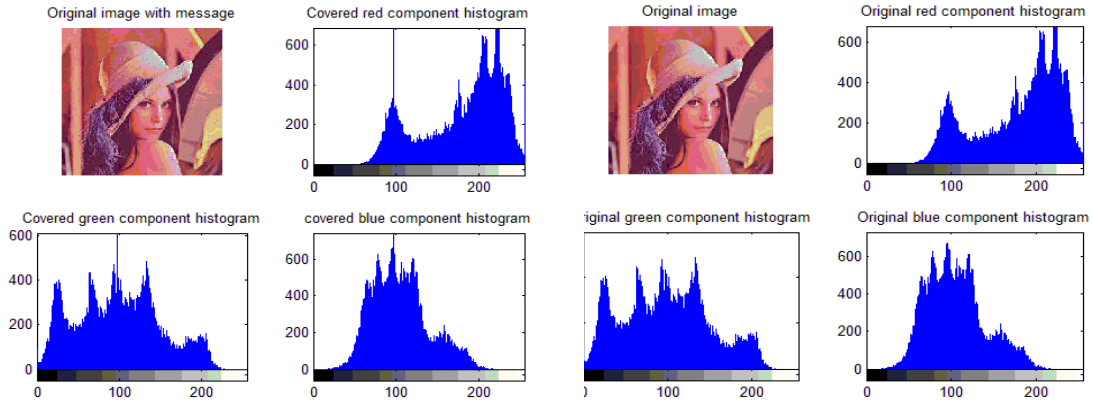


Fig 4.17 Lena.bmp (800*469) using Separate color channels method

The images of Figures 4.9 to 4.17 are included for perceptual comparison between the proposed algorithm and the other algorithms considered here. From these images it can be seen that they visually imperceptible.

4.3.2 Implementation tests

The embedding and extraction processing time and the peak signal to noise ratio for executing the proposed algorithm are computed for watermarking texts of different character combinations and different number of characters (sizes) embedded into various color images of various sceneries and sizes, too. In this chapter the same images, i.e. Jarash, Einstein, and Lena images will be listed here as examples. The experiment will also be performed using the LSB method and the separate color channels method and the results will be reported here for comparison purposes. For all the images involved in the tests, the text watermark sizes used were in the range from 100 to 2000 characters. Tables 4.3 to 4.5 list the embedding time, the extracting time, and the PSNR for implementing the proposed algorithm for hiding the text watermarks for the range under consideration, while Tables 4.6 to 4.8 and table 4.9 to 4.11 list the results when using LSB and separate color channel methods, respectively.

Table 4.3 Jarash.bmp (800*469) using the proposed algorithm

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.002746	0.000287	122.4811
250	0.004425	0.000867	113.0975
750	0.009575	0.001289	101.3833
1250	0.014333	0.002649	95.7979
2000	0.015746	0.004291	91.0756

Table 4.4 Einstein.bmp (337*268) using the proposed algorithm

Text Size (byte)	embedding Time(sec)	Extracting Time (sec)	PSNR
100	0.001462	0.000495	105.6661
250	0.002927	0.000589	95.5660
750	0.005924	0.001314	85.0605
1250	0.012835	0.001943	79.5655
2000	0.021532	0.003299	74.8961

Table 4.5 Lena.bmp (225*225) using the proposed algorithm

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.001280	0.000416	101.3503
250	0.001774	0.000581	91.8219
750	0.008457	0.001248	79.4299
1250	0.012809	0.003496	75.0089
2000	0.002887	0.002887	70.1729

Table 4.6 Jarash.bmp (800*469) using LSB algorithm

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	1.708339	0.101741	156.2086
250	1.838002	0.240047	145.6573
750	1.784629	0.378115	133.8458
1250	1.996868	0.607607	128.5472
2000	1.810302	0.673065	123.7436

Table 4.7 Einstein.bmp (337*268) using LSB algorithm

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.557875	0.089620	139.9674
250	0.641187	0.152528	130.7687
750	0.663024	0.262900	120.0071
1250	0.607541	0.530411	115.4919
2000	0.683862	0.590371	114.3283

Table 4.8 Lena.bmp (225*225) using LSB algorithm

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.382749	0.077110	133.6313
250	0.412733	0.127564	124.3898
750	0.426931	0.314536	114.1646
1250	0.478724	0.333288	113.6753
2000	0.455618	0.469714	113.6753

Table 4.9 Jarash.bmp (800*469) using the separate color channels method

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.01767	0.09916	128.1517
250	0.03919	0.09599	114.4798
750	0.04319	0.1502	101.5126
1250	0.04251	0.09365	96.0315
2000	0.04664	.0.9557	91.0393

Table 4.10 Einstein.bmp (337*268) using the separate color channels method

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.0560	0.01208	106.0534
250	0.0679	0.01299	95.3762
750	0.0633	0.01325	86.7080
1250	0.0761	0.01494	79.8441
2000	0.0720	0.01400	76.7915

Table 4.11 Lena.bmp (225*225) using the separate color channels method

Text Size (byte)	embedding Time (sec)	Extracting Time (sec)	PSNR
100	0.0283	0.0483	101.4345
250	0.0311	0.0560	92.1156
750	0.0305	0.0512	79.9475
1250	0.0308	0.0701	75.0877
2000	0.0469	0.0631	70.7896

4.3.3 Comparisons

The embedding and extraction time for different watermark text size into images of various sizes are computed for the proposed algorithm, LSB algorithm, and the separate color channels method are listed in Table 4.12 for comparison purposes. It is clear that the proposed method requires much less time in both processes. The three images used for these tests are Jarash.bmp, Einstein.bmp, and lena.bmp, with image size of 800*469, 337*268, and 225*225 pixels, respectively, and the text watermarks sizes used were in the range from 100 characters to 2000 characters.

Table 4.12: Embedding and Extraction Time Comparison

Name and size of the image	Text size (byte)	LSB algorithm		Separate color channels method		The Proposed algorithm	
		embedding time (sec.)	Extracting time (sec.)	embedding time (sec.)	Extracting time (sec.)	embedding time (sec.)	Extracting time (sec.)
Jarash.bmp (800*469)	100	1.708339	0.101741	0.01767	0.09916	0.002746	0.000287
	250	1.838002	0.240047	0.03919	0.09599	0.004425	0.000867
	750	1.784629	0.378115	0.04319	0.1502	0.009575	0.001289
	1250	1.996868	0.607607	0.04251	0.09365	0.014333	0.002649
	2000	1.810302	0.673065	0.04664	.0.9557	0.015746	0.004291
Einstein.bmp (337*268)	100	0.557875	0.089620	0.0560	0.01208	0.001462	0.000495
	250	0.641187	0.152528	0.0679	0.01299	0.002927	0.000589
	750	0.663024	0.262900	0.0633	0.01325	0.005924	0.001314
	1250	0.607541	0.530411	0.0761	0.01494	0.012835	0.001943
	2000	0.683862	0.590371	0.0720	0.01400	0.021532	0.003299
Lena.bmp (225*225)	100	0.382749	0.077110	0.0283	0.0483	0.001280	0.000416
	250	0.412733	0.127564	0.0311	0.0560	0.001774	0.000581
	750	0.426931	0.314536	0.0305	0.0512	0.008457	0.001248
	1250	0.478724	0.333288	0.0308	0.0701	0.012809	0.003496
	2000	0.455618	0.469714	0.0469	0.0631	0.002887	0.002887

Moreover, PSNR values are also calculated for the some cases of Table 4.12 and listed in Table 4.13. These PSNR values are also illustrated in the comparison histograms plotted in Figure 4.18.

Table 4.13: PSNR Value Comparison

The name and size of the image	Text size(byte)	LSB algorithm	Separate color channels method	The Proposed algorithm
Jarash.bmp (800*469)	100	156.2086	128.1517	122.4811
	250	145.6573	114.4798	113.0975
	750	133.8458	101.5126	101.3833
	1250	128.5472	96.0315	95.7979
	2000	123.7436	91.0393	91.0756
Einstein.bmp (337*268)	100	139.9674	106.0534	105.6661
	250	130.7687	95.3762	95.5660
	750	120.0071	86.7080	85.0605
	1250	115.4919	79.8441	79.5655
	2000	114.3283	76.7915	74.8961
Lena.bmp (225*225)	100	133.6313	101.4345	101.3503
	250	124.3898	92.1156	91.8219
	750	114.1646	79.9475	79.4299
	1250	113.6753	75.0877	75.0089
	2000	113.6753	70.7896	70.1729

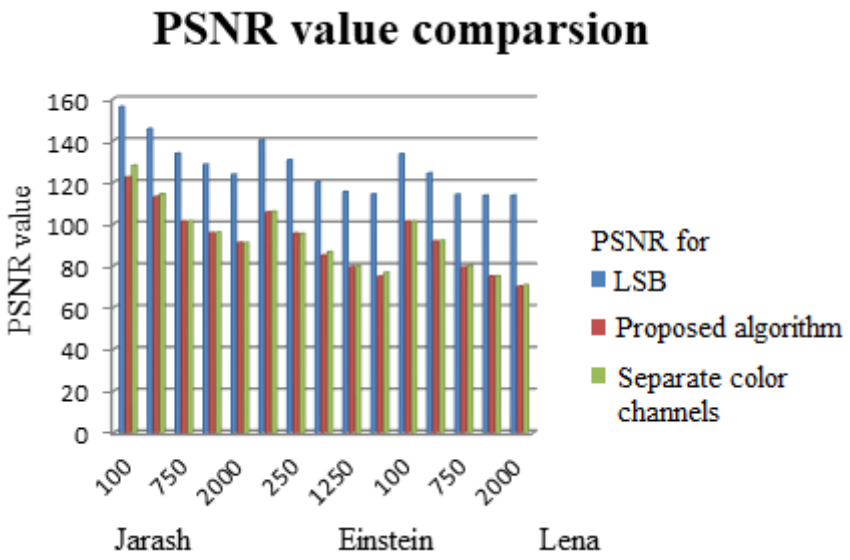


Fig 4.18 PSNR values comparison between the proposed algorithms with others

The calculated PSNR values listed in table 4.13 and plotted in Figure 4.18 show that the PSNR for the proposed algorithm is in the same range of that for the separate color channel algorithm but it is less than that of the LSB algorithm, besides its values get lower as the embedded text size increases. This can be explained as being attributed to the fact that the proposed method depends upon the replacement of the whole pixel in the selected place, while it is the change of only the least significant bit of the selected pixel in the case of LSB method. However, the PSNR values are still over 70 dB for text lengths of 2000 characters which is normally acceptable. In other word, the proposed method introduces more noise into the host images, and as watermarks are usually chosen small in size, therefore the proposed algorithm is more suitable for text watermarks, rather than steganographic long messages.

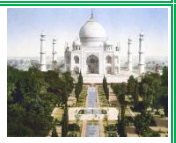
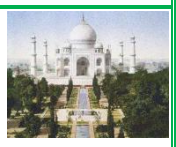
4.4 Performed Attacks

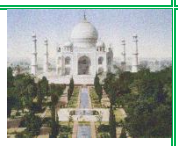
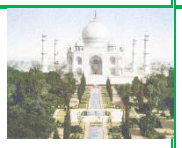
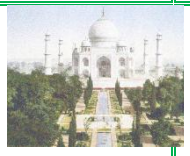
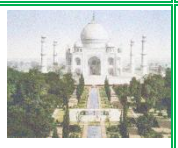
The attacks on any image might attributed to either noise may (whether intentional or not) or external processing effects. They are both cause affect the image quality. If an image is sent from one place to another, via any communication process, such disturbances are expected to occur in the image signal. These disturbances will have its effect on the images in different ways. The watermark in the images are used for copyright protection and are expected to withstand external effects, however, if one knows the type of expected errors, hence one can choose the most appropriate method in order to reduce these effects. In this chapter some attacks were applied that included Gaussian and Poison's noise as well as resizing, cropping, and rotation on different size watermarked images obtained by the proposed method. Although the proposed watermarking algorithm is known to be fragile, different types of attacks on the watermarked images were conducted to see if any possibility of watermark survival when different percentages of effects (Noise or Distortion) are used. All experiments have confirmed that the watermarks were lost. These attacks included the following:

4.4.1Gaussian noise test

The most wide notice in most image handling process is the Gaussian noise, which is usually an idealized form of white noise caused by random fluctuations in the signal (may be referred to as thermal noise). It is usually observed when watching a television program that is slightly mistuned to a particular channel. In this thesis, this noise is introduce with mean value ranges from 0 to 0.5 and variant values (0.01, 0.03, 0.05, 0.07, 0.09, and 0.11) on three images with deferent sizes as illustrated in table 4.14. The image sizes used in this test will be (MEU 640*360), (Taj-Mahal 1203*941), and (Penguin 1024*768).

Table 4.14 Addition of Gaussian Noise to the watermarked images

Mean	Variant	MEU	Taj-Mahal	Penguin
0	0.01			
0	0.03			
0	0.05			
0	0.07			
0	0.09			
0	0.11			
0.1	0.01			
0.1	0.03			
0.1	0.05			

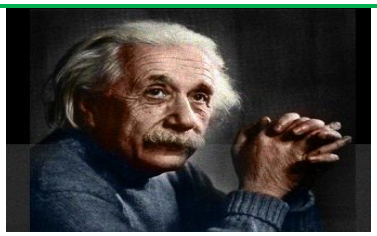
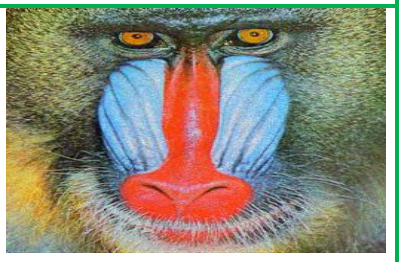
0.1	0.07			
0.1	0.09			
0.1	0.011			
Mean	**Variant**	**MEU**	**Taj-Mahal**	**Penguin**
0.3	0.01			
0.3	0.03			
0.3	0.05			
0.3	0.07			
0.3	0.09			
0.3	0.011			
0.5	0.01			

0.5	0.03			
0.5	0.05			
0.5	0.07			
0.5	0.09			
0.5	0.011			

4.4.2 Poisson noise test

Poisson noise are also called shot noise. This test highlights one type of watermarked image effects or attack. Table 4.15 illustrate the resulting images when Poison noise is added to the images.

Table 4.15 Addition of Poisson noise

Einstein	
Lena	
Baboon	

4.4.3 Resizing

The image size is changed by certain percentages and the resulting watermarked image is drown. Five images were considered; Baboon, Jarash, MEU building, Penguin and Taj-Mahal as shown in Table 4.16. All the obtained results lead to a damage in term of quality to the watermark. Using 50%,60%,70%,80% and 90% resizing on the original image that's had been implemented.

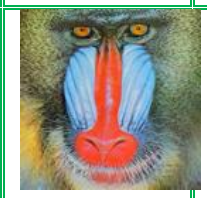
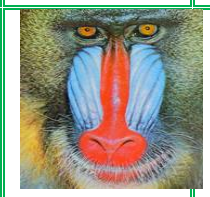
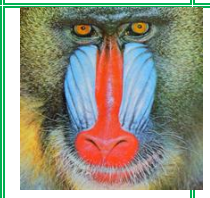
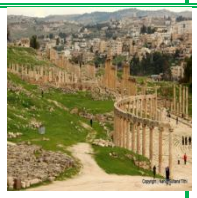
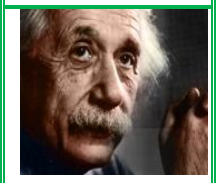
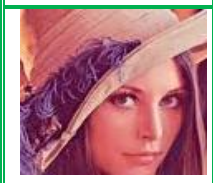
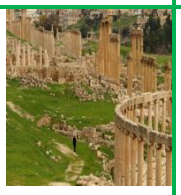
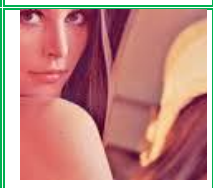
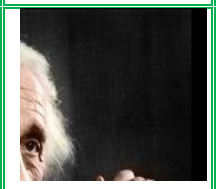
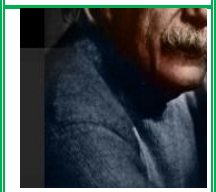
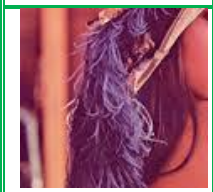
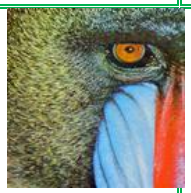
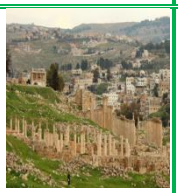
Resize	Baboon	Jarash	MEU	Penguin	Taj-Mahal
50%					
60%					
70%					
80%					
90%					

Table 4.16 Image resizing

4.4.4 Cropping:

Removing some parts of the image is called cropping. This involves cutting some of the image from the left, right, top, bottom or any combination. This action effects the position of all pixels in the image which leads to great differences in the pixel locations leading to changes of the embedding key. The images are shown in Table 4.17.

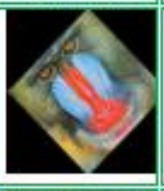
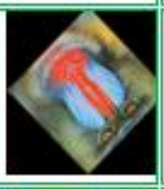
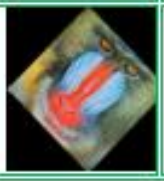
Table 4.17 Cropping

Cropping	Einstein	Lena	Baboon	Jarash	MEU
Center					
Down Right					
Upper Right					
Down Left					
Upper Left					

4.4.5 Rotating

Rotating simply means a test applied to an image in many anti clock wise position. In this thesis the rotations were in the following anti-clockwise angles, 45o, 90o, 135o, 227o and 335o, as showing Table 4.18.

Table 4.18 Image Rotation

Rotate	Einstein	Baboon	Lena	Taj-Mahal	Penguin
45 degree					
90 degree					
135 degree					
180 degree					
225 degree					
270 degree					
315 degree					

Chapter Five

Conclusions and Future Work

5.1 Conclusion

This thesis included the development, design, implementation, and testing of text watermarking algorithm into color images. Embedding of the text contents was investigated for various sizes of images and different length of texts. The proposed algorithm produces watermarks that are imperceptible by visual inspection and was implemented and tested for copyright protection and ownership judgment. In this algorithm, the text characters embedding is based on spatial domain embedding technique as noise insertion in the host image to be protected relying on a randomly generated secret key of variable length that is related to the text length and the message size.

Measurements of PSNR, MSE for the proposed techniques have shown that it is efficient. It has given a value of PSNR of over 70 dB for a text watermark of 2000 characters which may be considered good enough as compared with other techniques.

The proposed algorithm showed an encouraging improvement in having comparatively fast embedding and extraction processes speed as compared with other spatial watermarking techniques as the embedding and extraction time was much shorter as compared with LSB algorithm and the separated color channels method, as the algorithm relies on the random insertion of the text as noise into the images rather than bits into pixels.

The algorithm suggested an option of encrypting the watermark, which although will increase the execution time somehow, it would be useful for applications which requires watermark authentication. The encryption process for the text watermark use matrix manipulation procedure that requires a secret key matrix.

In brief, the proposed methodology is effective as compared with other spatial domain watermarking techniques, by achieving the following goals:

- The calculated embedding and extraction processing time was reduced, which makes the proposed method more suitable for applications that demand fast processing.
- For short watermark text, the noise in the watermarked image was very small and imperceptible.
- The PSNR values were very high, but it gets less and less as the embedded text size increase much faster than LSB method, however it suitable because watermarks are almost always kept as small as possible.

❑ The randomly generated embedding key influenced by the watermark size and the image size.

Therefore, it can be concluded that the proposed text watermarking algorithm is suitable for short text messages embedding into color image for the purpose of copyright protection and ownership judgment applications, rather than for steganography application, i.e. not for encrypting and decrypting long messages for secure data storage or messages transfer over the internet.

5.2 Future Suggestions

Future works and improvement to the proposed method would include the following:

1. More investigations would be required to see the effect of using environmental situation on the watermarked images, such as various noise like Gaussian, Poisson ,salt and pepper, and also the effect of distortion, compression, cropping, skewing, resizing, etc.
2. Trying the possibility of coupling this algorithm with other watermarking methods, i.e. working on hybrids watermarking methods in order to get more satisfactory results.
3. Using this algorithm for short message exchange or emails over smart telephones.
4. Design, test and implement online chat system with text watermarking capabilities.
5. Develop the method in order to use Arabic text watermarking.
6. Improve system that can use a watermarking on 3D images.

References

Adel Mohammed Salman, (2005), An implementation of encrypting watermarking for images using visual cryptography‖, Ms.c thesis, Informatics Institute for Postgraduate Studies, University of Technology, Baghdad.

Anderson R., (1996), "Information Hiding". Vol. 1174 of Lecture Notes in Computer Science, Berlin; New York: Springer-Verlag.

Asaad Flayih Qasim, (2005). Development of Invisible Text Watermarking using PDF and PostScript Files. Ms.c thesis, Informatics Institute for Postgraduate Studies, University of Technology, Baghdad.

Auday Jamal Fawzi, (2007), Data Hiding in Arabic Text, PhD thesis‖, Technical Education Department, University of Technology, Baghdad.

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).

Behrouz A. Forouzan, (2011) TCP/IP Protocol Suite , Fourth edition, McGraw Hill.

Bors Adrian G., and Ioannis Pitas, (1996), "Image watermarking using DCT domain constraint". IEEE Int. Conf. Image Processing (ICIP'96). Vol.3, pp. 231 – 234.

Chang Hsing Lee and Yeuan Kuen Lee, (2003) An Adaptive Digital Image Watermarking Technique for Copyright Protection , Department of computer Science, Chines Culture University, Proceedings of IEEE International Conference on Image Processing.

Chen Bo and Hong Shen, (2009), "A New Robust-Fragile Double Image Watermarking Algorithm". Third International Conference on Multimedia and Ubiquitous Engineering MUE '. PP. 153-157, November.

Cox Ingemar J., Matthew L. Miller and Jeffrey A. Bloom, (2001), "Handbook of Digital Watermarking". Morgan Kaufmann Publishers, Inc., San Francisco.

Cox Ingemar J., Matthew L. Miller and Jeffrey A. Bloom, (2008), "Handbook of Digital Watermarking". Morgan Kaufmann Publishers, Inc., San Francisco.

Craver S., N. Memon, Boon-Lock Yeo, and M. Yeung,(1998), Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. IEEE Transaction on Selected Areas in Communications, Vol. 16, No. 4, PP. 573–586.

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.

Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA).

F. Seb´e, J. Domingo-Ferrer, and J. Herrera (2000), "Spatial-Domain Image Watermarking Robust against Compression, Filtering, Cropping, and Scaling", Pieprzyk, E. Okamoto, and J. Seberry (Eds.): ISW 2000, pp. 44–53.

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.

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.

Hyoung Joong Kim, (2004), Audio Watermarking Techniques. Department of Control and Instrumentation Engineering, Kangwon National University, Korea.

I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, (1997), Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 6(12):1673–1687.

I. J. Cox and J.-P. Linnartz, (1998), Some general methods for tampering with watermarks. IEEE Trans. on Selected Areas of Communications, 16(4):587–593.

Jassim Mohmmed Ahmed and Zulkarnain Md Ali, (2011), Information Hiding using LSB technique, School of Computer Science, Faculty of Information Science and Technology, University Kebangsan Malaysia, Malaysia, International Journal of Computer Science and Network Security, VOL.11 No.4.

Jihad Nadir, Ziad Alqadi and Ashraf Abu Ein, (2016), Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image, International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 05 – Issue 05.

Johnson, N. F., Duric, Z. and Jajodia, S., (2000), Information Hiding: Steganography and Watermarking-Attacks and Countermeasures‖. Kluwer Academic Publishers, Boston Dodrecht London.

Jonathan K. Su, Frank Hartung and Bernd Girod, (1999), Digital Watermarking of Text, Image, and Video Documents. Telecommunications Laboratory University of Erlangen-Nuremberg, Germany.

Komatsu N. and H. Tominaga, (1988), “Authentication System Using Concealed Images in Telematics”. Memoirs of the School of Science and Engineering. Waseda University, PP. 45–60.

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.

Lawrence Hughes, (1998), Internet E-mail Protocols, Standards, and Implementation‖ , Artech House Boston , London, ISBN 0-89006-939-5.

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.

Malik H., Ashfaq Khokhar and Rashid Ansari, (2004), “Robust Audio Watermarking Using Frequency Selective Spread Spectrum Theory”. Proceedings in IEEE International Conference. Vol.5, PP. 385-388.

Mamta.Juneja , Parvinder S. Sandhu, (2013),“An improved LSB based Steganography with enhanced Security and Embedding/Extraction”, 3rd International Conference on Intelligent Computational Systems (ICICS'2013) , Hong Kong (China)J.

Manjit Thapa Dr. Sandeep Kumar Sood Meenakshi Sharma, (2001), Digital Watermarking: Current Status and Key Issues. International journal of Advances in Computer Networks and its security. Vol. 1, Issue 1, pp. 327-332.

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.

Mohamed-Salim Bouhlel, Hanène Trlchlll, Nabil Derbel and Lotji EamoNn, (2002) On the Image Watermarking Techniques Applications, Properties and fields. RIST, Vol. 12, No. 02, pp. 39-46.

Mohanty Saraju Prasad, (1999). Watermarking of Digital Images. MS.c. Thesis, Department of Electrical Engineering, Indian Institute of Science.

Morkel T., Eloff J. H. P., and Olivier M. S., (2005), An Overview of Image Steganography , Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria, South Africa.

M. S. Hsieh, D. C. Tseng and Y. H. Huang, (2001), Hiding Digital Watermarking Using Multiresolution WaveletTransform‖, IEEE Transactions on Industrial Electronics, Vol. 48, No. 5.

Ms. Nidhi Bux , Prof. K. J. Satao, (2015), Implementation of Watermarking Technique for Secured Transmission, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8.

Muntean T., E. Grivel and Mohamed Najim, (2002), "Audio Digital Watermarking Based on Hybrid Spread Spectrum". Proceedings, IEEE the Second International Conference on WEB Delivering of Music (WEDELMUSIC). PP. 150-155.

Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, (2013), Enhancing the security and quality of LSB based image steganography , International Conference on Computational Intelligence and Communication Networks.

N. Chowdhury, B. Banerjee T. Bhattacharjee "color image segmentation technique using natural grouping of pixels", International Journal of Image Processing, 1985-2304, 2010.

Nirmal Kumar , (2008), A wavelet domain implementation of digital watermarking. Ms.c thesis. department of electronics & communication engineering, university of delhi , delhi.

Oscar E. Ramos and Babak Rezaei, Scene Segmentation and Interpretation Image Segmentation using Region Growing, 2010.

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.

Petitcolas, F. A. P., R. J. Anderson and M. G. Kuhn, (1999), "Information hiding-a survey." Proceedings of the IEEE, vol. 87, pp. 1062-1078.

Provos Niels, (2009), "Hide and Seek: Introduction to steganography". IEEE Computer society.

R. C. Gonzalez and R. E. Woods, digital image processing, Pearson education, 2002.

Reena M Patel,D J Shah ,(2013), Concealogram : Digital image in image using LSB insertion method, International journal of electronics and communication engineering & technology(IJECET).

Rojo, M.G., G.B. García, C.P. Mateos, J.G. García and M.C. Vicente, 2006. Critical comparison of 31 commercially available digital slide systems in pathology. Int. J. Surg. Pathol., 14: 285-305.

S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, (1998), Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. IEEE Trans. on Selected Areas of Communications, 16(4):573–586.

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.

Simpson J. and E. Weiner, (2000), editors, "Oxford English Dictionary". New York: Oxford University Press.

S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, “A New Approach for LSB Based Image Steganography using Secret Key”, Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 201 I, Dhaka, Bangladesh.

S.K. Naik and C.A. Murthy, "Hue-preserving color image enhancement without gamut problem," IEEE Trans. on Image processing, vol.12, no.12, pp.1591-1598, December 2003.

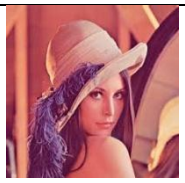
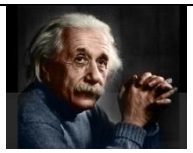
Sruthi, N., Sheetal, A. V., &Elamaran, V. (2014, April). Spatial and spectral digital watermarking with robustness evaluation. In Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on (pp. 500-505). IEEE.

Wong P.W. and E. J. Delp, (1999), "Security and Watermarking of Multimedia Contents" Proceedings of the Society of Photo-optical Instrumentation Engineers, Vol. 3657.

Yusof and Y. Khalifa, (2007), ”Digital watermarking for digital images using wavelet transform". IEEE International Conference on Telecommunications and Malaysia International Conference on Communications(ICTMICC). PP. 665-669.

Appendices A

The used image in this research.

Name and Size	Image	Name and Size	Image	Name and Size	Image
Eiffel 400*600		Bridge 256*256		Lena 225*255	
Istanbul 550*338		Red 720*640		Baboon 256*256	
Istanbul 1500*100		Camera 820*532		Lion 1560*1600	
Roma 1730*1100		Roma 540*359		Einstein 337*268	
Sydney 1650*1080		Sydney 300*168		Fruit 3818*2540	
London 1300*760		London 600*375		Petra 1200*630	
Baghdad T 564*702		Jerash 800*469		Penguin 1024*768	

Name and Size	Image	Name and Size	Image	Name and Size	Image
Mammon Tower 736*476		Taj-Mahal 1203*941		Camera Man 256*256	
MEU 640*360		Babylon 900*506		Cover 1024*768	
-	-	-	-	-	-
-	-	-	-	-	-
Ishtar Gate 512*512		Jordan Map 100*865		Great Wall 450*648	
Lighthouse 1024*768		Eye 225*225		Trees 259*194	
Balloon 300*168		Ship 275*183		Dinosaur 275*183