The Islamic University–Gaza
Research and Postgraduate Affairs
Faculty of Information Technology
Master of Information Technology

الجامعـــــــة الإســـلاميــة – غـزة
شئون البحث العلمي والدراسات العليا
كـليـــــــــــة تكنولوجيا المعلومات
ماجستيـــــر تكنولوجيا المعلومات

LSBs Steganography Based on R-Indicator

الإخفاء في البتات الأقل أهمية اعتمادا على المؤشر في القناة الحمراء

Sheren Mohammed Abo Mousa

Supervised by

Dr. Tawfiq Barhoom
Associate Prof. of Computer Science

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Information Technology

March/2017

إقـــــــــرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

LSBs Steganography Based on R-Indicator
الإخفاء في البتات الأقل أهمية اعتمادا على المؤشر في القناة الحمراء

أقر بأن ما اشتملت عليه هذه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل الاخرين لنيل درجة أو لقب علمي أو بحثي لدى أي مؤسسة تعليمية أو بحثية أخرى.

Declaration

I understand the nature of plagiarism, and I am aware of the University's policy on this.

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted by others elsewhere for any other degree or qualification.

Student's name:	شيرين محمد أبو موسى	اسم الطالب:
Signature:	شيرين أبو موسى	التوقيع:
Date:	21/03/2017	التاريخ:

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

الجامعة الإسلامية غزة
The Islamic University - Gaza

مكتب نائب الرئيس للبحث العلمي والدراسات العليا **هاتف داخلي:** 1150

الرقم ....ج س غ/35/....... Ref

التاريخ 2017/03/21 .... Date

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة شئون البحث العلمي والدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحثة/ **شيرين محمد جمعه ابوموسى** لنيل درجة الماجستير في **كلية *تكنولوجيا المعلومات*** برنامج تكنولوجيا المعلومات وموضوعها:

الإخفاء في البتات الأقل أهمية اعتماد على المؤشر في القناة الحمراء
LSBs Steganography Based on R-Indicator

وبعد المناقشة التي تمت اليوم الثلاثاء 22 جمادي الثانية 1438هـ، الموافق 2017/03/21م الساعة العاشرة والنصف صباحاً في قاعة اجتماعات مبنى القدس ، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. توفيق سليمان برهوم	مشرفاً و رئيساً	....
د. أشرف يونس مغاري	مناقشاً داخلياً	....
أ.د. سامي سليم أبو ناصر	مناقشاً خارجياً	....

وبعد المداولة أوصت اللجنة بمنح الباحثة درجة الماجستير في **كلية *تكنولوجيا المعلومات*/** برنامج **تكنولوجيا المعلومات.**

واللجنة إذ تمنحه هذه الدرجة فإنها توصيها بتقوى الله ولزوم طاعته وأن يسخر علمها في خدمة دينها ووطنها.

والله ولي التوفيق ،،،

شئون البحث العلمي والدراسات العليا
الجامعة الإسلامية غزة
The Islamic University
Research & Graduate Affairs

نائب الرئيس لشئون البحث العلمي والدراسات العليا

أ.د. عبدالرؤوف علي المناعمة

Abstract

Steganography is the art and science of hiding secret data inside other data called the cover data. This makes it hard to detect the existence of the secret data by third parties. There are different models of carrier that can be used as stego cover, such as text, image, audio and video to hide information. The most common way is the image due to the reluctance on the internet. And thus it can guarantee a high degree of security.

There are a lot of algorithms and techniques to hide data. Every algorithm has its own mechanism which has strengths and weaknesses points. Some techniques are limited with hiding inside specific type of data, and some can be used with multiple types of carriers.

This study introduces a new algorithm called ST_R-indicator steganography algorithm for hiding data based on the Least Significant Bit (LSB), where the algorithm embeds inside these LSB(s).

The researcher proposed a new algorithm that used benchmark RGB images (with png, bmp extention) as a cover media where each pixel is represented by three bytes (24 bit) red, green, and blue in pixel. The process of hiding depends on pixel indicator technique which is called R-indicator. They use the same principle of the Least Significant Bit (LSB), where the secret message is hidden at the least significant bits of the pixels, with more randomization in chosen of the number of bits used and the colour channels that are used. In addition, they may be embedded into one or two bits at the same time. This randomization makes the method robust against steganalysis and this is the advantage of this algorithm over normal LSB algorithm and also increases the capacity of information.

After completing implementation of the proposed algorithm, the researcher evaluated the proposed algorithm to measure its efficiency in aspects of imperceptibility, capacity, robust and ranomaization. Many tools were used such as PSNR, MSE, StegExpose and histogram. Experimental results showed an increasement capacity of information, increasing robust and better image quality. Its notability was compared to several existing methods.

الملخص

إخفاء المعلومات هو فن وعلم إخفاء البيانات السرية في بيانات أخرى، وهو ما يسمى بيانات الغطاء، ولذلك فمن الصعب الكشف عن وجود بيانات سرية من قبل أطراف ثالثة، هناك أنواع مختلفة ملف الناقل(الغطاء) يمكن استخدامه مثل النص، صورة، ملف الصوت ، ولكن الصورة هي الأكثر استخداما ، وبالتالى فانه يمكن أن يضمن درجة عالية من الامان .

هناك الكثير من الخوارزميات والتقنيات لإخفاء البيانات. كل خوارزمية لديها آلية خاصة بها وهذا يعطيها نقاط القوة والضعف. تقتصر بعض التقنيات على الاخفاء داخل نوع معين من البيانات، وبعضها يمكن استخدامها مع أنواع متعددة من الملف الناقل.

في هذه الدراسة قدمنا بتقديم خوارزمية جديدة ST_R-indicator حيث يتم اخفاء البيانات بطريقة LSB

في هذا المقترح تم استخدام الصور الملونة RGBبامتداد PNG, BMP حيث يتم تمثيل كل بكسل من 3 بايت (24 بت) الاحمر والاخضر والازرق في كل بكسل وعملية إخفاء المعلومات تعتمد على المؤشرات وسميت R_indictor ،حيث تستخدم نفس مبدأ البت الأقل أهمية ، حيث يتم إخفاءه بطريقة أكثر عشوائية في اختيار عدد البتات المستخدمة وقنوات الالوان التي تستخدم في الاخفاء حيث يتم اخفاء بت او اثنين في نفس الوقت . هذا التوزيع العشوائي يجعل طريقتنا قوية ضد تحليل الغطاء وهذا هوميزة هذه الخوارزمية على خوارزمية البت الاقل اهمية وأيضا يزيد من قدرة المعلومات.

بعد تنفيذ الطريقة المقترحة ، تم تقييم المنهج المقترح لقياس كفاءتها من حيث جودة الصورة ونسبة الحمولة والقوة والعشوائية ،حيث استخدمت مجموعة من الأدوات مثل PSNR,MSE,StegExpose,histogram ، وقد اظهرت النتائج زيادة في تحميل المعلومات،وزيادة قوة الخوارزمية وجودة أفضل للصورة وأظهرت تفوقها بالمقارنة مع العديد من الطرق الحالية .

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿ قُلْ هَلْ يَسْتَوِى الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لَا يَعْلَمُونَ إِنَّمَا يَتَذَكَّرُ
أُولُو الْأَلْبَابِ﴾

[الزّمر:9]

Dedication

I dedicate this research for
The soul of my father
My beloved mother
My beloved brothers
My heart sisters
My friends
And to all the people who helped me bring this research.

Acknowledgment

First of all, I thank God for giving me the strength and the ability to complete this study.

Also I would like to thank my parents, my brothers and sisters for their support and encouragement throughout the entire academic life.

I would like to thank the Information Technology Faculty members , my colleagues at the college of Information Technology.

Finally, I thank my supervisor **Dr. Tawfiq Barhoom** for his continuous support, encouragement and his help throughout my studies and continuous advice to reach the end of this research.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

BMP: a Microsoft Windows bitmap file.

DFT: Discrete Fourier Transform

GIF: Graphical Interchange Format.

HVS: Human Visual System.

JPEG: Joint Photographic Experts Group.

LSB: Least Significant Bit.

MSE: Mean Square Error.

PIT: Pixel Indicator Technique

PNG: Portable Network Graphics

PSNR: Peak Signal-to-Noise Ratio.

RGB: Red Green Blue.

Chapter 1
Introduction

Chapter 1

Introduction

Data is a basis element of computer communication. Many techniques are developed to achieve the goal of steganography in how to hide data in media object with more security to be undetectable .(Laskar & Hemachandran, 2013).

There are different models of carrier that can be used as stego cover, such as text, image, audio and video to hide information. The most common way is to hide in the image due to its reluctance on the internet.

Image Steganography is a steganography technique that uses image as a cover object. There are many kinds of image types that can be used as covers such as these examples: jpg, bmp, png etc(HUSSEIN, 2015).

Previous studies proposed many algorithms for hiding data, some of these algorithms depend on the nature of the carrier which is hiden into image, audios(Barhoom & Mousa, 2015; Khalil, 2011b) and other may be used with different types of carriers like Text, Image, Audio/Video which were the first common methods that were used to hide the information in the image cover (Das & Tuithung, 2012; Gupta & Garg, 2010). Image steganography is the most used type (Morkel et al., 2005). But many algorithms suffer from capacity (hide the maximum data inside cover image), randomization and Imperceptibility (quality of stego-image after data hiding) (Akhtar et al., 2013; M. R. Islam et al., 2014; S. M. Karim et al., 2011).

Any algorithm can measure three aspects which are imperceptibility (quality of stego-image after data hiding), capacity (number of bit that can be hidden), robustness (degree of difficulty required to retrieved information embedded without damaging the cover image).

This research introduce a new algorithm called ST_R-indicator steganography algorithm of hiding data based on the Least Significant Bit (LSB), where the algorithm is embedded inside the LSB(s).

We proposed a new algorithm that uses RGB image steganography based pixel Indicators technique which we call R-indicator. Actually, this method uses the same principle of the technique LSB method since it embeds at the least one or two bits, with more randomization in chosing the number of bits used and the colour channels that are used and it may be embedded into one or two bits at the same time. This randomization makes the method robust against steganalysis and this is the advantage of this algorithm over normal LSB algorithm. In addition, it increases the capacity of information. However, ST_R-indicator algorithm can be applied to RGB images (png, bmp) by formating it with a cover media where each pixel is represented by three bytes (24 bit) Red, Green, and Blue. The process of hiding depends on the indicators. The indicators are used to determine what cover bytes to embed into this RGB channel. Other indictors are used to determine how many secret bits are needed to embed at a time.

This Indicator Selection (IS) is chosen randomly in the Red channel by depending on the weight of the byte from fourth to seventh bits in this channel and then makes XORed operator with both the indicator and the next bit. Then, the result of all this will make the XORed with the previous bit, depending on the value (zero or one) and can hide data into the Green, Blue, Red channel or Blue, Green, Red channel. Other indicators (IN) determine how many secret bits to embed by depending on the value of the next and previous bit of Indicator Selection (IS).

Many of the tools that have been used to evaluate this algorithm like PSNR, MSE stegExpose and histogram.

Experimental results show an increasement capacity of information and randomization which makes a better imperceptibility (image quality). Evaluation of this algorithm measures its efficiency in aspects of imperceptibility, capacity, robust and randomiztion with making a comparison with simple LSB substation methods which show its notability and compars it with several existing methods.

1.1 Statement of the problem

Images based on steganography have a lot of algorithm that has three aspects of a good technique. These aspescts are capacity, robustness and imperceptibility. The previous work suffers from capacity, robustness and imperceptibility.

The problem of this research focuses on the problem of capacity, randomization and imperceptibility which needs to be solved.

1.2 Objectives

This section describes the main objective and other specific objectives.

1.2.1 Main objective

The main objective of this research is to Propose a new algorithm of hiding secret data based on pixel indicator technique. It is called ST_R-indicator. It useses the same principleof the Least Significant Bit (LSB), with more randomization .This randomization makes the method robust against steganalysis and this is the advantage of this algorithm over normal LSB algorithm and also increases the capacity of information and better imperceptibility.

1.2.2 Specific objectives

The specific objectives of the project are:

- To develope a new algorithm for steganography
- To Collect data set for testing (used Benchmark data set)
- To evaluate this algorithm through measuring capacity, robustness and imperceptibility compared with previous work.

1.3 Scope and Limitations of the Research

- This algorithm focuses on RGB image (extention PNG, BMP) as a cover medium.
- Using pixel indicator technique.
- Using LSB technique for hiding data.
- The performance (speed) is not considered in this work.
- Steganalysis is out of the scope, but will be used for testing robustness.

1.4 Thesis Structure

The thesis consists of chapters orderly concering the objectives of the research.

Chapter 1 (Introduction): gives an introduction about the steganography, the algorithm, research problem, and objectives.

Chapter 2 (Theory background) : describes the concepts of steganography, steganography types, the technique of steganography , explained steganalysis techniques and classified type of steganalysis and tools that can be used to measure steganography.

Chapter3 (RelatedWork): presents related works on steganography, image steganography, image steganography based on pixel indicator.

Chapter4 (Proposed Algorithm) : presents the Proposed Algorithm and how it is implemented (methodology).

Chapter 5 (Experimental Result): presents an evaluation of ST_R-indicator algorithm by the number of experiments on the algorithm.

Chapter6 (Conclusions and Future work) : presents the conclusions and the prospective future works.

Chapter 2
Theory background

Chapter 2
Theory background

This chapter introduces a general background of steganography as a method of covert communication. It describes different types of files that can be used as cover files, presents the technique of steganography, explains how to embed a secret message inside the cover file and explains steganalysis techniques and classified types of steganalysis. Finally it presents tools that can be used to measure steganography.

2.1 Steganography

Security of information is a significant issue of information technology and communication issues. It locates in the privacy of its existence and/or the privacy of how to decode it. Cryptography, watermarking and Steganography can be used in information security. The cryptography techniques hide secret information by encrypting it using encryption key (s). The output of encryption is chipper text or the secret information in unreadable format. This may draw the attention of attackers to the existence of confidential information. Digital watermarking is the process of embedding information into digital multimedia content so that the information (watermark) can be extracted or detected for different purposes including copy prevention and control. The proposed method of information security in the thesis is steganography(HUSSEIN, 2015).

Steganography is the art of hiding information by different ways which avoid the discovery of hidden messages. Steganography, derived from Greek, literally means "covered writing" (Greek words "stegos" meaning "cover" and "gratia" meaning "writing")(Das & Tuithung, 2012).

A steganographic system involves a cover media into which the secret information is embedded. The embedding process produces medium stego replacing information with data from hidden message. To hide the information, steganography gives a great opportunity in such a way that no one can know the existence of a hidden message.

The aim of steganography is to maintain its own information undetectable (M. Karim, 2011).

In steganographic model, message is the data that the sender desires to keep confidential. It can be plain text, cipher text, another image, or anything that can be embedded in the bit stream, such as the copyright, secret communications, or a serial number known password as stego key, which ensures that the only receiver that Learn to decipher the key to be able to extract a message from the cover object, and then the cover object with a message embedded is called the stego object. The Figure 2.1 Shows the Steganographic Process Model

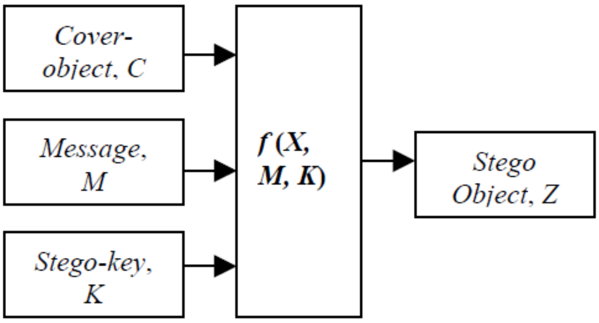
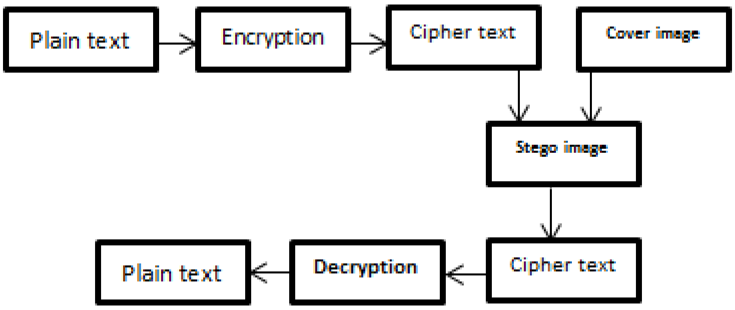


Figure (2.1): Steganographic Process Model(Barhoom & Mousa, 2015)

On the other hand, cryptography is not concerned with hiding the existence of a message, but its meaning through a process called encryption.The word cryptography derived from the Greek word kryptos, meaning ’hidden’(Challita & Farhat, 2011). Its method used for secure communication(Thangadurai & Sudha Devi, 2014).
Nowadays Cryptography is a significant research area where the scientists develop some good encryption algorithm to protect encrypted message from intercepting by intruders. There are two types of classical cryptographic, the first type is the symmetric key cryptography: it useses the same key for encryption and decryption operation. The second type is the Public key cryptography that used one key for encryption and another key used for decryption. (Chatterjee et al., 2011).

Cryptography and Steganography techniques are well known and widely used to cipher or hide information (Raphael & Sundaram, 2011). Figure 2.2 shows the integration of cryptography and Steganography



Figure(2.2): Integration of cryptography and steganography(Thangadurai & Sudha Devi, 2014)

The main objective of steganography is to avoid the attention to the transmission of hidden information. If uncertainty occurred, then hackers will be noted that there is a change in the sent message and then they will try to know the hidden information. (Wu et al., 2010).

2.1.1 Types of Steganography

Steganography ensures the confidentiality of data objects within the digital carriers such as images, audio and video so that can not easily be detected by a human visual system (HVS).

There are two ways for the general classification of steganographic systems. The first is based on the type of cover file, while the second approach is based on a method of hiding data(Al-Mohammad, 2010).

2.1.1.1 Cover Type

There are five types of steganography according to the object which is used for embedding secret data. These types are briefly described as given in Figure2.3 (Muhammad et al., 2015).

1. **Text steganography**: in a text file hiding information is the most common method of steganography. It hides a secret message into a text message. The appearance of the Internet and different types of digital file formats has a little importance. Text steganography by digital files is not used very often because text files have a very small amount of surplus data.

2. **Image steganography**: Images are used as a popular cover object for steganography. The message was embedded in a digital image using an algorithm,

using a secret key. It is sent resulting stego image to the receiver. On the other hand, it is processed by the extraction algorithm.

3**. Audio steganography:** is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication, transmission security and robustness are essential for the transfer of vital information for the intended sources while denying access by unauthorized persons. Therefore, an audible sound can be inaudible in the presence of another louder audible sound. This feature allows selecting the channel to hide the information. Audio steganography software can embed messages in WAV and MP3 sound files.

4. Video steganography: is a technique to hide any type of files in any extension into a carrrying Video file.

5. Protocol steganography: used for embedding information within network protocols such as TCP/IP. Information will be hidden in the header of a TCP/IP packet in fields that can be either optional or never used (Devi, 2013).

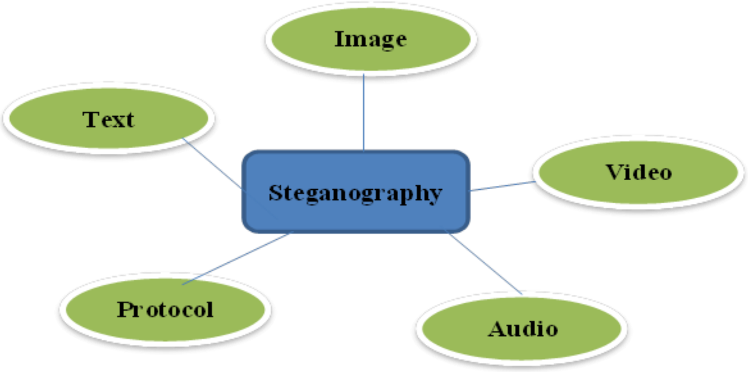


Figure (2.3): Types of Steganograph

2.1.1.2 Method of Hiding Data

Hiding information can be classified according to the method used to hide secret data. Moreover, this approach of classification in steganography is the most preferred in the research community approach for hiding the information, there are three different ways to hide secret data in a cover files: insertion-based, substitution-based and generation-based method.

1. Insertion-Based Method

Insertion-based method hide data in sections of a file that have been ignored by the processing application and not to modify bits that define that the contents are relevant to the end user file(Weiss, 2012). This method inserts secret data within the cover file, also stego file size will be larger than the cover file size. The main advantage of this method is that the contents of the cover file will not change after the embedding process because this method depends on the accumulation or to add the secret data to the cover file(Al-Mohammad, 2010).

2. Substitution-Based Method

In a Substitution-based algorithm, , it is replaced by the most insignificant bit of information that identifies the original content of the file with the new data in a way that causes the least amount of distortion. However, the file size does not change during the implementation of the algorithm, and the amount of data that can be hidden includes unlimited amounts of insignificant bits in the file.(Al-Mohammad, 2010; Weiss, 2012).

3. Generation-Based Method

This method does not need a cover file like insertion and substitution methods, it uses secret data to generate a suitable stego files. This steganography detection technique is based on comparing cover files with stego files. One advantage of this method is to prevent such kind of detection. So the major limitation of this method is that there are limited stego files that can be generated. Moreover, the generated stego files might be unrealistic files for end users (e.g. an image contains different shapes and colours without any sense or a text without any meaning)(Al-Mohammad, 2010).

2.2 Image steganography

Image steganography focused on hiding data inside cover images. Images have a lot of visual repetition in the sense that eyes does not usually care about changes in color. One can use this redundancy to hide the text, audio or image data inside cover images without making significant changes to the visual perception. Nowadays Image steganography become popular on the internet, a steganographic image looks like any other image, it has less attention than an encrypted text and a secure channel(Gupta & Garg, 2010).

2.2.1 Image definition

The image is a collection of numbers that includes different light intensity in different parts of the image (Johnson & Jajodia, 1998). These numeric representation forms, grids and individual points are referred to as pixels. Most of the image on the Internet consists of a rectangular pixel map of the image (represented by bit), where each pixel is located and its color. The presentation of these pixels is horizontally (row by row). The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current colour is 8 and this means that there is an 8-bit used to describe the color of each pixel.

Greyscale image uses 8 bits per pixel and capable of displaying 256 different colors or shades of gray. Typically digital color images in 24-bit files are stored, and RGB color model is used which is also known as true color. All the color variations of the pixels of the 24-bit image are derived from the three main colors: red, green and blue. Then they are represented by all the primary colors by 8-bit(Barhoom & Mousa, 2015).

2.2.2 Image compression

Compression techniques must be integrated to decrease the image’s file size by using mathematical formulas to analyze and compress the image data in smaller file sizes. (Morkel et al., 2005).

In an image, there are two types of compression: lossy and lossless compression.

Lossy compression reduces a file by eliminating redundant information. When the file is uncompressed, only a part of the original information is still there. It is expected to be something like the original image, but not the same as the original. Example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group)(Devi, 2013).

Lossless compression it does not remove any information of the original image, but instead it represents data in mathematical formulas. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most popular image that use lossless compression are GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file)(Morkel et al., 2005)

2.3 Image Steganographic Techniques

Steganographic techniques are separated into two categories of domain:

1. **Spatial domain techniques:** Spatial domain techniques to deal directly with the pixels of the image.Pixel values are changed for enhancing desired. Spatial domain techniques such as the logarithmic transforms, power law transforms, histogram equalization, depend on the direct manipulation of pixels in the image. This technique is useful for changing directly the values of individual pixels and hence the overall contrast of the entire image. But they usually promote the full image in a uniform manner and produced in many cases undesirable results. It is not possible to selectively edges or other required information effectively(S. Sharma & Kumar, 2013).
2. **Transform domain technique:** Transformation / frequency domain techniques to manipulate the image in the orthogonal transform domain rather than the image itself. It is suitable for processing image according to the frequency content.The principle behind the Transformation domain of image enhancement consists of computing a 2-D discrete unitary transform of the image, for an instance of 2-D DFT, manipulation of transfer by the operator M, and then performing the inverse transform. Orthogonal transform of the image has two components phase and magnitude. The phase is used to restore the image back to the spatial domain and the magnitude consists of the frequency content of the image. (S. Sharma & Kumar, 2013).

2.4 LSB Based Data Hiding Technique

The most popular and simplest Steganography technique is the Least Significant Bits (LSB). It embed in the secret messages directly. In this technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding (M. Islam et al., 2014). This example shows how the character **A (10000001)** can be hidden in the first eight bytes of three pixels in a 24-bit image.

Table (2.1): Data hiding using LSB

X: The Pixels before the embedding process		
00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001
Y: The resulting after the embedding process		
00100111	1110100**0**	11001000
0010011**0**	11001000	1110100**0**
11001000	00100111	11101001

The three bits are the only three bits that actually change. LSB requires on average that only half the bits that are changed in an image. The 8-bit character A only requires 8 bytes to hide it in cover object. The 9 byte of the three pixels can be used to hide the next character of the hidden message.

There are many advantages of the Least-Significant-Bit (LSB) steganography, it is simple to understand, easy to implement, produces stego-image that is almost similar to cover image and its visual infidelity cannot be tried by the naked eyes.

A good technique for image steganography includes three aspects, the first one is capacity (hide the maximum data inside cover image) and the second is the imperceptibility (quality of stego image after data hiding) and the last one is robustness. This technique is good imperceptibility, but the capacity of hidden data is low because the use of only one bit per pixel to hide the data. It is also not robust because it can be retrieved easily as a secret message and the image can be detected that it has some hidden secret data by retrieving the LSBs (Akhtar et al., 2013).

2.5 Pixel Indicator Technique:

The Pixel Indicator Technique (PIT) is used for steganography by using RGB images as a cover media. This technique useses at least one or two bits of one of the red channel as an indicator of the existence secret data in the other two channels. The selected indicator is in R channel.

They have selected the indicators in Red channel. Channel 1 is the Green and channel 2 is the Blue. The sequence embedded is GBR or BGR.

2.6 Characteristics feature of Data Hiding Techniques

The key properties that must be considered when using data hiding techniques are: Figure 2.4 shows the Measurement triangle of steganography

Imperceptibility: Imperceptibility is the property of which the person is unable to differentiate between the original image and stego image.

Capacity: the amount of secret data that can be embedded without deterioration of image quality

Robustness: Degree of difficulty required to destroy information embedded without destroying the cover image (Sumathi et al., 2014).

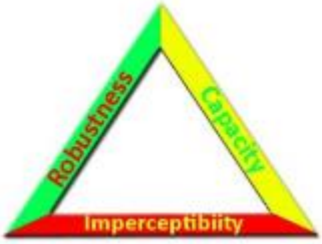


Figure (2.4): Measurement triangle of steganography(Altaay et al., 2012)

2.7 Steganalysis

Steganalysis is the science of detecting hidden data in the cover media files, it is emerging in parallel with steganography (Meghanathan & Nayak, 2010) The objective of steganalysis is to brake steganography and detect stego image. Almost all steganalysis algorithms based on steganographic algorithms introduce statistically differences between the cover and stego image (Devi, 2013).

There are two main classifications of Steganalysis: **targeted**, and **blind**(Bateman & Schaathun, 2008).

2.7.1 Targeted Steganalysis:

Targeted Steganalysis consists of three different types:

- **Visual attacks** it discovers the hidden information and separates the image into bit planes for more analysis.
- **Statistical attacks** Consists of two types; passive or active, the passive attacks determining the presence or absence of a secret message or embeds the algorithm used, and the active attacks investigate embedded message length or message hidden location or secret key used in embedding.
- **Structural attacks** It changes the format of the data files as the data to be hidden and embedded, identifying these changes characteristic structure can help us to find the presence of an image or text file (Devi, 2013).

2.7.2 Blind Steganalysis

Blind steganalysis is the process of performing steganalysis without any knowledge about the cover media used.

Blind steganalysis doesn't know the algorithm and the cover image that is used to produce a suspect image. It trys to assess the possibility of attacks included by depending on data from the suspicious image.These approaches are most common in the steganalysis because steganalyst knows much about the image which can be extracted from the image itself (Bateman & Schaathun, 2008).

2.8 Tools used to measure steganography

There are several tools available to be used to evaluate steganography such as:

2.8.1 Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)

PSNR and MSE are the most common and widely used metrics for image quality evaluation(Al-Mohammad, 2010). The fist one,PSNR, measures the similarity between the two images (how two images are close to each other), while MSE measures the difference between two images (how two images differ from each other)(Al-Mohammad, 2010). Therefore, image quality is better with higher values of PSNR and smaller values of MSE. The best image quality is when MSE value is very small or going to be zero, the difference between the original image and the stego image is negligible(Al-Mohammad, 2010). For PSNR, the higher PSNR value is the better degree of imperceptibility, since the similarity between the original image and the stego image is high. For example, it is difficult to recognize any difference between a grey-scale cover image and its stego image if the PSNR value exceeds 40 dB(Al-Mohammad, 2010). PSNR and MSE are defined as follows(Al-Korbi et al., 2016) .

$$PSNR = 10 \times \log 10(\frac{n^2}{MSE}) \qquad (2.1)$$

Where n is the maximum pixel value for 8 bits.

$$MSE = \frac{1}{M \times N} \quad \sum_{i=1}^{m} \sum_{j=1}^{n} \left(J_{ij} - \widetilde{J_{ij}}\right)^2 \qquad (2.2)$$

Where:

J_{ij} represents the cover image dimensions

$J`_{\mathrm{ij}}$ represents the dimensions of the stegos image.

N and M are the width and the height of the image,

2.8.2 StegExpose tool for Detecting LSB Steganography

StegExpose is a steganalysis tool heading towards bulk analysis of lossless images like the Portable Network Graphics (PNG), Bitmap format (BMP).

This tool is measured by three basic criteria, speed, accuracy and practicality. Speed means the average time it takes to analyze a file, accuracy means the performance binary classifier. The practicality means the ability of analysing files in bulk, resulting in a detailed report steganalytic on all processed files.

2.9 Summary

This chapter introduces the background of steganography, steganographic model. The main file types which have been discussed can be used for steganography as a cover medium. Particularly images steganography which are the main role of this work. It explained steganography techniques and how we embed a secret message within a cover file like LSB which can be used as an adation to pixel indicator techniques to add more randomization. Then, we have investigated steganalysis and types of steganalysis. Finally, presented tools can be used to measure steganography like **PSNR**, **MSE** and **StegExpose** which can be used to evaluate these most important aspects; Imperceptibility, Capacity and Robustness.

Chapter 3
Related work

Chapter 3

Related work

This chapter introduces many research works which has been conducted in Steganography. For the purpose of secured secret image embedding, these works are introduced and analyzed in relation to the research problem to show how these works address the problem of our research requirements. Parts of these relevant works can be considered as basis to solve the problem of the research. They focus on Image steganography based on LSB pixel indicator. The followings are some relevant works carried out by different research groups: LSB image Steganography and Image steganography based on LSB indicator.

3.1 LSB Image steganography:

Techniques of this method modify pixels at the image to hide secret information. Images are considered to be the best cover objects to hide information because it contains a large amount of redundant bits.

Many researchers proposed approaches to enhance LSB-based image steganography.

Researchers (M. Islam et al., 2014) using the LSB to hide data depending on the filtering basis of the algorithm. This filtering requires knowledge of any pixel is more, pixels lighter or darker, by checking three MSBs of pixels. And it is embedding done in the dominant area. They also suggested encrypting data using the ASE before the embedding process in order to add randomness to the process of hiding by using the LSB.

Researchers (Akhtar et al., 2013) implemented Steganography for images, with improving both security and quality of the image. A variation of the (Least Significant Bit) LSB algorithm had been performed to improve the quality of stego image by using bit inversion technique. In this technique, some of the least significant bits of the cover image are inverted after hiding the LSB information that coincides with some pattern from other bits, and it reduces the number of LSBs adjusted. Thus, this causes a change in the number of the least significant bits of the cover image in comparison with the plain method of LSB. In addition, it improves

PSNR of stego image. By storing the bit patterns of the inverted LSBs, message image can be obtained correctly. To improve the robustness of steganography, RC4 algorithm is used to achieve randomization in hiding message at the cover image instead of being stored sequentially.This process disperses bits of the messeage in a random way in the cover image. Therefore, it becomes difficult for unauthorized people to extract to the original message. This method appears to promote good technique Least Significant Bit to look at security as well as image quality.

Researchers (Ren-Er et al., 2014) presented image steganography along with the pre- processing DES encryption.When transferring secret information, first, encrypt information is designed to be hiden by DES encrypted, then it is written in the image through the LSB steganography. Encryption algorithm improves the corresponding minimum performance between the image and secret information by changing the statistical properties of the secret information to strengthen the fight against disclosure of image steganography.

Researchers (Das & Tuithung, 2012) provides a new technique to image steganography on the basis of Huffman coding and using an image of two 8-bit gray level of the size M X N and P X Q as the cover image and the image of a secret respectively. The Huffman coding is implemented over the image secret / message before embedding, and each bit of the Hoffman code of secrecy message /image becomes inside the cover image by changing the least significant bit (LSB) for each of the pixel intensities of the cover image.

Researcher (Khalil, 2011a) presented a process of hiding short audio message into digital images by encrypting audio message before hiding it in the image file.

Researchers (V. K. Sharma & Shrivastava, 2012) introduced a new algorithm for the steganographic to 8bit (gray) or 24 bit (color image), on the basis of the logical operation. The algorithm embedded MSB of secret image in to LSB of cover image. In this n LSB of the cover image, the bytes are replaced n MSB secret image.stego image quality of the image can be greatly improved with low additional computational complexity.

Researchers (S. M. Karim et al., 2011) proposed a new way to hide secret data in a green or blue channel of the image carrier on the basis of secret key bits and red channel LSB.This is done in more than one level security method which are added to the existing LSB technique through the use of the secret key. And xored red channel LSB bit with secret key then a decision is made on the basis of the result of the replacement of LSB of the green or blue channel .The proposed method has the same payload, better security and more robustness is compared to simple LSB method. However keys secure exchange of the secret key is a challenge at the overload of the proposed method.

Researchers (Barhoom & Mousa, 2015) used LSB to hide the data that Presented algorithm to 8bit (grayscale) or 24-bit (color image), also suggested to encrypt data using the blowfish encryption algorithm before embedding process. To improve the security and quality of the image, the algorithm has a high capacity and well invisibility.

3.2 Image steganography based on LSB indicator

Researcher (Gutub, 2010) proposed more powerefull technology by using one channel while using the other two channels to embedding secret data in a predetermined manner cycle. This enhances the robustness of the proposed method. Experimental results showed a high capacity and better imperceptibility of the proposed algorithm. This method also avoids excessive key exchange.

Researchers (Laskar & Hemachandran, 2013) algorithm embeds data in the red channel of the image pixel and useses a random number generator.It is impossible to observe the changes in the image. It uses stego key (pseudo-random number generator) PRNG to determine the location of the pixels. This paper focuses on increasing the security of the message and reducing the distortion ratio.

Researchers (Swain & Lenka, 2012) proposed a method of steganography technique in the RGB channel steganography based on the RSA algorithm which is used to encrypt and decrypt. In the RGB image, each pixel (24-bit) is the presence of R channel 8-bit, channel G 8-bit and B channel 8-bit.The image is divided into 8 blocks and encrypted text is divided into eight blocks.One block cipher in allocated to be embedded in a block of only one image by the user subkey definition. The three channels of each pixel of one image is used as a channel indicator.Channel indicator for different blocks are not the same. It useses two other channels (called data channels) to hide encrypt text bits in 4 (LSB) least significant bit position. The data channel can be embedded in four (4) bits of the text cipher if the embedding change in the pixel value is less than or equal to 7. Two LSBs of indicator will know whether the encrypted text embedded into a one data channel only, or in both data channels, so that recovery can be made accordingly in the receiver. But pixel indicator techniques was a drawback to treat all the components of red, green and blue alike, but in the actual contribution of the red, green, blue components are not the same for visual perception. Therefore, it is introduced as a constituent approach.

Researchers (Goel et al.) presents lossless data hiding approach for hiding the text in color image. We use integer wavelet transform (IWT), LZW compression and Modified pixel indicator technique, for the ability to achieve high-hiding capacity and good visual quality.

Researchers (Kukapalli et al.) presents a promote pixel index method (PIM) by comparing the three of the MSB bits in each pixel to embed data. We also use the Blowfish algorithm to convert the message into cipher text. Using a combination of two of these techniques we can achieve more complexity.

Researchers (Tiwari & Shandilya, 2010) used two methods for RGB image steganography. The first one is the pixel indicator technique and the other is a triple algorithm. They use the same principle of LSB, where the secret is hidden in the least significant bits of pixels, with more randomization in the selection of the number of bits used and the color channels that are used. It is expected to increase the security of the system, as well as increasing the capacity of this randomization.

Researchers (Al-Korbi et al., 2016) presents algorithm steganography which is highly efficient and able to hide the large size of diverse data (text, binary images, color image or a combination of these types of data) in the cover image and useses the Haar wavelet transform. It converts an image of the spatial domain to the frequency domain by applying horizontal and vertical operations, respectively.

3.3 Related work Discussion

Many researches had been mentioned to improve the security of steganography. Each one of them has its own way of hiding and involves some of the advantages and disadvategese in hiding data. The elimination of threats and attacks in steganography also can not be solved, so we proposed a new algorithm for data hidden in an RGB image based on pixel indicator LSB steganography.This new algorithm has been compared with other algorithms and experimental results to show the power of the new algorithm in hiding and extracting data with a high storage capacity(payload) and without being evident or being discovered with electronic techniques (high robustness) and better imperceptibility (image quality after embedding data).

Table (3.1): summary of the most related work to this work

Research Name	Description	Short come
Pixel indicator technique for RGB image steganography 2010	This technology is presented more powerful since it uses one channel while using the other two channels to embed secret data in a predetermined manner cycle. This enhances the robustness of the proposed method.	Medium capacity (payload) • Using indicator more increase capacity. • Two least significant bits of one of the channels red, green or blue as an indicator of the existence of secret data in other two channels. Better imperceptibility • stego image after applying the PIT algorithm using 2-bit LSB did not release any visual difference identified High robustness • Much randomization
Steganography based on Random Pixel Selection for Efficient Data Hiding 2013	This algorithm embeds data in the red channel of the image pixel and useses a random number generator.It is impossible to observe the changes in the image. It used stego key (pseudo-random number generator) PRNG to determine location of the pixels.	Medium capacity (payload) • Embedded data only in the red channel of the image high imperceptibility • impossible to observe the changes in the image high robustness • adds more Randomization • using key

A Novel Approach to RGB Channel Based Image Steganography Technique 2012	RSA algorithm is used for encrypt and decrypt.In the RGB image, each pixel (24-bit) is the presence of R channel 8-bit, channel G 8-bit and B channel 8-bit.The image is divided into 8 blocks and encrypted text is divided into eight blocks. one block cipher is allocated to be embedded in a block and only one image by the user subkey definition. the three channels in each pixel of one image is used as a channel indicator.Channel indicator for different blocks are not the same. It useses two other channels (called data channels) to hide encrypt text bits in 4 (LSB) least significant bit position. the data channel can be embedded in four (4)bits of the text cipher if after embedding the change in the pixel value is less than or equal to 7. Two LSBs of indicator know whether the encrypted text embedded into a one data channel only, or in both data channels	Very high capacity (payload) The embedding into channel1 or /and channel2 is done by difference calculation of 4 data bits and 4 LSBs high imperceptibility high robustness • much Randomization • Using RSA for encryption and decryption adds more secure
High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator Technique 2014	Presents lossless data hiding approach for hiding the text in color image. We use integer wavelet transform (IWT), LZW compression and Modified pixel indicator technique, for the ability to achieve high-hiding capacity and good visual quality.	High Capacity (payload) • 3bits embed or 1 bits embed based on MSB frequency coefficients value good imperceptibility • apply optimal pixel adjustment procedure (OPAP) after embedding the Secret message. high robustness • much randomization • using LZW compression
Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare 2014	It is presented to promote Pixel Index Method (PIM) by comparing the three of the MSB bits in each pixel to embed data. We also use the Blowfish algorithm to convert	Medium Capacity (payload) • Uses two bits inserted inside two least significant bits of a specific color . High Imperceptibility • Embed message bits in two least significant bits, the message will be hard to detect and changes in image will be small .

	the message into cipher text. By using a combination of two of these techniques we can achieve more complexity	High robustness • Using Blowfish algorithm add more secure. • Indicator used adds more randomization
Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm- An Incremental Growth 2010	Used two methods for RGB image steganography. The first is pixel indicator technique and the other is a triple algorithm. They use the same principle of LSB, where the secret is hidden in the least significant bits of pixels, with more randomization in the selection of the number of bits used and the color channels that are used. It is expected to increase the security of the system, as well as increasing the capacity of this randomization.	High Capacity (payload) • Triple algorithm has maximum capacity ratio better than the pixel Indicator • Adds more randomization Good Imperceptibility • Visual change between the original image and stego image can not predict. However, the differences between the images before and after hiding the data can be sensed through histograms Low robustness • The robustness of algorithm is not investigated thoroughly
Highly Efficient Image Steganography Using Haar Dwt For Hiding Miscellaneous Data 2016	It is a highly efficient algorithm steganography which is able to hide the large size of diverse data (text, binary images, color image or a combination of these types of data) in the cover image and using the Haar wavelet transform. It converts an image of the spatial domain to the frequency domain by applying horizontal and vertical operations, respectively.	High Capacity (payload) • hiding a large size of diverse data (text, binary images, coloured images or a combination of these types of data in cover image • Measuring the high PSNR and low MSE high Imperceptibility • Measuring the high PSNR and low MSE high robustness • colour images and texts are not affected by the attacks

3.4 Summary

This chapter presents a number of related works in LSB image Steganography and Image steganography based on LSB indicator.

The table (3.1), is the most related work to this work. We can conclude that this work works on the idea of touching terms of (capacity, robustness and Imperceptibility) of the use of steganography, but we will focus on the Image steganography based on LSB indicator. Additionally these works suffer from capacity, robustness and imperceptibility and used backword steganography. These weaknesses are the focus of this work by bideriction hiding forword and backword in each pixel and by resulting more rooms and more randomization.

Chapter 4

Proposed Algorithm

“ ST_R-indictor ”

Chapter 4
Proposed Algorithm

In this chapter the proposed algorithm has been presented, we call it ST_R-indicator, and then the methodology of how to implement it. This algorithm for hiding data in RGB image Extention BMP , PNG as a cover medium. This algorithm contain two parts: hiding and retrieving message using LSB technique to hide and retrieve secret data into the least one or two bits by depending on pixel indictor technique .

4.1 Proposed Algorithem: ST_R-indicator steganography algorithm

In this algorithm for hiding data we hide the secret data bits into the least one or two bits (rightmost bits), this process is done based on indicators we call it R-indicator. We use an Indicator Select (IS) to determine the byte G or B into which we embed the secret bit(s) first and another indicator (Indicator Number of bit IN) to determine how many bits to embed at a time. The indicator (IS) is a bit that is chosen randomly after computeing the weight of the byte in Red channel of the RGB channel other than the least two bit, the third and eight bit.

The indicator (IS) chosen randomly from the bit is set between (4-7) within channel Red. The bit (1, 2, 3, 8) has been excluded because the first bit has no previous bit, the eighth bit has no next bit, and the first and the second bit are used to contain the secret data. The third bit excluded because it will change the value from zero to one or one to zero that are affecting the data retrieval process. We call this algoritm ST_R-indictor steganography algorithm.

To clarify the ST_R-indicator let's assume this byte **10110001** that compute the indicator (IS) , the first bit will not be chosen because it has no previous bit , if the second bit (0) changed from 0 to 1 this will affect the retrieval data, the eight bit 1 has no bit next.

We select the indicator (IS) firstly and compute the Weight (w) of the byte from the fourth bit to the seventh bit in the Red channel , suppose the Weight w(C)= 16+32=48 that is between 32 and 64 let assume w(A)=32 and w(B)=64

128	64	32	16	8	4	2	1
1	0	1	1	0	0	0	1

If the weight from fourth to seventh bit is zero, then the indicator fourth bit is selected.

Otherwise if the weight from fourth to seventh bit 64 or above, the indicator seventh bit is selected.

Else if (w (B) - w(c) = w(c) - w (A) or w (B) - w(c) < w(c) - w (A))

IS = **B**

Else if (w (B) - w(c) > w(c) - w (A))

IS = **A**

Where **IS** is the indicator, **B** is the seventh bit, **A** is the sixth bit

C is the weight of the byte.

after selecting the indicator(IS) , we will hide in the G or B channel depending on the next bit of the indicator and the previous bit before this indicator which will make the XORed operate for both the indicator with the next bit then the result of all this will make the XORed with the previous bit. If the value is zero, our current secret bits will be embedded into the Green channel and if the value is 1, our current secret bits will be embedded into the Blue channel. Then it will be hiden in the R channel (as shown in Table 4.1).

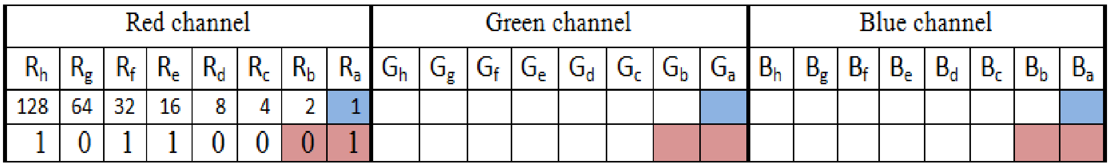
Also through the process of hiding, we don't always embed only one bit at a time, we may embed one or two bits into the RGB channel. This can be done depending on another indicator (IN). The value of previous bit(IN_G) from the indicator IS (embedded into Green channel depending on the value of the next bit for the indicator IS) and next bit (IN_B) from indicator IS (embedded into blue channel depend on the value of the previous bit for the indicator IS). let's assume that the next and previous bit which tells us how many secret bits to embed at a time in the Green and the Blue channel, If the value is 0, we embed only one bit, and if it is one, we embed two bits . After that, the embedded will be in the Red channel depending on the indicator IS value. If the value is zero, the embed will be only one bit, and if it is one, then we embed two bits.

This process adds more randomness to the process of hiding because it is not a fixed amount of bits that can be embedded and not just forward but forward and backward, So we can not determine the number of bits embedded in each byte without checking the indicator.

On the other hand, this process increases the capacity of the hiding process more than the LSB, which included only one bit at a time and this is another advantage besides the random increasement which making it difficult to retrieve the secret data by unauthorized parties.

Let's assume the byte (pixel)

Table (4.1): represented the pixel



Red channel								Green channel								Blue channel							
R_h	R_g	R_f	R_e	R_d	R_c	R_b	R_a	G_h	G_g	G_f	G_e	G_d	G_c	G_b	G_a	B_h	B_g	B_f	B_e	B_d	B_c	B_b	B_a
128	64	32	16	8	4	2	1								🟦								🟦
1	0	1	1	0	0	0	1							🟥	🟥							🟥	🟥

4.1.1 ST_R-indicator Algorithm

This algorithm contain two part embedding and extracting algorithm

4.1.1.1 Embedding Algorithm (as shown in Figure 4.1):

Step 1: Computing the IS which will be not the first, second, third and eighth bit (R_a, R_b, R_c, R_h) in the red channel.

Suppose the byte, the indicator IS will be once of R_d, R_e, R_f, R_g

$(0*2^3+1*2^4+1*2^5+0*2^6\ ) = 48= w(c)$

if $(w(R_g) - w(c) = w(c) - w(R_f)$ or $w(R_g) - w(c) < w(c) - w(R_f)\ )$

IS = R_g

Else if $w\ (R_g) - w(c) > w(c) - w\ (R_f)$

IS =R_f.

Suppose the indicator is IS, Indicator Number of bit IN_G , IN_B

IS = R_g

$IN_G = R_f$

$R_h\ =\ IN_B$

Step2: if $((R_g \oplus R_h\ ) \oplus R_f\ ) = 1$

Embedded the secret pixel of image in **B** channel

Else embedded the secret pixel of image in **G** channel

Step3: if (R_h =1) embed two bits at G_a , G_b

Else embed one bit at G_a

If (R_f =1)

Embed two bits at B_a , B_b

Else embed one bit at B_a

Step4: If (IS = 1) embed two bits at R_a , R_b

Else embed one bit at R_a .

Where R_a, R_b the least two bit in the red channel

G_a , G_b the least two bit in the Green channel

B_a , B_b the least two bit in the Blue channel

IS indicator selection

IN_G Indictor number for previous bit from the indicator IS

IN_B Indictor number for next bit from the indicator IS

IS : indicator selection

IN_G : indicator number of bit can be embedded / retrieved (previous bit for IS)

IN_B : indicator number of bit can be embedded / retrieved (next bit for IS)

Ih = the result of XOR for ((IN_B $\oplus$IS) $\oplus$$IN_G$)

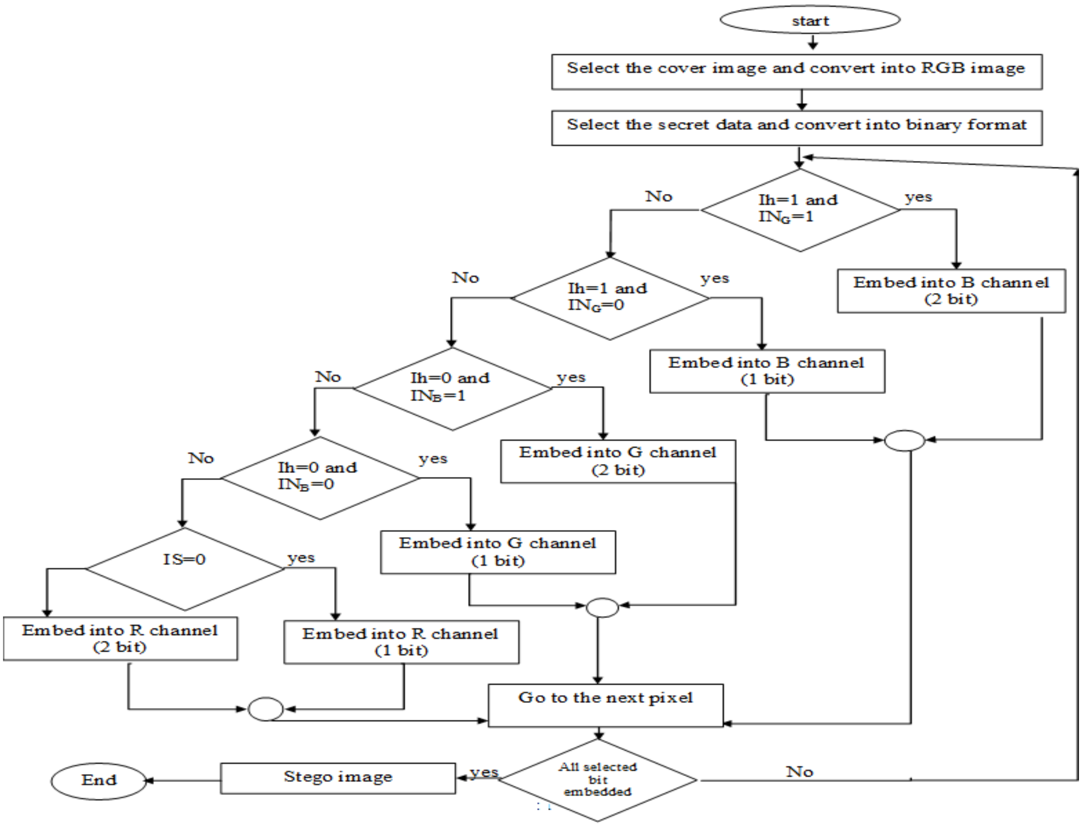

start
Select the cover image and convert into RGB image
Select the secret data and convert into binary format
No
Ih=1 and ING=1
yes
Embed into B channel (2 bit)
No
Ih=1 and ING=0
yes
Embed into B channel (1 bit)
No
Ih=0 and INB=1
yes
Embed into G channel (2 bit)
No
Ih=0 and INB=0
yes
Embed into G channel (1 bit)
IS=0
yes
Embed into R channel (2 bit)
Embed into R channel (1 bit)
Go to the next pixel
All selected bit embedded
yes
No
Stego image
End

Figure (4.1): flow chart for hiding data

4.2 Example to hide secret data using ST_R-indicator:

Suppose we want to hide the following bits **01101011,01011101,10110111** into the RGB channel using indicators-based LSB Algorithm, as we see the hiding process is not sequentially like LSB. The secret bits are hidden into cover bytes randomly based on the values of the indicator bits of the cover bytes.

Table (4.2): Example of hiding Data using pixel Indicators based LSB

X: The byte before embedding process:		
R(0)	**G(0)**	**B(0)**
1**0**110001	01001100	01001101
R(1)	**G(1)**	**B(1)**
1**1**010110	10100101	11010100
R(2)	**G(2)**	**B(2)**
100**1**0111	10101001	01010100
R(3)	**G(3)**	**B(3)**
0**1**011010	00101100	11001101
R(4)	**G(4)**	**B(4)**
0000**0**111	11010010	01101001
R(5)	**G(5)**	**B(5)**
1000**1**001	10110010	11010111
Y: The result bytes after embedding process:		
R(0)	**G(0)**	**B(0)**
1011000[0]	010011[11**]**	010011[10**]**
R(1)	**G(1)**	**B(1)**
110101[01**]**	101001**[11)**	1101010**(0)**
R(2)	**G(2)**	**B(2)**
100101**[01)**	1010100**(1)**	0101010[**1**]
R(3)	**G(3)**	**B(3)**
010110(11]	0010110**(0)**	1100110**(1)**
R(4)	**G(4)**	**B(4)**
0000011**(1)**	1101001[**1**]	011010**(01)**
R(5)	**G(5)**	**B(5)**
10001001	1011001[**1**]	1101011**[0]**

X: Container bytes before embedding,
Y: Container bytes after embedding
IB : Indicator byte : where to embed (R,G, B), Ic: what to embed
(B) The new value of the bit is the same as the original
[b] The new value of the bit is different from the original
(Bb] Only the right bit new value is different from the original
[bB) Only the left bit new value is different from the original
(BB) Both new values are the same as the original
[bb] Both new values are different from the original

As we see in Table 4.2, the order of the cover bytes that were embedded into is G(0),B(0),R(0),G(1), B(1),R(1),B(2),G(2),R(2),B(3),G(3), (3), (4),G(4),R(4),B(5), G(5)and the amount of embedded bits in the same order is 2,2,1,2,1,2,1,1,2,1,1,2,2,1,1,1,1 . Here we can perceive that the hiding process is not sequential unlike LSB technique and some bytes contain only one secret bit and others contain two bits.

4.1.1.2 Extraction Algorithm (as shown in Figure 4.2):

Step1: Computing the weight of the red channel to select the indicator IS will not be the first, second, third and eighth bit.

Suppose the byte, the indicator will be once of R_d, R_e, R_f, R_g

$(0*2^3+1*2^4+1*2^5+0*2^6) = 48 = w(c)$

if $(w(R_g) - w(c) = w(c) - w(R_f)$ or $w(R_g) - w(c) < w(c) - w(R_f))$

IS = R_g

Else if $w(R_g) - w(c) > w(c) - w(R_f)$

IS =R_f.

Suppose the indicator is IS, Indicator Number of bit IN_G , IN_B

IS = R_g

$IN_G = R_f$

$R_h = IN_B$

Step2: if $((R_g \oplus R_h) \oplus R_f) = 1$

Get LSB of the secret pixel of image in B channel

Else Get LSB of the secret pixel of image in G channel

Step3: if (R_h =1) Get two bits at G_a , G_b

Else Get one bit at G_a

If (R_f =1)

Get two bits at B_a , B_b

Else Get one bit at B_a

Step4: If (IS = 1) Get two bits at R_a , R_b

Else Get one bit at R_a .

Where R_a, R_b the least two bit in the red channel

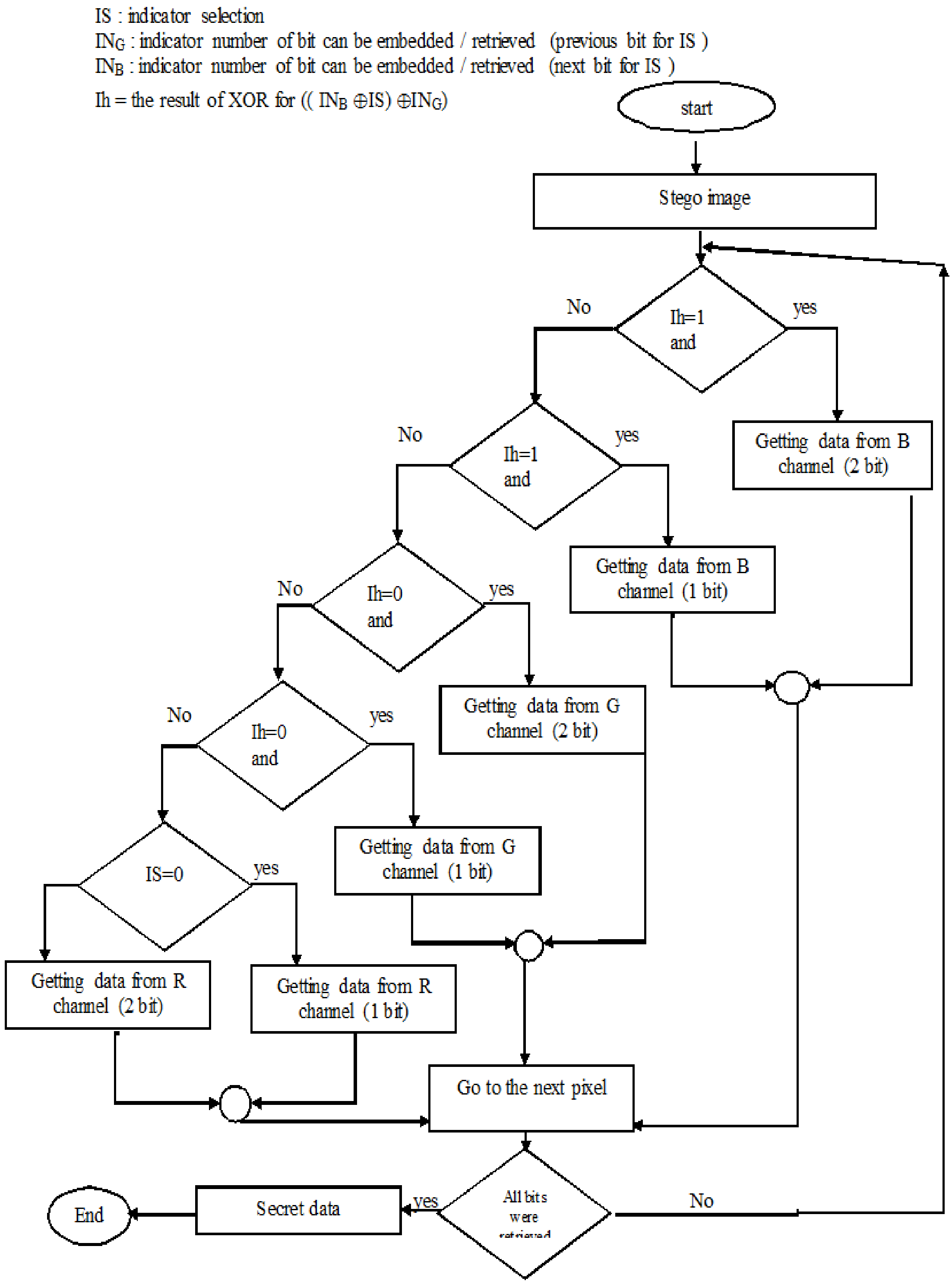
G_a , G_b the least two bit in the Green channel

B_a , B_b the least two bit in the Blue channel

IS indicator selection

IN_G Indictor number for previous bit from the indicator IS

IN_B Indictor number for next bit from the indicator IS



IS : indicator selection

IN_G : indicator number of bit can be embedded / retrieved (previous bit for IS)

IN_B : indicator number of bit can be embedded / retrieved (next bit for IS)

Ih = the result of XOR for (($IN_B \oplus IS) \oplus IN_G$)

start
Stego image
Ih=1 and
No
yes
Getting data from B channel (2 bit)
Ih=1 and
No
yes
Getting data from B channel (1 bit)
Ih=0 and
No
yes
Getting data from G channel (2 bit)
Ih=0 and
No
yes
Getting data from G channel (1 bit)
IS=0
yes
Getting data from R channel (2 bit)
Getting data from R channel (1 bit)
Go to the next pixel
All bits were retrieved
yes
No
Secret data
End

Figure (4.2): flow chart for retrieved hiding data

4.3 Example to extract secret data using ST_R-indicator:

Suppose the hidden byte in the previous example in table 4.2

Table (4.3): Example of Retrieve Data hiding using pixel Indicators based LSB

R		**G**		**B**	
R(0)	10110000	G(0)	01001111	B(0)	01001110
R(1)	11010101	G(1)	10100111	B(1)	11010100
R(2)	10010101	G(2)	10101001	B(2)	01010101
R(3)	01011011	G(3)	00101100	B(3)	11001101
R(4)	00000111	G(4)	11010011	B(4)	01101001
R(5)	10001001	G(5)	10110011	B(5)	11010110

As we see in table 4.3, the order of the cover bytes that were retrieved into are G(0),B(0),R(0),G(1), B(1),R(1),B(2),G(2),R(2),B(3), G(3), R(3), (4),G(4),R(4),B(5), G(5) and the amount of retrieve bits in the same order is 2,2,1,2,1,2,1,1,2,1,1,2,2,1,1,1,1 that bytes hidden 01101011,01011101,10110111.

Researches mentioned previously have mentioned ways to improve the security of steganography. Each one of them has its own way of hiding and involves some of the advantages and limitations. The most related works are (Gutub, 2010; Laskar & Hemachandran, 2013; Swain & Lenka, 2012; Tiwari & Shandilya, 2010). This work discussed the idea of touching terms of (capacity, robustness and Imperceptibility) of the use of steganography, but we will focus on the Image steganography based on LSB indicator. Additionally these works, suffers from capacity, robustness and Imperceptibility and used backword steganography. These weaknesses are the focus of this work by bideriction hiding forword and backword in each pixel and by resulting more rooms and more randomization.

ST_R-Indicator algorithm has been compared with other algorithms and experimental results and showed that the power of the new algorithm to hide and extract data has a high storage capacity (payload), described in chapter 5 in (section 5.2) and without being evident or being discovered with electronic techniques (high robustness) describe in (section 5.3) and better imperceptibility (image quality after embedding data) describe in (section 5.1).

4.2 Methodology

To accomplish the objectives of the research, the methodology of this research consist of the following phases (as shown in Figure 4.3):

1. **Develop the proposed** steganography algorithm that enable user to transfer hidden message between them securely.
2. **Implementation:** Java libraries (version 8.0.1) used to help us implement this algorithm. There are many functions that used in implementing this algorithm which are hide, embed, retrieve and extract methods which are showen in table (4.4). The speed of this algorithm can be done by tools of steganography like PSNR, MSE and StegExpose that can be used to evaluate the most important aspects: Imperceptibility, Capacity, Robustness.

Table (4.4): function used in implementation this algorithm

Function	**What are**
hide	Method to hide secret message in RGB image using ST_R-indicator algorithm
embed	Method to embed the secret bits in the cover byte
retrieve	Method to retrieve secret message image using ST_R-indicator algorithm
extract	Method to extract the secret bits in the cover byte

3. **Data collection**
   In this phase, we perform the steps as shown in Figure 4.4:
   - Determining the secret message that have characteristics like type (text messge), size (any size can be hidden but less than the size of cover media) to be embedded and convert into binary format.
   - Implementing of the algorithm that embed the secret data inside the RGB benchmark image with png, bmp extention with size 512×512. It is showed in table (4.5). Image jpge format is not used because theses images are lossy compession that reduces a file by eliminating redundant information. When

the file is uncompressed, only a part of the original information is still there. It is expected to be something like the original image, but not the same as the original.

- Find the result of the stego image and show the change in the original image.

Table (4.5): Benchmark image used

Image benchmark name	Type	Size
Leena	Png	512×512
Baboon	Bmp	512×512
Peppers	Bmp	512×512
Airplan	Bmp	512×512
Girl	png	512×512

4. **Testing**: we have used benchmark RGB image (png, bmp) format of data collection to show results for testing the proposed algorithm for hiding and retrieval data, the reason for choosing these images were being well known and used in the areas of digital image processing, compression and steganography, then we used other image from the internet (with png, bmp extention) as it is showen in (chapter 5) (table 5.9) of the effect of the Characteristics image on the robust image.
5. **Evaluation :**

In this phase, Experimental for collection data set for benchmark RGB image from the internet like (leena image, baboon image, peppers image, Airplan image and Girl imge ,with png, bmp extention) to measure:

- Size of the hidden messages to measure the percentage of the increment in the capacity over the normal LSB.
- Randomization.
- The quality of stego-image after data hiding (The change of the image)

Used Peak signal to noise ratio (PSNR) to evaluate the imperceptibility of stego images, and used as measure of quality image. The higher ratio of

PSNR is the better for the quality of the stego image. StegExpose steganalysis tool is used to measure the robustness of this method as described in (chapter 2 sections 2.6).

Then the researcher compared the work with other similar work and made optimization to identify the strength and weakness of this algorithm and how can it improve efficiency in terms (imperceptibility, capacity, robustness).

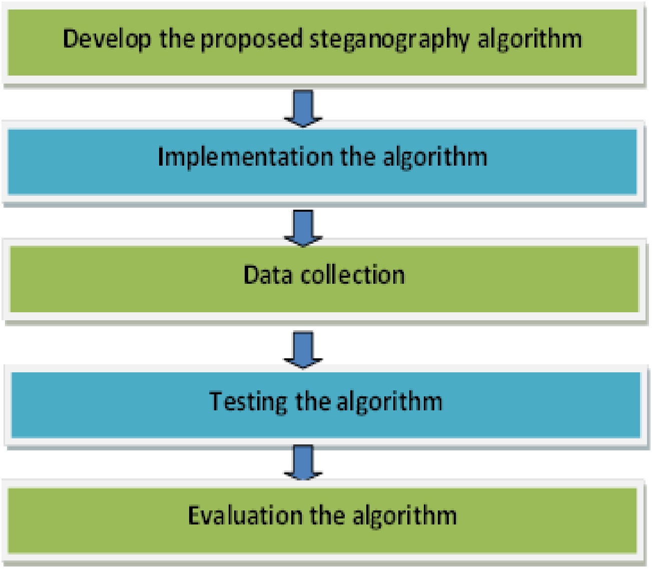

Develop the proposed steganography algorithm
Implementation the algorithm
Data collection
Testing the algorithm
Evaluation the algorithm

Figure (4.3): Steps of Methodology

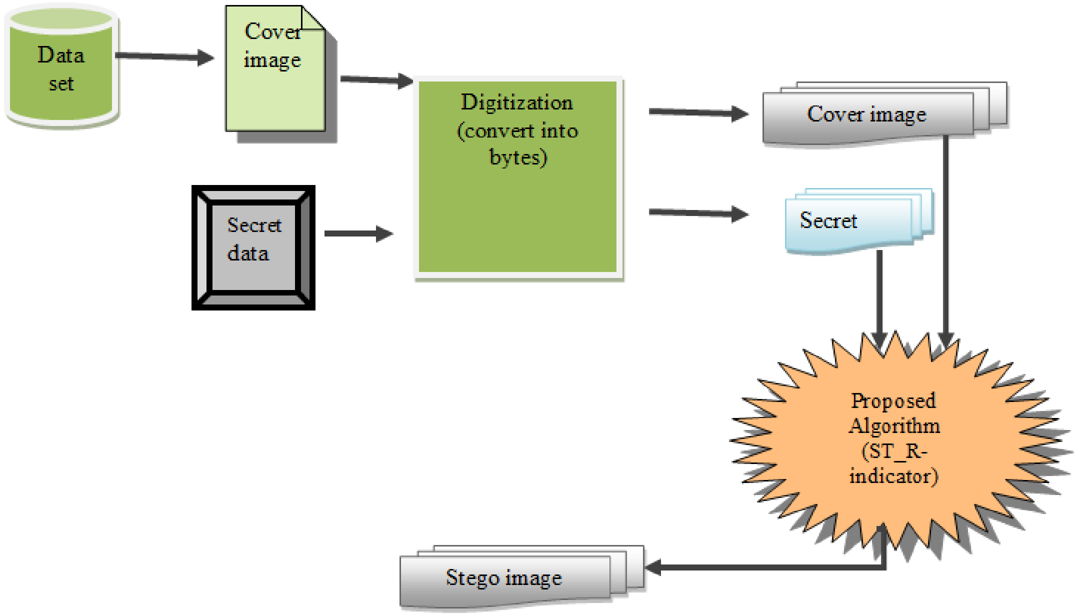

Data set
Cover image
Secret data
Digitization (convert into bytes)
Cover image
Secret
Proposed Algorithm (ST_R-indicator)
Stego image

Figure (4.4): The process of hiding secret data

4.3 Summary

This chapter presented the algorithm which called ST_R-indicator and then the methodology followed in the work. ST_R-indicator is used to hide data in RGB image Extention BMP, PNG as a cover medium, ST_R-indicator contains two phases one to hide and another to retrieve message using LSB technique. The bits used to hide the secret data are the least one or two bits by depending on the pixel indictor technique, where there are two indicators used. The first one is to determine the byte G or B into the embedded secret bit(s) and the other indicator to determine how many bits to embed at the same time.

Chapter 5

Experimental Result and Discussion

Chapter 5
Experimental Result and Discussion

In this chapter, we present the experiments performed for the evaluating the ST_R-indicator algorithm.Also it introduceses the measures we considered to evaluate our steganographic system effectiveness and efficiency. The evaluation is done to find out how good is the algorithm in general, after evaluating all the aspects considered by steganography.

5.1 Evaluation the Aspects of Steganography

To evaluate steganography algorithms, we need to take into account the purpose of steganography field to measure the degree of how much an algorithm meets that purpose. As clarified before, the main purpose of steganography is hiding the communication to preserve the security of the information. Steganography does communication hiding by hiding the presence of the secret data inside the stego mediums. For hiding the presence of the secret data, the stego files mustn't arouse any suspension to avoid getting detected. Thus, the first aspect of hiding algorithms to evaluate is the imperceptibility which is concerned with making the stego files perceptually undetectable, and this is done by making stego files as identical to the cover files as possible. For images, the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the metrics of the similarity between images before and after processing. So, through the tests, they are going to be the metrics of the similarity between cover images and stego images. Another aspect that could be considered is the capacity of the algorithm. Since we need to hide the data for transferring it over the internet, the larger amount of data can be loaded and sent at once by the better algorithm. Here we encounter the fact that the more data we hide inside a cover file, the more distortion we cause, which in turn increases the probability of the detectability. Hence, there is a tradeoff between the steganographic capacity and imperceptibility, and it is obvious that imperceptibility is more important to maintain, since it is a main component of the hidden data security. Therefore, increasing the imperceptibility is considered a significant contribution. Additionally, increasing the capacity is a good contribution, but with maintaining the imperceptibility. The last aspect is the robustness which is the degree of how much an algorithm can resist steganalysis. In fact, the main contribution of most each new developed algorithm is its new own way of hiding the data, and robustness depends on how the algorithm works and embeds the data. So, there are no metrics for robustness, and its evaluation is the evaluation of the strength of the algorithm itself. However, for measuring the robustness, some steganalysis methods would be applied to see how much the algorithm can resist attacking by passing them without getting detected. Hence, we want to measure the percentage of the data that can get embedded to the size of the cover image without getting detected when the stego image is subjected to steganalysis. Also, since we use LSB technique for data hiding, we would show the least and the second least bit planes to check if there are any visual signs of embedding. AS shown in table (5.1).

Table (5.1): steganoghraphy aspects for evaluation

Aspect	What are
Imperceptibility	Concerned with making the stego files perceptually undetectable, and this is done by making stego files as identical to the cover files as possible.
Capacity	larger amount of data that can be loade
Robustness	The degree of how much an algorithm can resists steganalysis.

5.2 Experimental environment

The proposed method, LSB technique and pixel indicator technique are implementated using java programming language (version8.0.1) and related APIs.

The proposed ST-R-indicator algorithm was applied on 24-bit colored bmp, png images for the purpose of the algorithm efficiency validation where it is processed on lap top with processor Core(Tm)-i3-2350M, CPU 2.30 GHz ,RAM equals 4 GB and 64 bit operating system, windows10. .

For experiments we have embedded variable amount of data in different standard benchmark RGB images extention BMP and PNG to evaluate the performance of these proposed techniques. There are many parameters to measure the steganographic system performance. Some parameters as follows: Capacity, imperceptibility, Robustness.

Used Peak Signal to Noise Ratio (PSNR) to compute how well the methods perform. It computes the peak signal to noise ratio between the two images. This ratio is used as a measure of quality between the two images. If the ratio of PSNR is high then the images have better quality. In addition, Mean Squared Error is the average squared difference between original image and a modified image (stego image). StegExpose steganalysis tools are used for Detecting LSB Steganography.

5.3 Expriemental Hiding and Retrieving Data

In our experiments, we used steganography to hide secret data and get a stego image in order to assess the efficiency of the proposed algorithm, and considered variables: capacity, Imperceptibility **(**the quality of stego images) and Robustness.

The experimental results are given to demonstrate the performance of the proposed algorithm. We used some RGB images as the cover image like leena 768 KB size image is used as the hidden secret message.

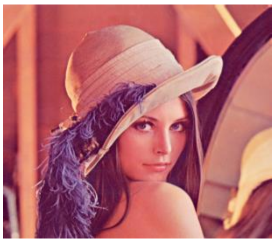


Figure (5.1): Leena used Original cover image

The secret messages hiden for applying ST_R-indicator algorithm these messages have taken different size but this size less than the cover image size.

We used Leena image as a cover image. This image are shown in Figuer 5.1 The secret message which is used to hide into the cover image can take any size but this size is less than the cover image size like 16191 byte. Hidden secret messages it is included in the cover image after applying ST_R-indicator algorithm that hided the secret message in the cover image of leena.

The result image is called stego image. The stego images resulted from our proposed algorithm as it is shown in Figure 5.2.

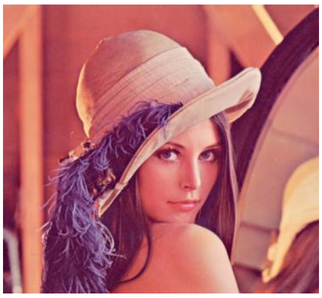
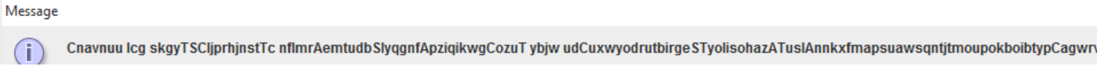


Figure (5.2): Resulted stego images

As a result of stego image is indistinguishable to the naked eye from the image of the original cover. Any attacker can not show any difference between the cover imge and stego cover. ST_R-indicator algorithm improved security and image quality.

On the other hand, Experimental result for retrieving secret message size 16191 byte used stego image in figure 5.2. Retrieved secret messages from a cover image after applying Extraction ST_R-indicator algorithm which extracted secret message in the cover image of leena is shown in Figure 5.3.



Message

Cnavnuu Icg skgyTSCljprhjnstTc nflmrAemtudbSlyqgnfApziqikwgCozuT ybjw udCuxwyodrutbirgeSTyolisohazATuslAnnkxfmapsuawsqntjtmoupokboibtypCagwr

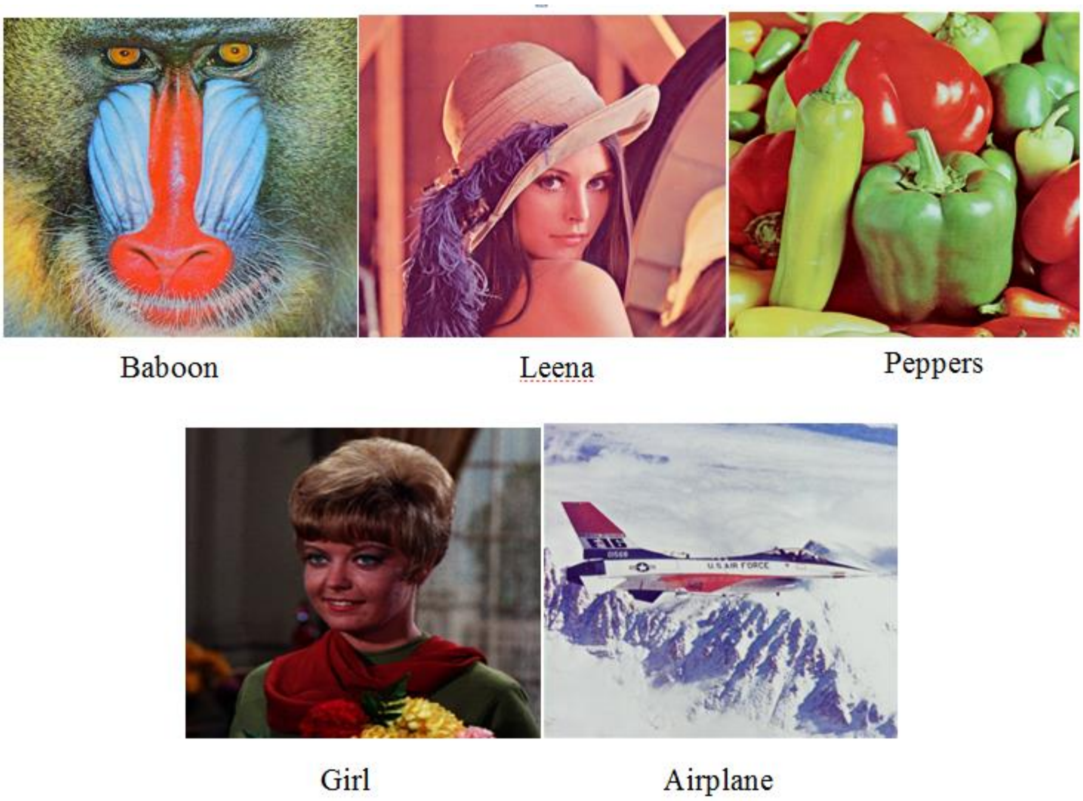
Figure (5.3): Retrieving secret message

5.4 Test image quality

This test measures the image quality through comparing between the original image and the Stego image, It assesst the secret data percentage of the image percentage through PSNR(Peak-Signal-to -Noise- ratio), taking into account that the typical value is 40 and MSE(Mean Squared Error).

In the experiment we have chosen benchmark images like: Lena, Baboon, Peppers, Airplane and Girl with png, bmp extention (Figure 5.4), each of 512x512 pixels was selected and downloaded then used as cover images. However, the reason for choosing these images were being well known and used in the areas of digital image processing, compression and steganography

The first secret message size starting from 10%, and the size will be increased in the next secret message until the 50% of the image size (increase 5% each time of the size of the hidden data).



Baboon Leena Peppers

Girl Airplane

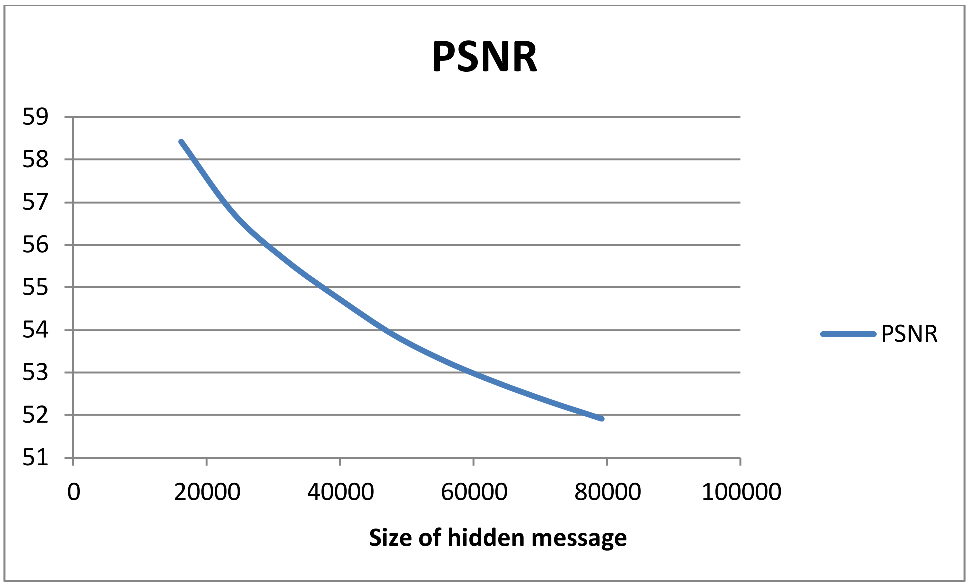
Figure (5.4): Test Image (512x512 pixels) used in our experiments

Table (5.2) shows the results of stego images and contains the PSNR, MSE values of stego images:

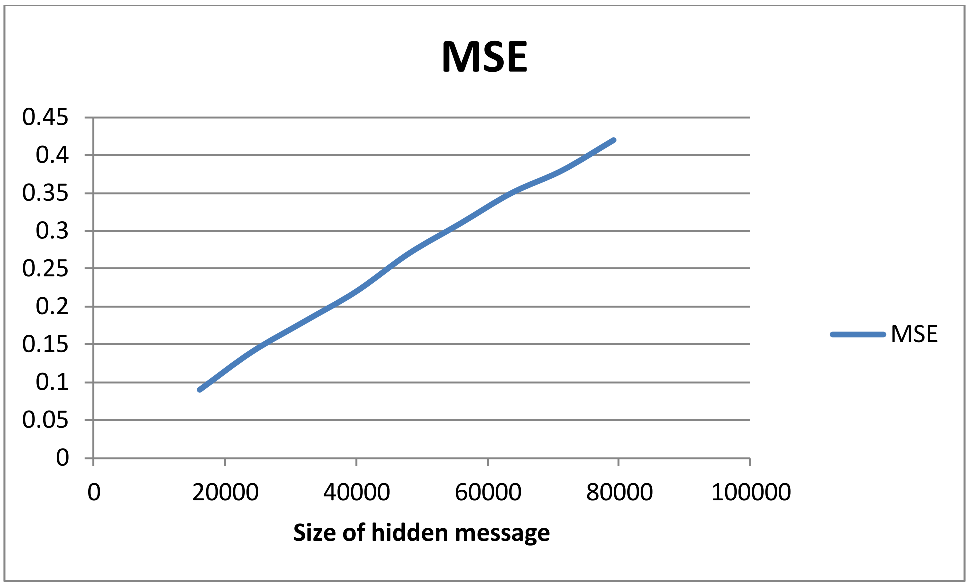
Table (5.2): the image quality test (PSNR) and (MSE) for Leena image.

Image name	image size	size of hidden data	PSNR	MSE	Detected or Not
Leena. png	512 x512	16191	58.42	0.09	No
		24118	56.72	0.14	No
		32063	55.61	0.18	No
		40034	54.71	0.22	No
		48016	53.88	0.27	No
		55914	53.25	0.31	No
		63657	52.75	0.35	No
		71398	52.31	0.38	Yes
		79211	51.91	0.42	Yes

Figures (5.5) (5.6) show the PSNR, MSE values for images chosen (leena).



Figures (5.5): the PSNR and MSE values for Leena image



Figures (5.6): the MSE values for Leena image

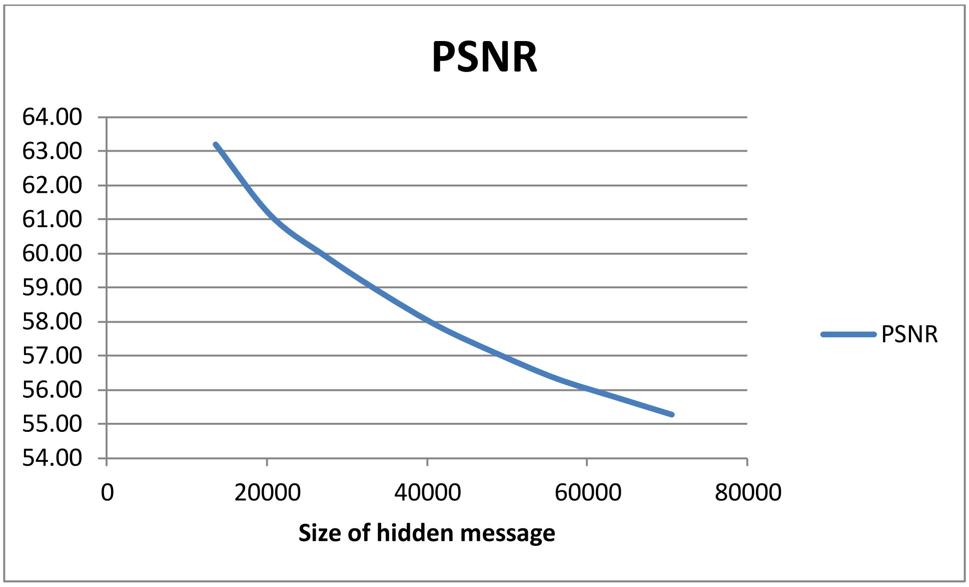
In these Figures Clarification PSNR and MSE. the PSNR start 58.42 with size of secret message 16191 Byte , if the size of a secret message increases it reduces the PSNR value, Mean Squared Error (MSE) increased the size of secret message hide and increases the MSE. It is shown in the table 5.2

The table (5.3) shows the results of stego images and contains the PSNR, MSE values of stego images:

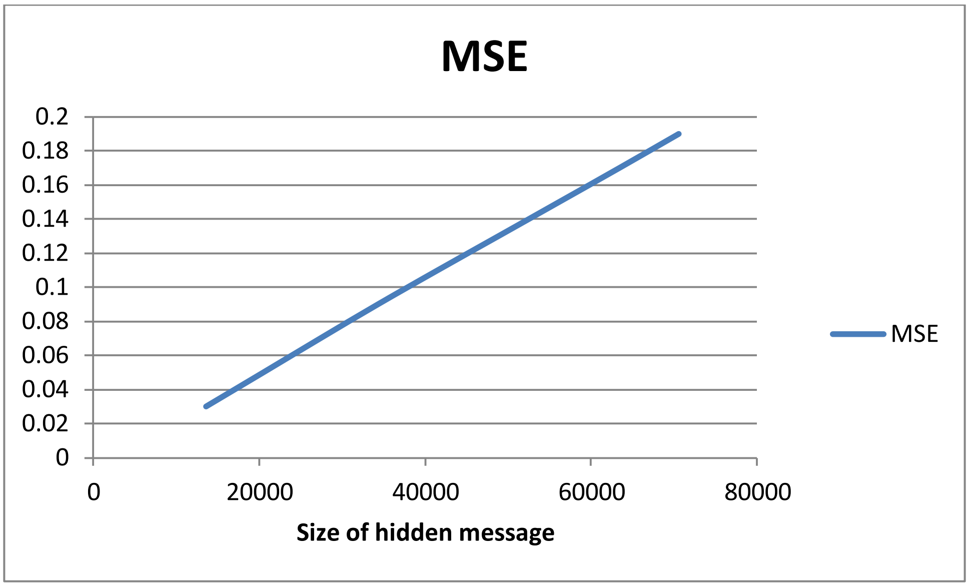
Table (5.3): the image quality test PSNR and MSE for baboon image.

Image name	image size	size of hidden data	PSNR	MSE	Detected or Not
Baboon.bmp	512 x512	13602	63.20	0.03	No
		20502	61.11	0.05	No
		27368	59.91	0.07	No
		34323	58.84	0.09	No
		41520	57.85	0.11	No
		48836	57.05	0.13	No
		56135	56.33	0.15	No
		63405	55.79	0.17	No
		70568	55.27	0.19	No

Figures (5.7) (5.8) show the PSNR and MSE values for images chosen (Baboon).



Figures (5.7): The PSNR values for Baboon image



Figures (5.8): The MSE values for Baboon image

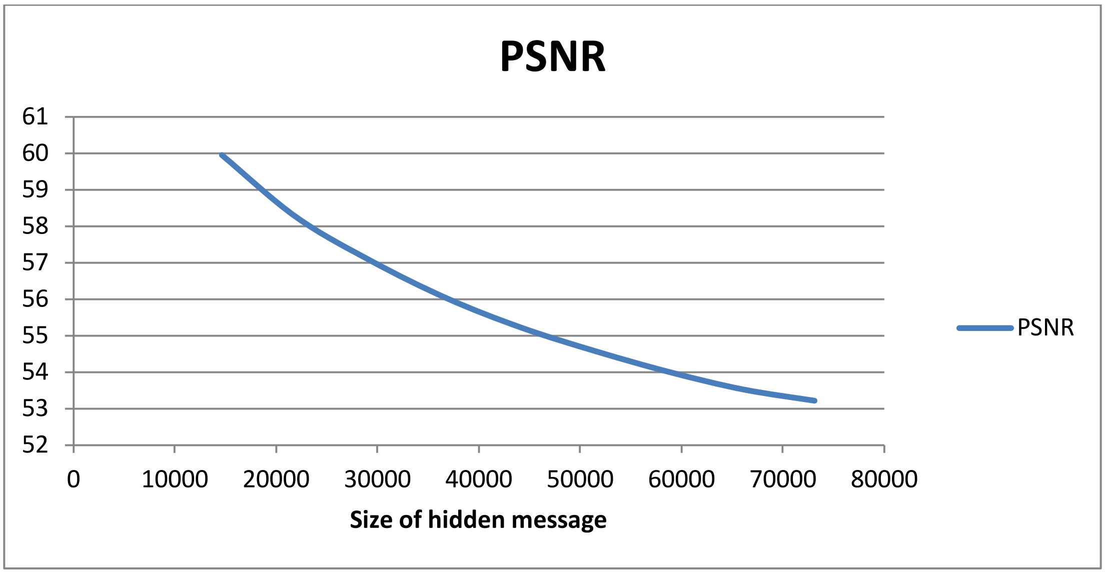
In these Figures Clarification PSNR and MSE. the PSNR start 63.20 with size of secret message 13602 Byte, if the size of a secret message inceases it reduces the PSNR value shown in the table 5.3, Mean Squared Error (MSE) increased the size of secret message hiden and increases the MSE.

The table (5.4) shows the results of stego images and contains the PSNR and MSE values of stego images:

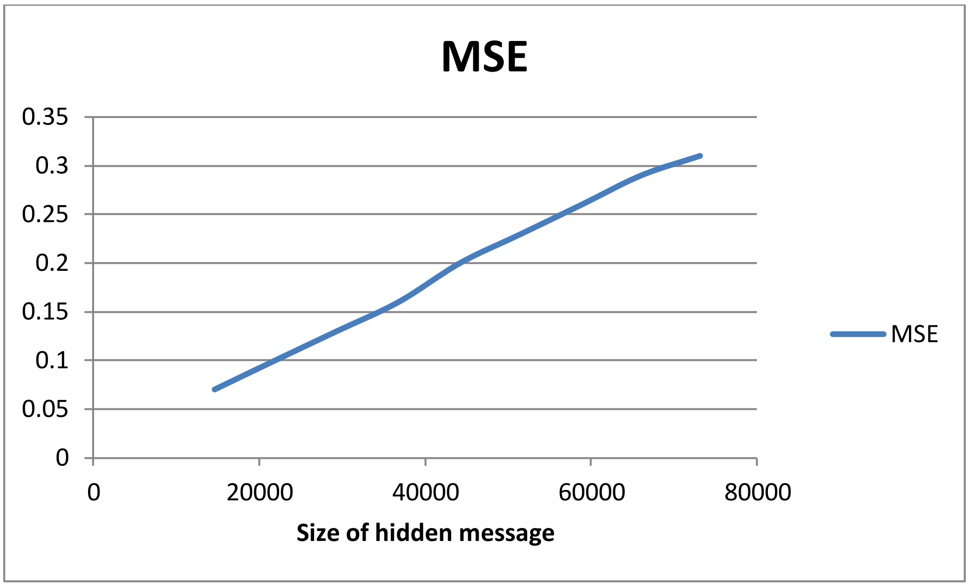
Table (5.4): the image quality test PSNR and MSE for peppers image.

Image name	image size	size of hidden data	PSNR	MSE	Detected or Not
peppers bmp	512 x512	14633	59.95	0.07	No
		21962	58.25	0.10	No
		29395	57.04	0.13	No
		36838	56.02	0.16	No
		44240	55.21	0.20	Yes
		51618	54.56	0.23	Yes
		58897	53.99	0.26	Yes
		66077	53.52	0.29	Yes
		73135	53.21	0.31	Yes

Figures (5.9) (5.10) show the PSNR and MSE values for images chosen (peppers).



Figures (5.9): The PSNR values for Peppers image



Figures (5.10): The MSE values for Peppers image

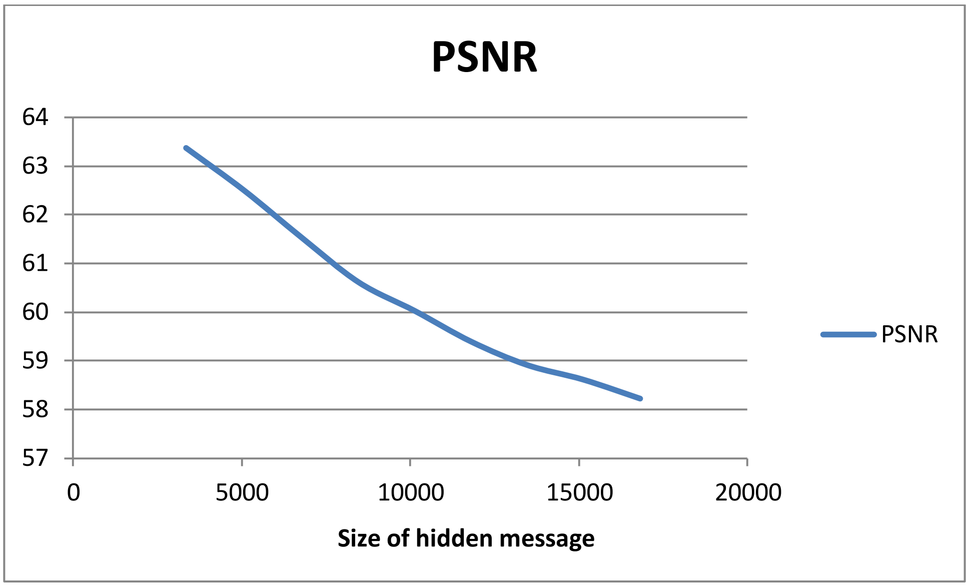
In thses Figures Clarification PSNR and MSE. the PSNR start 59.95 with size of secret message 14633 Byte , if the size of a secret message increases it reduces the PSNR value shown in the table 5.4, Mean Squared Error (MSE) increased the size of secret message hiden and increases the MSE .

The table (5.5) shows the results of stego images and contains the PSNR, MSE values of stego images:

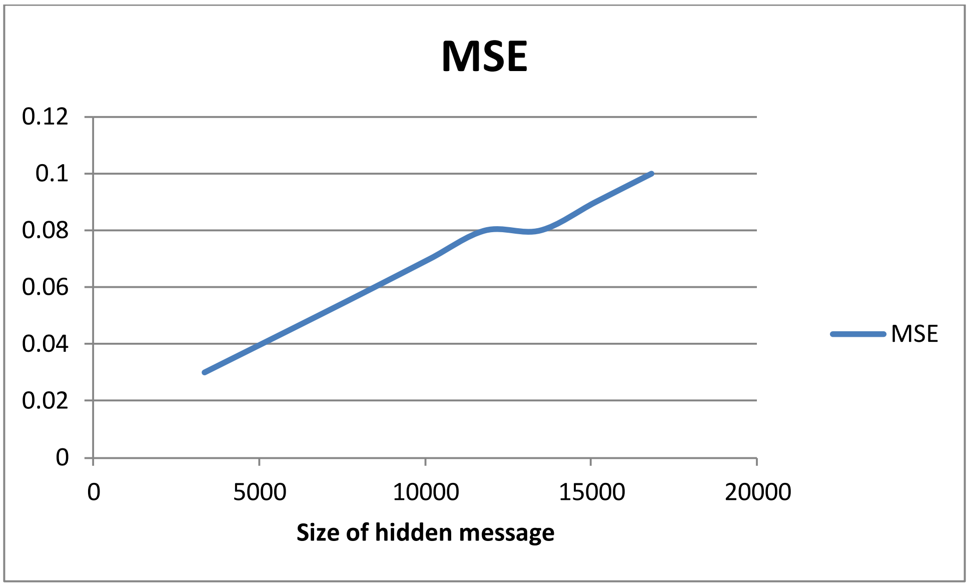
Table (5.5): the image quality test PSNR and MSE for Girl image.

Image name	Image size	size of hidden data	PSNR	MSE	Detected or Not
Girl png	512 x512	3355	63.37	0.03	No
		5070	62.50	0.04	No
		6781	61.53	0.05	No
		8474	60.61	0.06	No
		10143	60.02	0.07	No
		11812	59.39	0.08	No
		13473	58.91	0.08	No
		15136	58.61	0.09	Yes
		16821	58.22	0.10	Yes

Figures (5.11) (5.12) show the PSNR and MSE values for images chosen (Girl).



Figures (5.11): The PSNR values for Girl image



Figures (5.12): The MSE values for Girl image

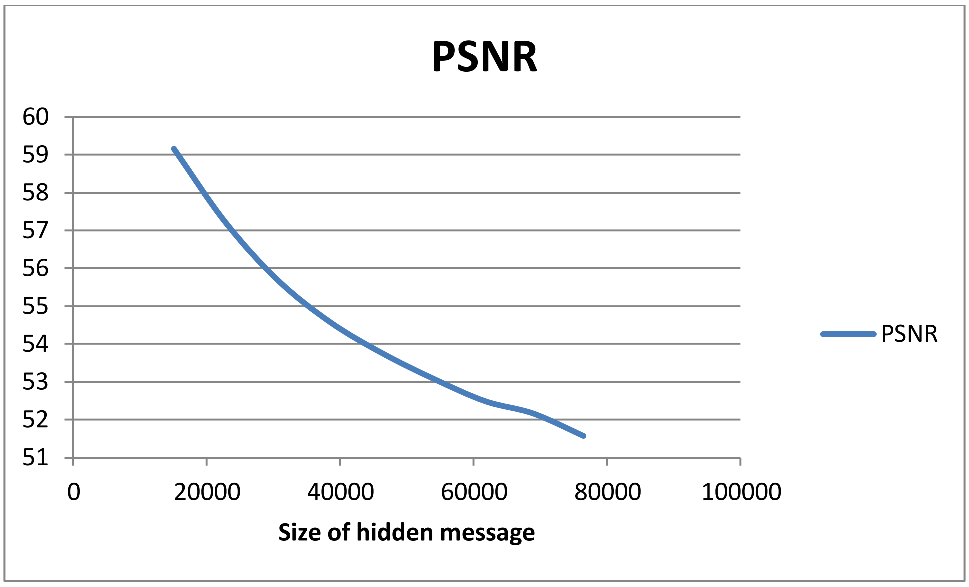
In these Figures Clarification PSNR and MSE. the PSNR start 63.37 with size of secret message 3355 Byte, if the size of a secret message increases it reduces the PSNR value shown in the table 5.5, Mean Squared Error (MSE) increased the size of secret message hiden and increases the MSE.

The table (5.6) shows the results of stego images and contains the PSNR, MSE values of stego images:

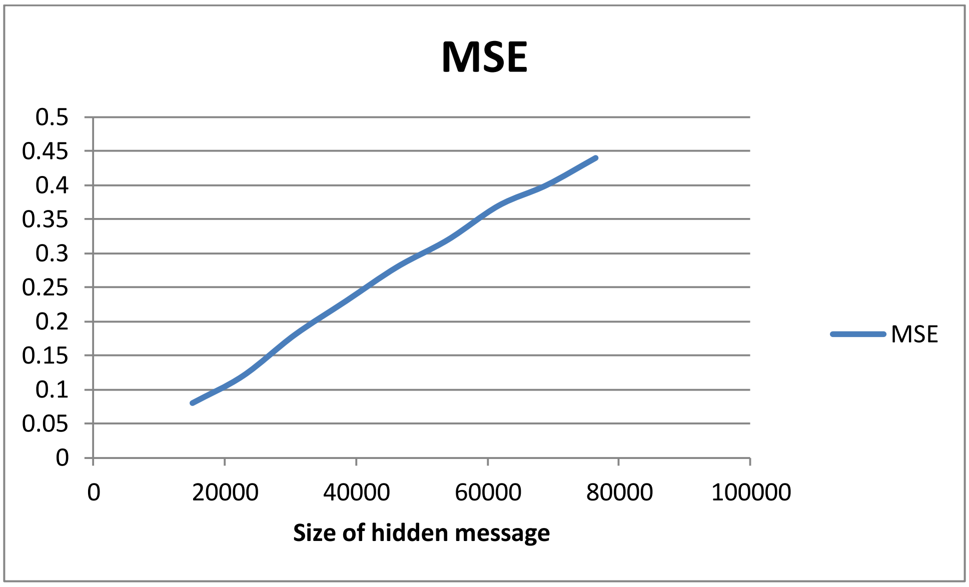
Table (5.6): the image quality test PSNR, MSE and time for Airplane image.

Image name	image size	size of hidden data	PSNR	MSE	Detected or Not
Airplane bmp	512 x512	15105	59.16	0.08	No
		22807	57.22	0.12	No
		30652	55.69	0.18	No
		38497	54.58	0.23	No
		46274	53.76	0.28	No
		54018	53.08	0.32	Yes
		61713	52.49	0.37	Yes
		68991	52.16	0.40	Yes
		76467	51.57	0.44	Yes

Figures (5.13) (5.14) show the PSNR, MSE values for images chosen (airplan).



Figures (5.13): The PSNR value for Airplane image



Figures (5.14): The MSE value for Airplane image

In these Figures Clarification PSNR and MSE. the PSNR start 59.16 with size of secret message 15105 Byte, if the size of secret message increases it reduces the PSNR value shown in the table 5.6, Mean Squared Error (MSE) increased the size of secret message hiden and increases the MSE.

5.5 Capacity (payload) test

The data load which is embedded by using the proposed algorithm is bigger than the data that embedded by other algorithms and the reason for that because the proposed algorithm can be embedded from 3 bit to 6 bits in each pixel and the secret message is hidden at least significant bits of the pixels, with more randomization.

The table (5.7) shows the secret message load which can be embedded inside different loads of the RGB images by using proposed algorithm .

Table (5.7): Show Payload of data which can be embedded in different RGB bmp,png images

Image name	Image Size	Usable byte to contain	Hiding Capacity (Byte)
Leena png	782 KB (801,429 bytes)	786432	79211
Peppers bmp	768 KB (786,486 bytes)	786432	73135
Baboon bmp	768 KB (786,486 bytes)	786432	70568
Girl png	165 KB (169,058 bytes)	196608	16821
Airplane bmp	768 KB (786,486 bytes)	786432	76467

Figure 5.15 shows Payload of data which can be embedded inside images Leena, Peppers, Baboon, Girl, and Airplane.

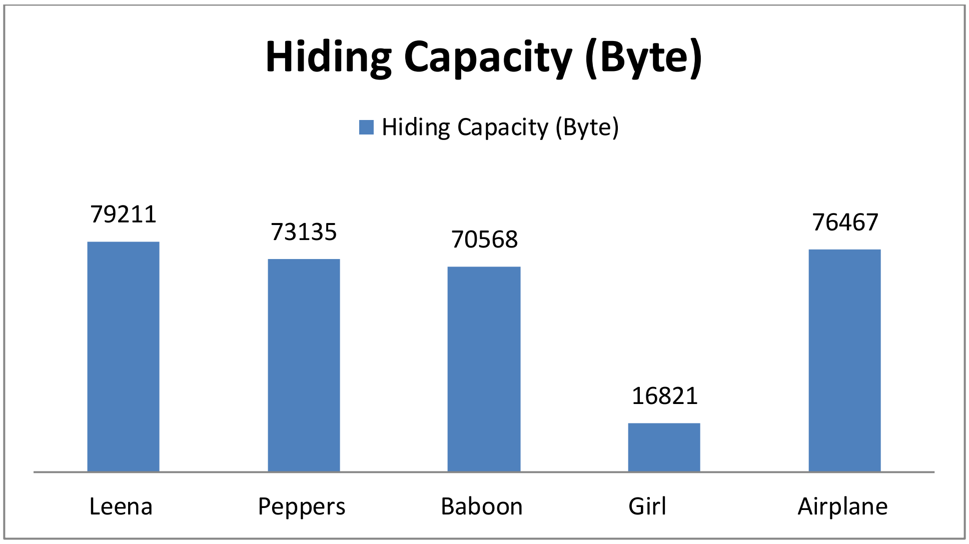


Figure (5.15): shows the payload inside different RGB bmp,png images

Figures (5.15 A, B) show Cover-image, Stego-image after embedding 32063 byte inside Leena image by proposed algorithm.

Figure (5.15,A):Cover Image

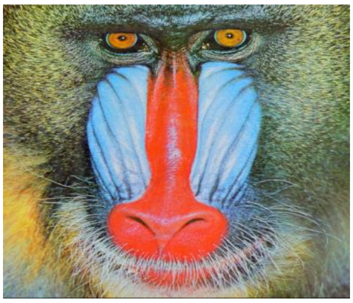
Figure (5.15,B):Stego Image

Figures (5.16A, B) show Cover-image, Stego-image after embedding 29395 byte inside Peppers image by proposed algorithm.

Figure (5.16,A):Cover Image

Figure (5.16,B):Stego Image

Figures (5.17A, B) show Cover-image, Stego-image after embedding 27368 byte inside Baboon image by proposed algorithm.



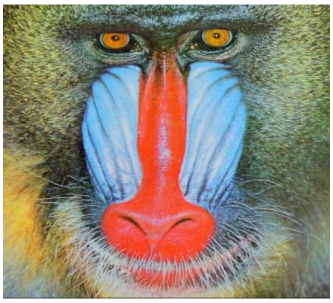


Figure (5.17,A):Cover Image

Figure (5.17,B):Stego Image

Figures (5.18A, B) show Cover-image, Stego-image after embedding 6781 byte inside Girl image by proposed algorithm.

Figure (5.18,A):Cover Image

Figure (5.18,B):Stego Image

Figures (5.19A, B) show Cover-image, Stego-image after embedding 30652 byte inside Airplane image by proposed algorithm.

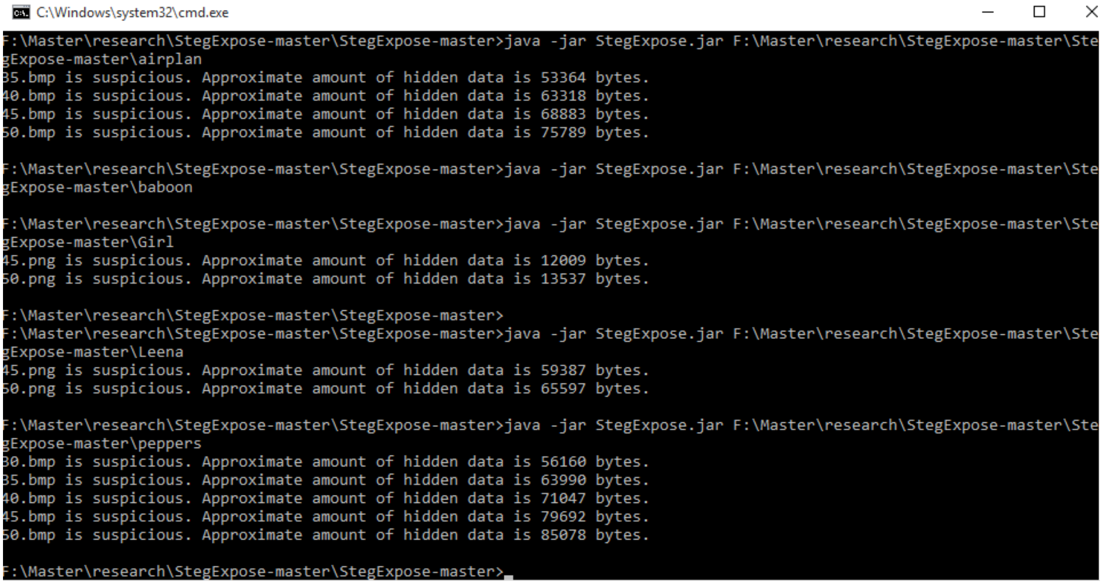
Figure (5.19,A):Cover Image

Figure (5.19,B):Stego Image

The difference of stego image can be hard to distinguish after being embedded. The Human Visual System (HVS) can not differentiate between the original image and the image stegoand also the stego-images does not generate any suspicion

5.6 Robustness test

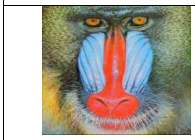
In our experimental test we used steganalysis tools for detecting LSB Steganography. The image extention used for this experiment are PNG and BMP. The result of the stego image in this tool catch 2 images which are suspicion of girl and leena image, catch 4 image of airplan image, catch 5 image of peppers image and baboon image don't catch any image of the total stego image 9 image for each image. They are summarize in table 5.8. This shows the robust of the algorithm, it is shows in figure 5.20.



```
F:\Master\research\StegExpose-master\StegExpose-master>java -jar StegExpose.jar F:\Master\research\StegExpose-master\Ste
gExpose-master\airplan
35.bmp is suspicious. Approximate amount of hidden data is 53364 bytes.
40.bmp is suspicious. Approximate amount of hidden data is 63318 bytes.
45.bmp is suspicious. Approximate amount of hidden data is 68883 bytes.
50.bmp is suspicious. Approximate amount of hidden data is 75789 bytes.

F:\Master\research\StegExpose-master\StegExpose-master>java -jar StegExpose.jar F:\Master\research\StegExpose-master\Ste
gExpose-master\baboon

F:\Master\research\StegExpose-master\StegExpose-master>java -jar StegExpose.jar F:\Master\research\StegExpose-master\Ste
gExpose-master\Girl
45.png is suspicious. Approximate amount of hidden data is 12009 bytes.
50.png is suspicious. Approximate amount of hidden data is 13537 bytes.

F:\Master\research\StegExpose-master\StegExpose-master>
F:\Master\research\StegExpose-master\StegExpose-master>java -jar StegExpose.jar F:\Master\research\StegExpose-master\Ste
gExpose-master\Leena
45.png is suspicious. Approximate amount of hidden data is 59387 bytes.
50.png is suspicious. Approximate amount of hidden data is 65597 bytes.

F:\Master\research\StegExpose-master\StegExpose-master>java -jar StegExpose.jar F:\Master\research\StegExpose-master\Ste
gExpose-master\peppers
30.bmp is suspicious. Approximate amount of hidden data is 56160 bytes.
35.bmp is suspicious. Approximate amount of hidden data is 63990 bytes.
40.bmp is suspicious. Approximate amount of hidden data is 71047 bytes.
45.bmp is suspicious. Approximate amount of hidden data is 79692 bytes.
50.bmp is suspicious. Approximate amount of hidden data is 85078 bytes.

F:\Master\research\StegExpose-master\StegExpose-master>
```

Figure (5.20): the result of using stegExpose tools

Table(5.8): Summary of Percentage robust for the image

Image	Image name	No of Image detected	No of Image robust	Percentage robust
	Leena	2	7	0.77%
	peppers	5	4	0.44%
	Baboon	0	9	100%
	Girl	2	7	0.77%
	Airplan	4	5	0.55%

Table(5.9): image used for impact the robust for the image

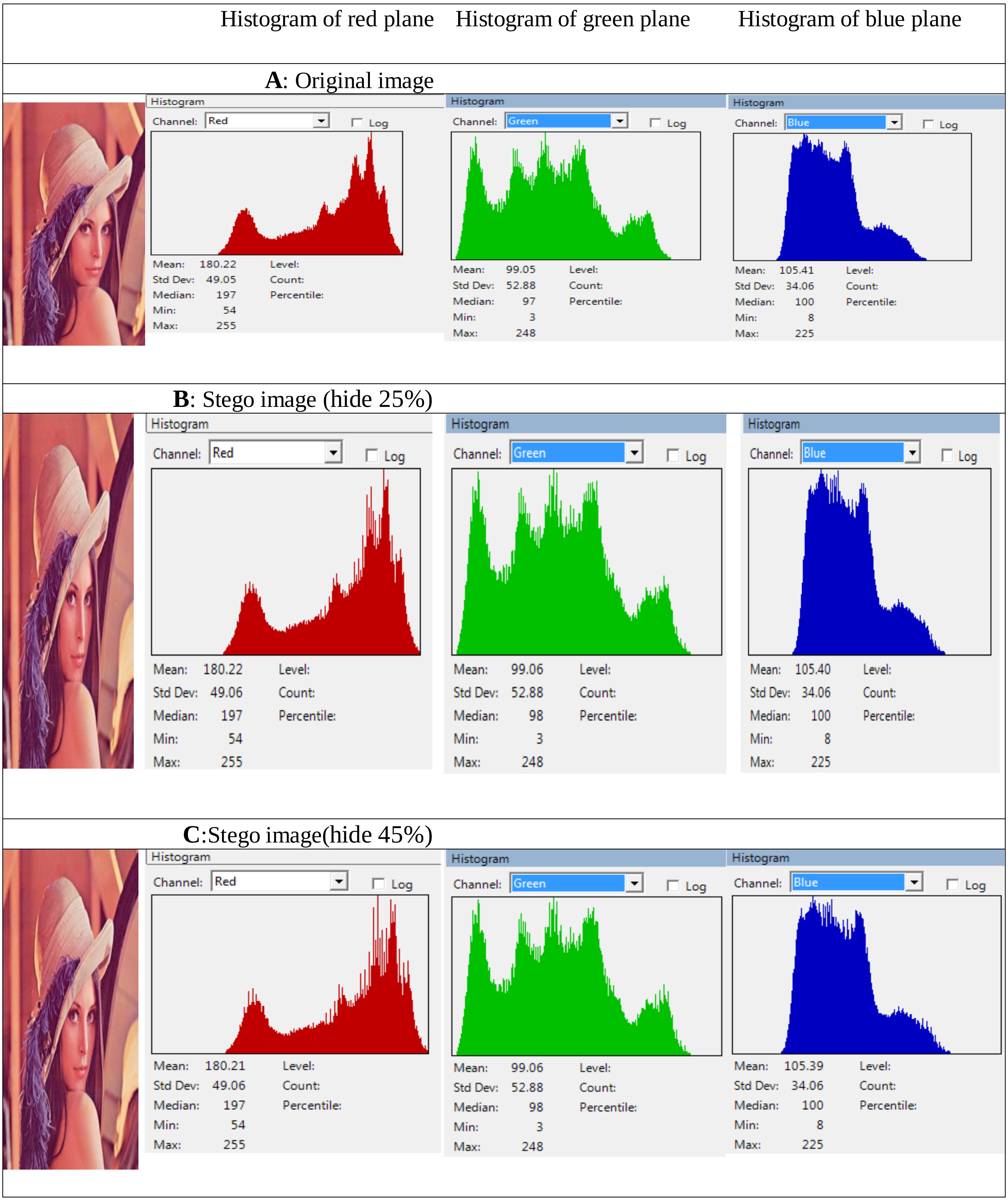
Image	Percentage to detected	No of Image detected	No of Image robust	Percentage robust
	45%	2	7	0.77%
	Not detect	0	9	100%
	15%	8	1	0.11%
	50%	1	8	0.88%
	10%	9	0	0%

Table5.8 shows that a robust percentage to benchmark images used, depend on the image Characteristics. In other hand experiment done using another images (Table5.9) with similar Characteristics of the benchmark images. As a result, the percentage for the detection is not fixed which mean the Characteristics dos not affect in the robust. perhaps revealed in 40% image, revealed 45% or 50%of size image, experiment another image that are revealed while hidden data 10%, or 15% that are detected.

5.7 Security Test

This test is based on the comparison from the original image and the stego image(image after embedding data through the following statistical tool Histogram. Histogram is a graphical display of tabulated frequencies, The degradation of the images quality can also be visually noticed by applying the histogram analysis.

We have compared the histogram of five images (Lena, Baboon, Peppers, Airplane and Girl) where calculated the histogram for R, G and B channel separately. The Figure (5.21), Figure (5.22), Figure (5.23), Figure (5.24) and Figure (5.25) shows comparison result s of histograms of lena.png, girl.png, Peppers.bmp, Airplane.bmp and Baboon.bmp with their stego images different size data embedding(A: originl imge , B: hide 25% of size image and C : hide 45% of size image).



Histogram of red plane Histogram of green plane Histogram of blue plane

A: Original image

Histogram

Channel: Red □ Log

Mean: 180.22 Level:
Std Dev: 49.05 Count:
Median: 197 Percentile:
Min: 54
Max: 255

Histogram

Channel: Green □ Log

Mean: 99.05 Level:
Std Dev: 52.88 Count:
Median: 97 Percentile:
Min: 3
Max: 248

Histogram

Channel: Blue □ Log

Mean: 105.41 Level:
Std Dev: 34.06 Count:
Median: 100 Percentile:
Min: 8
Max: 225

B: Stego image (hide 25%)

Histogram

Channel: Red □ Log

Mean: 180.22 Level:
Std Dev: 49.06 Count:
Median: 197 Percentile:
Min: 54
Max: 255

Histogram

Channel: Green □ Log

Mean: 99.06 Level:
Std Dev: 52.88 Count:
Median: 98 Percentile:
Min: 3
Max: 248

Histogram

Channel: Blue □ Log

Mean: 105.40 Level:
Std Dev: 34.06 Count:
Median: 100 Percentile:
Min: 8
Max: 225

C:Stego image(hide 45%)

Histogram

Channel: Red □ Log

Mean: 180.21 Level:
Std Dev: 49.06 Count:
Median: 197 Percentile:
Min: 54
Max: 255

Histogram

Channel: Green □ Log

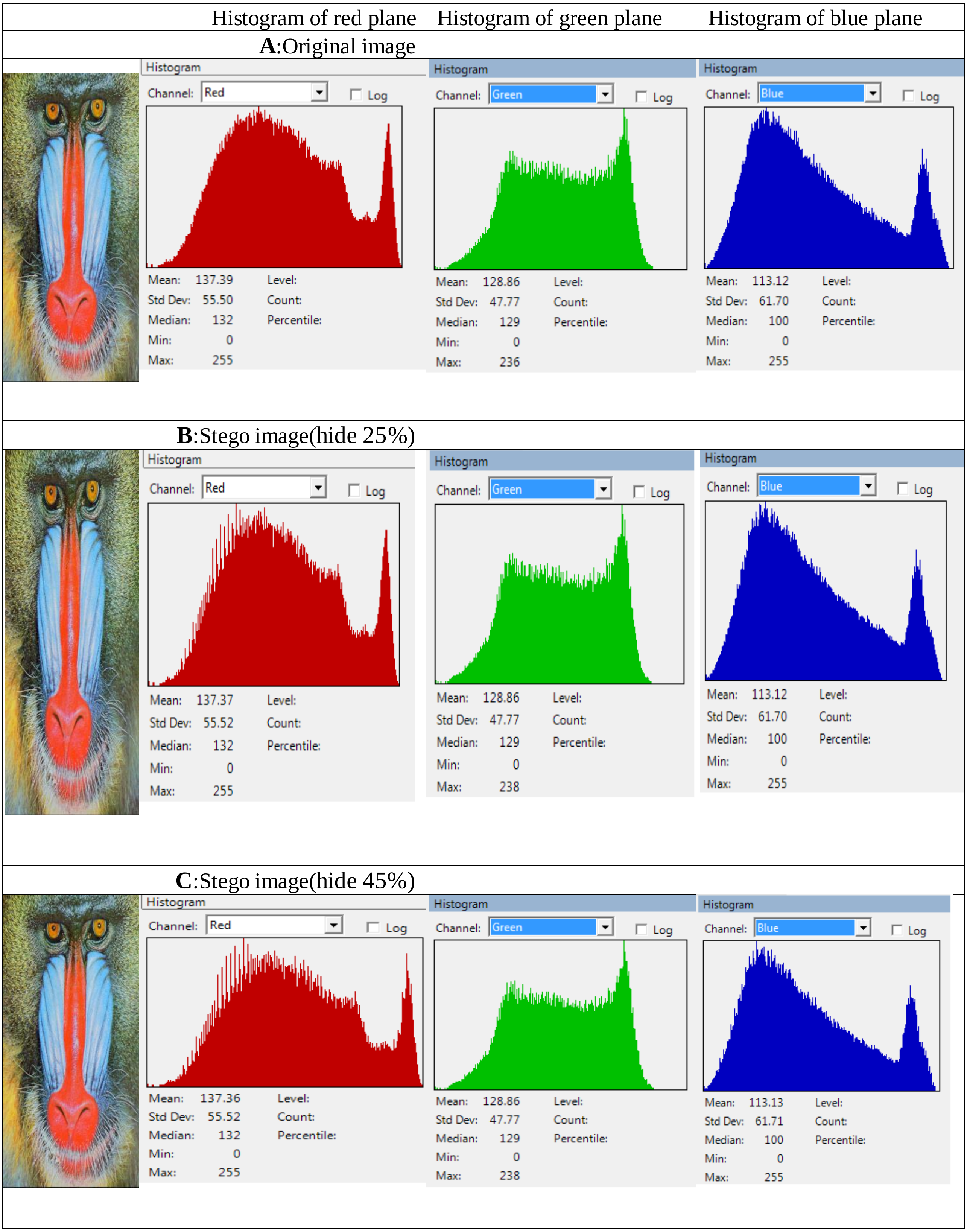
Mean: 99.06 Level:
Std Dev: 52.88 Count:
Median: 98 Percentile:
Min: 3
Max: 248

Histogram

Channel: Blue □ Log

Mean: 105.39 Level:
Std Dev: 34.06 Count:
Median: 100 Percentile:
Min: 8
Max: 225

Figure (5.21): Histogram of Original and stego image leena



Histogram of red plane Histogram of green plane Histogram of blue plane

A:Original image

Histogram
Channel: Red □ Log
Mean: 137.39 Level:
Std Dev: 55.50 Count:
Median: 132 Percentile:
Min: 0
Max: 255

Histogram
Channel: Green □ Log
Mean: 128.86 Level:
Std Dev: 47.77 Count:
Median: 129 Percentile:
Min: 0
Max: 236

Histogram
Channel: Blue □ Log
Mean: 113.12 Level:
Std Dev: 61.70 Count:
Median: 100 Percentile:
Min: 0
Max: 255

B:Stego image(hide 25%)

Histogram
Channel: Red □ Log
Mean: 137.37 Level:
Std Dev: 55.52 Count:
Median: 132 Percentile:
Min: 0
Max: 255

Histogram
Channel: Green □ Log
Mean: 128.86 Level:
Std Dev: 47.77 Count:
Median: 129 Percentile:
Min: 0
Max: 238

Histogram
Channel: Blue □ Log
Mean: 113.12 Level:
Std Dev: 61.70 Count:
Median: 100 Percentile:
Min: 0
Max: 255

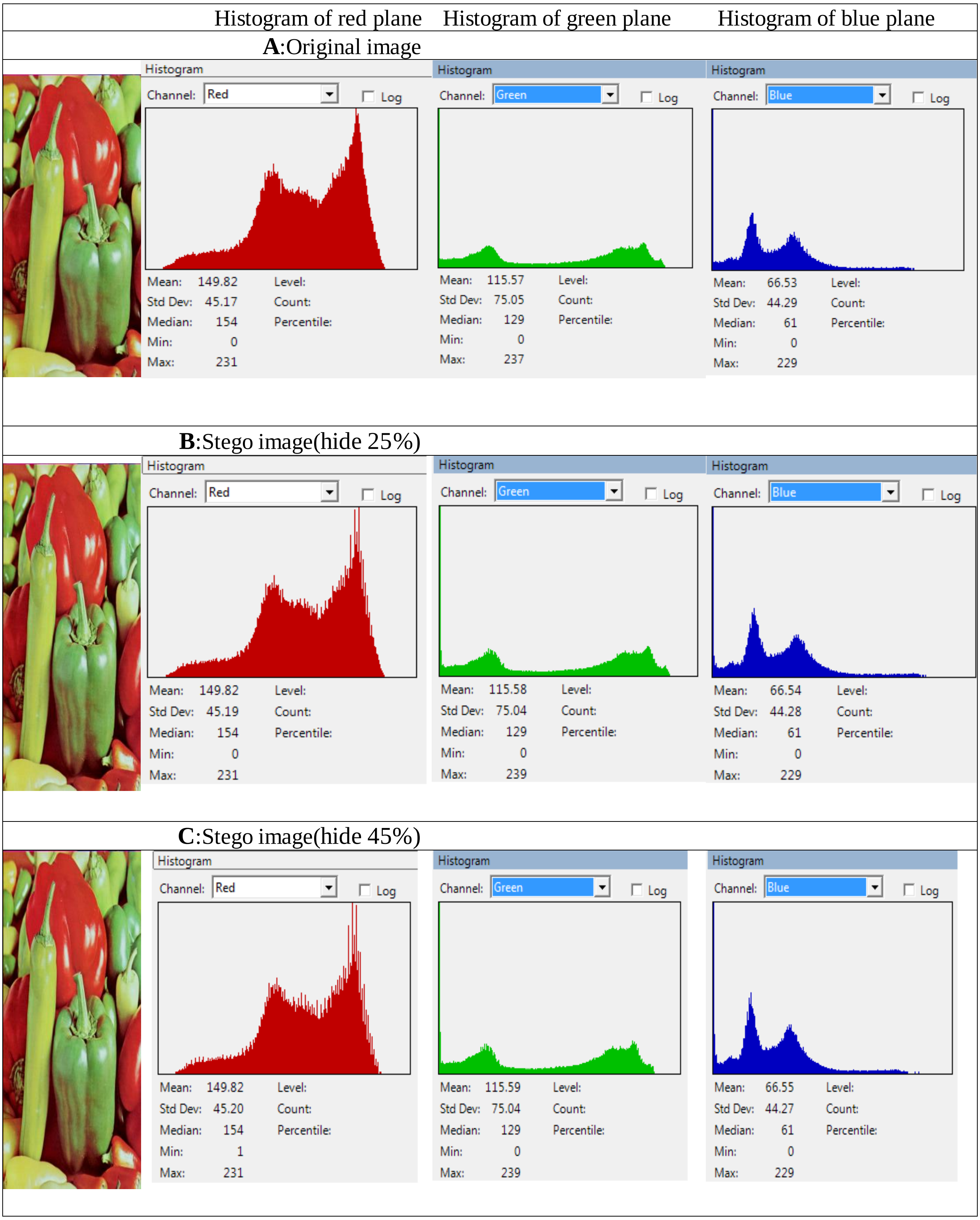
C:Stego image(hide 45%)

Histogram
Channel: Red □ Log
Mean: 137.36 Level:
Std Dev: 55.52 Count:
Median: 132 Percentile:
Min: 0
Max: 255

Histogram
Channel: Green □ Log
Mean: 128.86 Level:
Std Dev: 47.77 Count:
Median: 129 Percentile:
Min: 0
Max: 238

Histogram
Channel: Blue □ Log
Mean: 113.13 Level:
Std Dev: 61.71 Count:
Median: 100 Percentile:
Min: 0
Max: 255

Figure (5.22): Histogram of Original and stego image Baboon



Histogram of red plane Histogram of green plane Histogram of blue plane

A:Original image

Histogram
Channel: Red □ Log
Mean: 149.82 Level:
Std Dev: 45.17 Count:
Median: 154 Percentile:
Min: 0
Max: 231

Histogram
Channel: Green □ Log
Mean: 115.57 Level:
Std Dev: 75.05 Count:
Median: 129 Percentile:
Min: 0
Max: 237

Histogram
Channel: Blue □ Log
Mean: 66.53 Level:
Std Dev: 44.29 Count:
Median: 61 Percentile:
Min: 0
Max: 229

B:Stego image(hide 25%)

Histogram
Channel: Red □ Log
Mean: 149.82 Level:
Std Dev: 45.19 Count:
Median: 154 Percentile:
Min: 0
Max: 231

Histogram
Channel: Green □ Log
Mean: 115.58 Level:
Std Dev: 75.04 Count:
Median: 129 Percentile:
Min: 0
Max: 239

Histogram
Channel: Blue □ Log
Mean: 66.54 Level:
Std Dev: 44.28 Count:
Median: 61 Percentile:
Min: 0
Max: 229

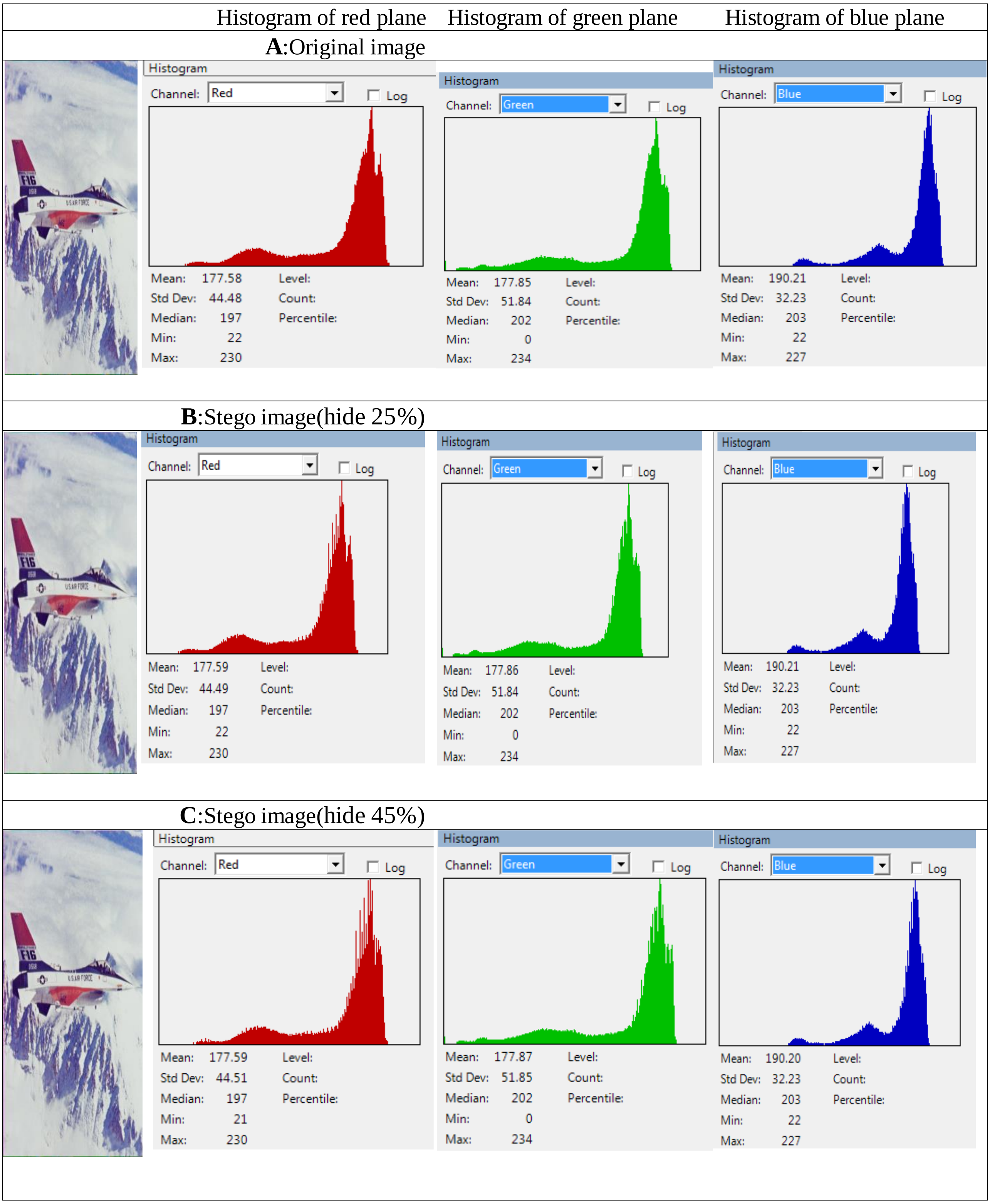
C:Stego image(hide 45%)

Histogram
Channel: Red □ Log
Mean: 149.82 Level:
Std Dev: 45.20 Count:
Median: 154 Percentile:
Min: 1
Max: 231

Histogram
Channel: Green □ Log
Mean: 115.59 Level:
Std Dev: 75.04 Count:
Median: 129 Percentile:
Min: 0
Max: 239

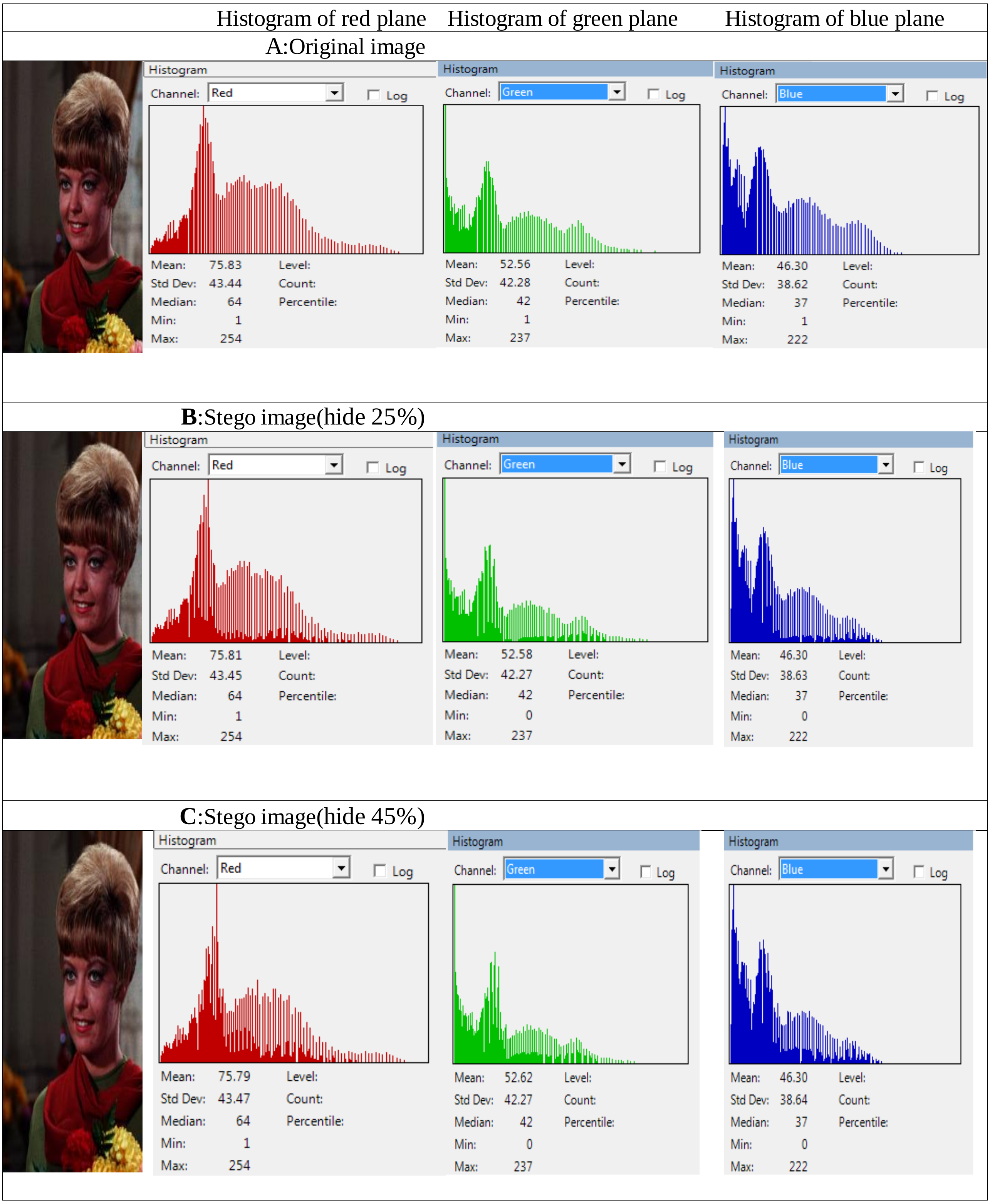
Histogram
Channel: Blue □ Log
Mean: 66.55 Level:
Std Dev: 44.27 Count:
Median: 61 Percentile:
Min: 0
Max: 229

Figure (5.23): Histogram of Original and stego image peppers



	Histogram of red plane	Histogram of green plane	Histogram of blue plane
A:Original image	Channel: Red Mean: 177.58 Std Dev: 44.48 Median: 197 Min: 22 Max: 230	Channel: Green Mean: 177.85 Std Dev: 51.84 Median: 202 Min: 0 Max: 234	Channel: Blue Mean: 190.21 Std Dev: 32.23 Median: 203 Min: 22 Max: 227
B:Stego image(hide 25%)	Channel: Red Mean: 177.59 Std Dev: 44.49 Median: 197 Min: 22 Max: 230	Channel: Green Mean: 177.86 Std Dev: 51.84 Median: 202 Min: 0 Max: 234	Channel: Blue Mean: 190.21 Std Dev: 32.23 Median: 203 Min: 22 Max: 227
C:Stego image(hide 45%)	Channel: Red Mean: 177.59 Std Dev: 44.51 Median: 197 Min: 21 Max: 230	Channel: Green Mean: 177.87 Std Dev: 51.85 Median: 202 Min: 0 Max: 234	Channel: Blue Mean: 190.20 Std Dev: 32.23 Median: 203 Min: 22 Max: 227

Figure (5.24): Histogram of Original and stego image Airplane



Histogram of red plane Histogram of green plane Histogram of blue plane

A:Original image

```
Histogram
Channel: Red          □ Log
Mean:      75.83   Level:
Std Dev:   43.44   Count:
Median:       64   Percentile:
Min:           1
Max:         254
```

```
Histogram
Channel: Green        □ Log
Mean:      52.56   Level:
Std Dev:   42.28   Count:
Median:       42   Percentile:
Min:           1
Max:         237
```

```
Histogram
Channel: Blue         □ Log
Mean:      46.30   Level:
Std Dev:   38.62   Count:
Median:       37   Percentile:
Min:           1
Max:         222
```

B:Stego image(hide 25%)

```
Histogram
Channel: Red          □ Log
Mean:      75.81   Level:
Std Dev:   43.45   Count:
Median:       64   Percentile:
Min:           1
Max:         254
```

```
Histogram
Channel: Green        □ Log
Mean:      52.58   Level:
Std Dev:   42.27   Count:
Median:       42   Percentile:
Min:           0
Max:         237
```

```
Histogram
Channel: Blue         □ Log
Mean:      46.30   Level:
Std Dev:   38.63   Count:
Median:       37   Percentile:
Min:           0
Max:         222
```

C:Stego image(hide 45%)

```
Histogram
Channel: Red          □ Log
Mean:      75.79   Level:
Std Dev:   43.47   Count:
Median:       64   Percentile:
Min:           1
Max:         254
```

```
Histogram
Channel: Green        □ Log
Mean:      52.62   Level:
Std Dev:   42.27   Count:
Median:       42   Percentile:
Min:           0
Max:         237
```

```
Histogram
Channel: Blue         □ Log
Mean:      46.30   Level:
Std Dev:   38.64   Count:
Median:       37   Percentile:
Min:           0
Max:         222
```

Figure (5.25): Histogram of Original and stego image Girl

After studying the figures(5.21,5.22,5.23,5.24,5.25) in the histogram analysis we can conclude that the hiding capacity of the proposed algorithm shows more satisfied experimental out comes, retains good visual clarity of stego images. In the histogram analysis the histogram of red channel, green and blue channel can be easily noticeable when increasing the size of secret message.

5.8 Comparison with other algorithms

The study RAJSHREE NOLKHA Algorithm(NOLKHA et al., 2016) was compared with the ST_R-indicator Algorithm that used five images like (leena, pepper, grapes, koala and rose)with secret massage 16384 bytes. (Table 5.10) shows the result

Table (5.10): Comparison RAJSHREE NOLKHA with ST_R-indicator Algorithm

image	Image Size	RAJSHREE NOLKHA Algorithm	ST_R-indicator Algorithm
leena	512×512	45.41	58.42
pepper	512×512	45.59	59.95
grapes	512×512	45.75	60.50
koala	512×512	45.35	63.20
rose	512×512	45.64	53.08

Another study Gutub Pixel Indicator Algorithm was compared with the ST_R-indicator Algorithm that used images like (Animal 1, Animal 2, Animal 3, football 1 and football 2) with secret massage 2120 bytes. (Table 5.11) shows the result

Table (5.11): Comparison Gutub Pixel Indicator with ST_R-indicator Algorithm

image	Image Size	Gutub Pixel Indicator Algorithm	ST_R-indicator Algorithm
Animal 1	1024×1024	57.94	67.24
Animal 2	1024×1024	58.10	70.66
Animal 3	1024×1024	58.11	68.02
football 1	1024×1024	57.96	73.09
football 2	1024×1024	57.50	74.96

We find out through the results that proposed algorithm is more satisfied experimental out comes than RAJSHREE NOLKHA algorithm and Gutub pixel indicator algorithm due to non-existence of difference between the original image and the stego image.

5.9 Summary

This chapter, present the experiments performed for the evaluation of the ST_R-indicator algorithm.Also the aspects steganography for evaluation has been introduced (capacity, imperceptibility and robustness). In addition, it defined environment experimental and the experimental hiden and retrieved data. Some testing and evaluation of the image quality, capacity and robustness are done.

ST_R-Indicator algorithm has been compared with other algorithms and experimental results show that the power of the new algorithm had hided and extracted data with a high storage capacity (payload) as it is describe in (section 5.5) and without being evident or being discovered with electronic techniques (high robustness) as it is describe in (section 5.6) and better imperceptibility (image quality after embedding data) which is describe in (section 5.4) and testing security using histogram analysis.

Chapter 6
Conclusions and Future work

Chapter 6
Conclusions and future work

6.1 Conclusions

Steganography is the science of hiding secret data inside other data, which is called the cover data, carrier or container, in order to hide communications, that no one apart from the meant parties can detect the existence of the secret data and thus the covert communication that are taking place.

There are different models of carrier that can be used as stego cover, such as text, image, audio and video to hide information, but the most common way to hide is the image due to the reluctance on the internet

Image Steganography is a technique of using image as a cover object. There are many kinds of image types that can be used as covers , for Example: jpg, bmp, png.

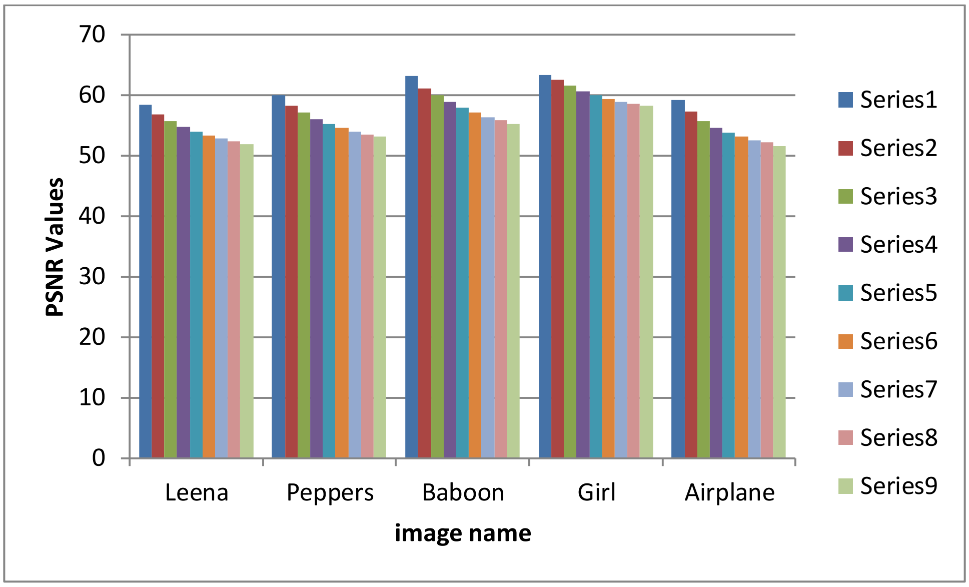
The algorithm called ST_R-indicator of hiding data based at Least Significant Bit (LSB), where the algorithm embeds inside the LSB(s).

This algorithm can be applied to RGB images (with bmp, png extentions) it is a cover media where each pixel is represented by three bytes (24 bit) red, green, and blue in pixel. The process of hiding depends on indicators. The indicators are used to determine what cover bytes to embed into this RGB channel, and how many secret bits to embed at a time.

Measuring the performance of the proposed algorithm has been applied using many experiments and calculating two values of each experiment(PSNR and MSE), the first value is Peak signal to noise ratio (PSNR) , this ratio is used as a quality measurement between two images. If the ratio of PSNR is high the images has the best quality, the second measurement value is Mean Squared Error (MSE) which is the difference between original image and a modified image (stego image). The proposed algorithm shows more satisfied experimental out comes.

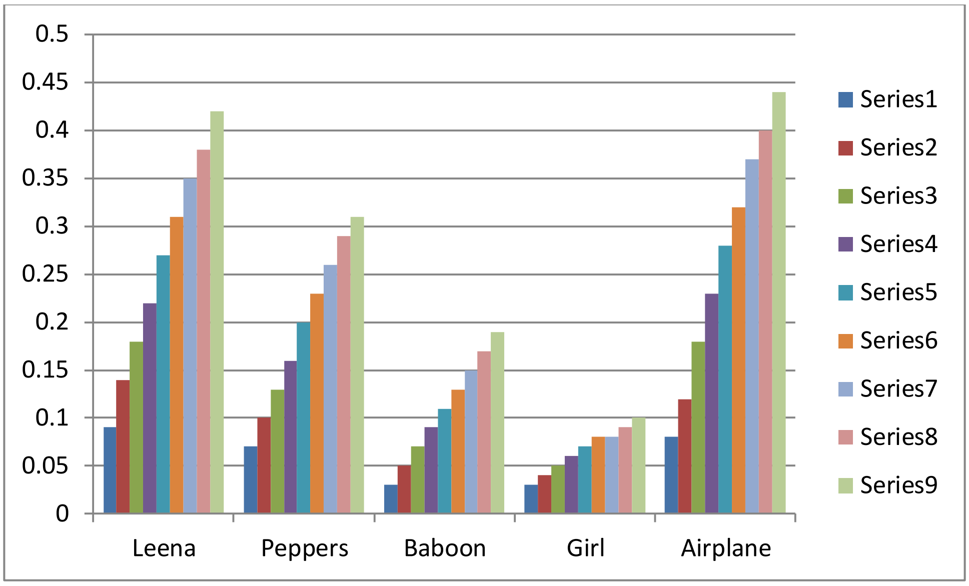
There are many experiments have been conducted through different size of Secret messages and concealed in RGB images (png, bmp extentions) with different size as a cover image, the output is stego images.

Figuer (6.1) show image quality by comparing between the original images after embedding the secret data inside it by using PSNR of the images (leena, peppers, baboon, airplan.girl).



Figuer (6.1): Shows the PSNR test on the images (leena, peppers, baboon, and airplan.girl).

Figure 6.2 show the result value of MSE on the images (leena, peppers, baboon, and airplan.girl).



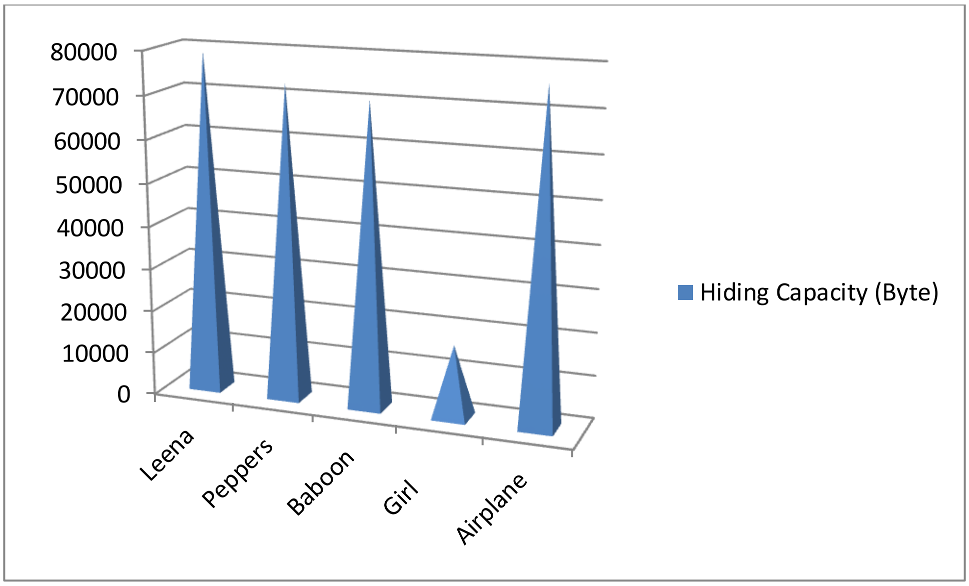
Figuer (6.2): Shows the MSE test on the images (leena, peppers, baboon, and airplan.girl).

After the completing all experiments of the PSNR and MSE values that have been calculated for each experiment, the results of each experiment were taken and Compared with each other after making summariziation. The best PSNR value is resulted 63.37 For Girl stego_image and the low MSE value is resulted at the Girl image.

Some results have been concluded from experimental results which explain the factors affecting in image quality after applying the proposed method. The most important factors are the quality of stego image, whenever the size of secret message hide is increased, the quality of stego image (PSNR) decreased. Mean Squared Error (MSE) increased the size of secret message hiden and the MSE increases.

The data load that embedded by using the proposed algorithm is bigger than the data which is embedded by other algorithms(Gutub, 2010; NOLKHA et al., 2016) and the reason for that the proposed algorithm can be embedded from 3 bit to 6 bits in each pixel and the secret messaage is hidden at the least significant bits of the pixels with more randomization.

Figuer 6.3 shows the payload inside the following images (leena, peppers, baboon, and airplan.girl).



Fiuger (6.3): shows the payload inside the images (leena, peppers, baboon, and airplan.girl).

Testing robustness using stegoExpose tools shows the robust proposed algorithm. It used another image to affect the characteristics image on the robust image. the resulted percentage of the detection is not fixed which mean the Characteristics dose not affect in the robust. After testing the security by using histogram analysis, we can conclude that the hiding capacity of the proposed algorithm shows more satisfied experimental resulting. It retains good visual clarity of stego images. In the histogram analysis the histogram of red channel,green and blue channel can be easily noticeable when increasing the size of secret message.

6.2 Future Works

The following operations can be carried out to improve the performance of this algorithm:

1. The proposed algorithm is used to hide data using the 24-bit RGB images. Thus, this study can be expanded to 32-bit RGB images to image format png.bmp.

2. Increase the System functionality to hide all other data types such as audio, video images not only text data.

The Reference List

The Reference List

Akhtar, N., Johri, P., & Khan, S. (2013). *Enhancing the security and quality of LSB based image steganography.* Paper presented at the Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on.

Al-Korbi, H. A., Al-Ataby, A., Al-Taee, M. A., & Al-Nuaimy, W. (2016). HIGHLY EFFICIENT IMAGE STEGANOGRAPHY USING HAAR DWT FOR HIDING MISCELLANEOUS DATA. *Jordanian Journal of Computers and Information Technology, 2*(1), 17-36.

Al-Mohammad, A. (2010). *Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility.* Brunel University, School of Information Systems, Computing and Mathematics Theses.

Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012). *An introduction to image steganography techniques.* Paper presented at the Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on.

Barhoom, T. S., & Mousa, S. M. A. (2015). A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm. *International Journal of Research in Engineering and Science (IJRES), 3*(3).

Bateman, P., & Schaathun, H. G. (2008). Image steganography and steganalysis. *Department Of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom, 4th August*.

Challita, K., & Farhat, H. (2011). Combining steganography and cryptography: new directions. *International Journal of New Computer Architectures and their Applications (IJNCAA), 1*(1), 199-208.

Chatterjee, D., Nath, J., Dasgupta, S., & Nath, A. (2011). *A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm.* Paper presented at the Communication Systems and Network Technologies (CSNT), 2011 International Conference on.

Das, R., & Tuithung, T. (2012). *A novel steganography method for image based on Huffman Encoding.* Paper presented at the Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on.

Devi, K. J. (2013). *A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique.* National Institute of Technology-Rourkela.

Goel, S., Kumar, P., & Saraswat, R. High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator.

Gupta, A., & Garg, R. (2010). Detecting LSB Steganography in Images.

Gutub, A. A.-A. (2010). Pixel indicator technique for RGB image steganography. *Journal of Emerging Technologies in Web Intelligence, 2*(1), 56-64.

HUSSEIN, H. A. (2015). *Multi Level Image Steganography by Using Pixel Intensity.* Sudan University of Science and Technology.

Islam, M., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. (2014). *An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography.* Paper presented at the Informatics, Electronics & Vision (ICIEV), 2014 International Conference on.

Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014). *An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography.* Paper presented at the Informatics, Electronics & Vision (ICIEV), 2014 International Conference on.

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26-34.

Karim, M. (2011). *A new approach for LSB based image steganography using secret key.* Paper presented at the 14th International Conference on Computer and Information Technology (ICCIT 2011).

Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011). *A new approach for LSB based image steganography using secret key.* Paper presented at the Computer and Information Technology (ICCIT), 2011 14th International Conference on.

Khalil, M. (2011a). Image Steganography: hiding Short Audio Message within Digital Images: JCS&T.

Khalil, M. (2011b). Image steganography: hiding short audio messages withidin digital images. *Journal of Computer Science & Technology, 11*.

Kukapalli, V. R., Rao, B. T., & Reddy, M. B. S. Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare.

Laskar, S. A., & Hemachandran, K. (2013). Steganography based on Random Pixel Selection for Efficient Data Hiding. *International Journal of Computer Engineering and Technology, 4*(2), 31-44.

Meghanathan, N., & Nayak, L. (2010). Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *international journal of Network Security & Its application (IJNSA), 2*(1), 43-55.

Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). *An overview of image steganography.* Paper presented at the ISSA.

Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. *arXiv preprint arXiv:1503.00388*.

NOLKHA, R., VERMA, A., AGRAWAL, G., & VISHWAKARMA, V. P. (2016). A Secured Image Steganographic Technique for RGB Images Using Discrete Wavelet Transform.

Raphael, A. J., & Sundaram, V. (2011). Cryptography and Steganography- A Survey. *International Journal of Computer Technology and Applications, 2*(3).

Ren-Er, Y., Zhiwei, Z., Shun, T., & Shilei, D. (2014). *Image Steganography Combined with DES Encryption Pre-processing.* Paper presented at the Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on.

Sharma, S., & Kumar, U. (2013). Review of Transform Domain Techniques for Image Steganography. *International Journal of Science and Research (IJSR), 4*(5), 4.

Sharma, V. K., & Shrivastava, V. (2012). A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize detection. *Journal of Theoretical and Applied Information Technology, 36*(1), 1-8.

Sumathi, C., Santanam, T., & Umamaheswari, G. (2014). A Study of Various Steganographic Techniques Used for Information Hiding. *arXiv preprint arXiv:1401.5561*.

Swain, G., & Lenka, S. K. (2012). A Novel Approach to RGB Channel Based Image Steganography Technique. *Int. Arab J. e-Technol., 2*(4), 181-186.

Thangadurai, K., & Sudha Devi, G. (2014). *An analysis of LSB based image steganography techniques.* Paper presented at the Computer Communication and Informatics (ICCCI), 2014 International Conference on.

Tiwari, N., & Shandilya, M. (2010). Secure RGB image steganography from pixel indicator to triple algorithm-an incremental growth. *International Journal of Security and Its Applications, 4*(4), 53-62.

Weiss, M. (2012). Principles of steganography.

Wu, H.-C., Wang, H.-C., Tsai, C.-S., & Wang, C.-M. (2010). Reversible image steganographic scheme via predictive coding. *Displays, 31*(1), 35-43.