MEU جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY

Enhancement of A Steganographic algorithm for Hiding Text Messages in Images

تعزيز خوارزمية تقنية فن الاختزال
لإخفاء الرسائل النصية داخل الصور

By

Yazan Abdallah . H . Seidan

Supervisor

Dr. Oleg Victorov

Submitted in Partial Fulfillment of the Requirements for

the Master Degree in Computer Science

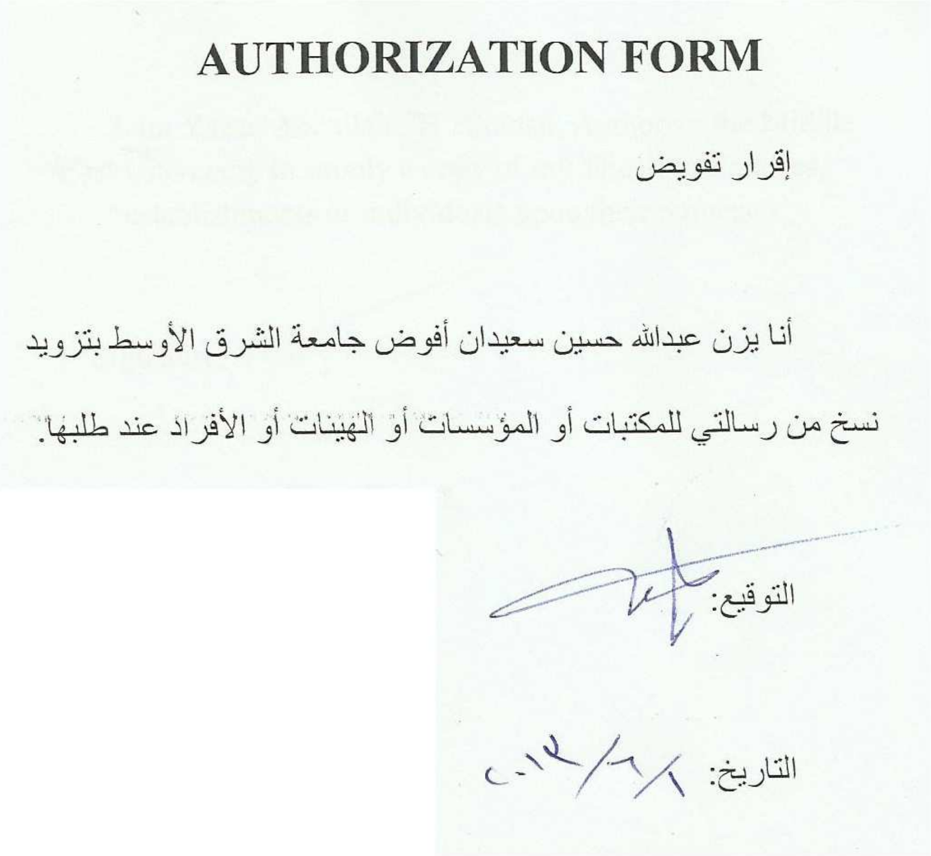
Department of Computer Science

Faculty of Information Technology

Middle East University

Amman, Jordan

June, 2013



AUTHORIZATION FORM

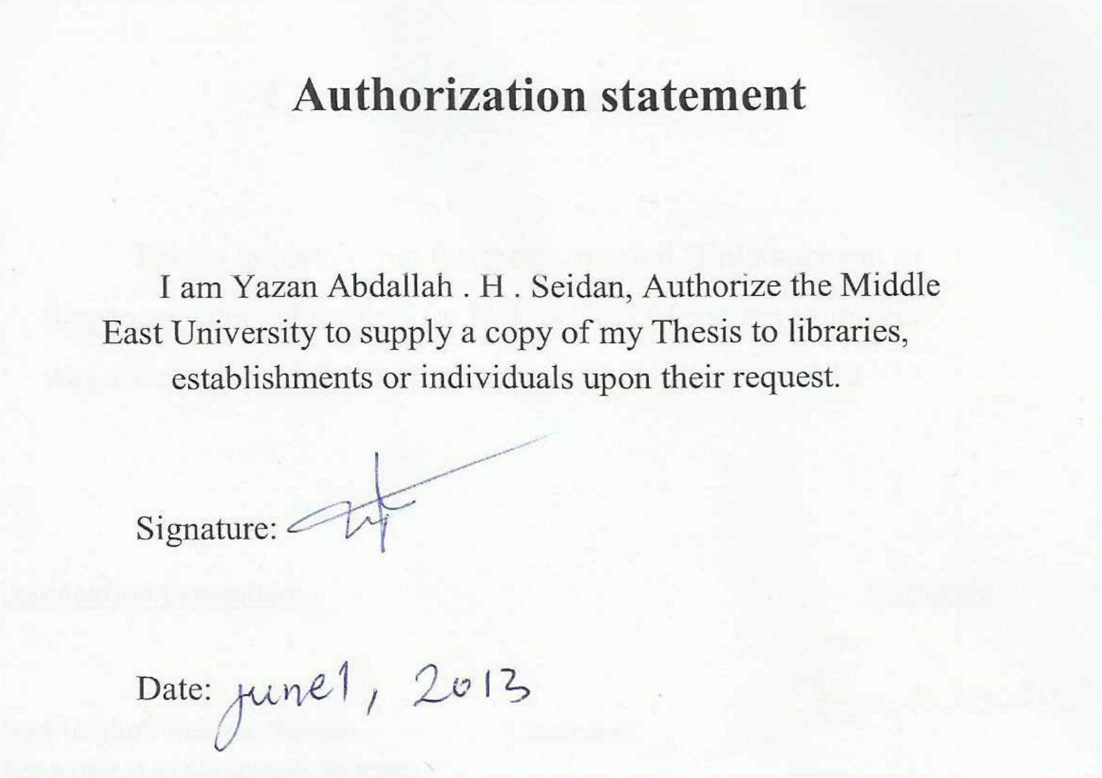
إقرار تفويض

أنا يزن عبدالله حسين سعيدان أفوض جامعة الشرق الأوسط بتزويد

نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الأفراد عند طلبها.

التوقيع:

التاريخ: ١/٦/٢٠١٢



Authorization statement

I am Yazan Abdallah . H . Seidan, Authorize the Middle East University to supply a copy of my Thesis to libraries, establishments or individuals upon their request.

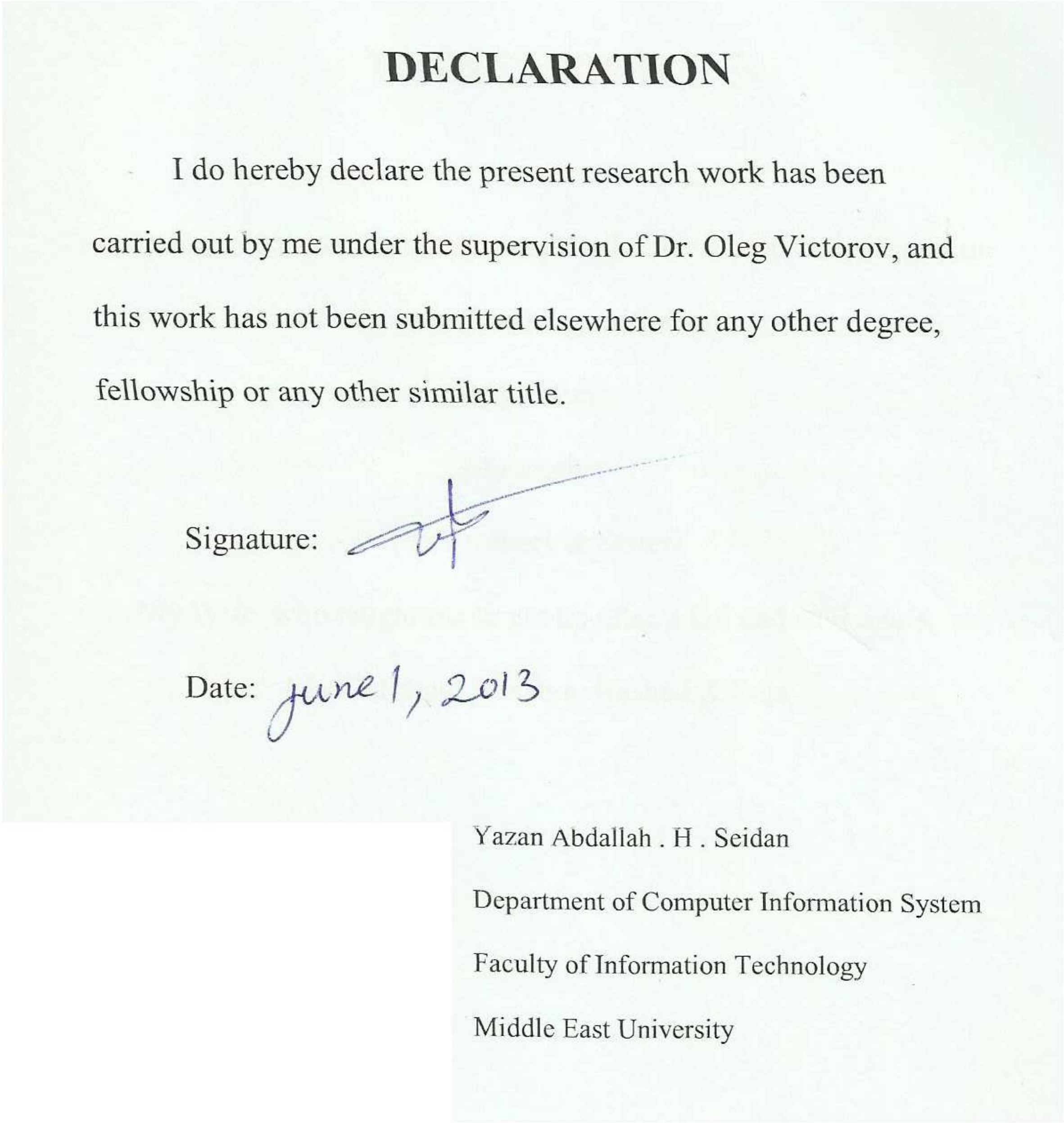
Signature:

Date: june1, 2013

Committee Decision

This is to certify that the thesis entitled "Enhancement of A Steganographic algorithm for Hiding Text Messages in Images" was successfully defended and approved on June 1st 2013

Examination Committee		**Signature**
Prof. Reyadh Shaker Naoum **Department of Computer Science** **(Middle East University)**	**Chairman**	R. Naoum
Dr. Oleg Victorov **Department of Computer Science** **(Middle East University)**	**Member & Supervisor**	
Dr. Mohammad Hassan Alharibat **Department of Computer Science** **(Middle East University)**	**Member**	



DECLARATION

I do hereby declare the present research work has been carried out by me under the supervision of Dr. Oleg Victorov, and this work has not been submitted elsewhere for any other degree, fellowship or any other similar title.

Signature:

Date: june 1, 2013

Yazan Abdallah . H . Seidan
Department of Computer Information System
Faculty of Information Technology
Middle East University

DEDICATION

This thesis is dedicated to all the people who never stop believing in me

and who along with God

My father

My mother

My Brothers & Sisters

My Wife, who taught me to get up after a fall and start again.

My Children: Hashem, Rashed & Saja

ACKNOWLEDGMENTS

I would like to thank my father and my mother for their continuous support during my study.

I also would like to thank my great supervisor Dr. Oleg Victorov for his support, encouragement, proofreading of thesis drafts, and for helping me throughout my studies, putting me in the right step of scientific research. I would like to thank the Information Technology Faculty members at the Middle East University. I would also like to thank all of my family members .

Table of Contents

Submitted in Partial Fulfillment of the Requirements for I

the Master Degree in Computer Science.. I

Department of Computer Science.. I

Faculty of Information Technology.. I

Middle East University I

Amman, Jordan.. I

June, 2013 I

AUTHORIZATION FORM..II

Authorization statement III

DECLARATION..V

DEDICATION VI

ACKNOWLEDGMENTS.. VII

Table of Contents...VIII

List of Figures XIII

List of Tables.. XVI

List of Abbreviations XVII

Abstract XVIII

الخلاصة XIX

Chapter One... 1

Introduction 2

1.1. Introduction 2

1.2. Problem definition... 4

1.3. Objectives 5

1.4. Significance of the problem... 5

1.5. Thesis Organization 6

Chapter Two 8

Information Hiding 9

2.1. Introduction 9

2.2. Importance of Information Hiding... 10

2.3. Applications of Information Hiding... 11

2.4. Overview on the subject 12

2.5. Classifications of Information Hiding.. 13

Chapter Three 15

Principles of Steganography 16

3.1. Overview 16

3.2. Prisoners problem 18

3.3. Steganography Terminology 19

3.4. Steganography Goals 21

3.5. Steganography Types 22

3.5.1 Pure Steganography.. 22

3.5.2 Secret Key Steganography 23

3.5.3 Public Key Steganography 24

3.6. System Security of Steganography 25

3.7. Type of Attackers 26

3.7.1 Passive Attacker 27

3.7.2 Active Attacker 27

3.7.3 Malicious Attacker 29

3.8. Steganalysis 29

3.9. Kerckhoff Principles 30

3.10. Steganography System Security 31

3.10.1 Similarity function 31

3.10.2 Entropy function 33

3.11. Invisibility of Steganography 33

Chapter Four 35

Related works 36

4.1. Introduction 36

4.2. Substitution systems 37

4.2.1 Least Significant Bit (LSB): 37

4.2.2 PSEUDO-RANDOM PERMUTATIONS 40

4.2.3 Image Downgrading and cover Channels 42

4.2.4 Quantization and Dithering 43

4.2.5 Cover-Regions and Party Bits 45

4.2.6 Information Hiding In Binary Image 45

4.3. Transform Domain Techniques 47

4.4. Statistical Steganography 48

4.5. Distortion techniques 49

4.6. Cover Generation Techniques 49

4.7. Gutub's Pixel Indicator Algorithm 50

4.8. Ghosal's New Pair Wise Bit Algorithm 53

4.9. Analytical study of the previous techniques 56

Chapter Five 58

Proposed Algorithm 59

5.1. Overview 59

5.2. The Proposed Model 59

5.2.1 Embedding Algorithm 60

5.2.2 Extraction Algorithm 62

5.2.3 Example 67

Chapter Six 70

Experimental Results 71

6.1. The Image Quality Test 71

6.2. Payload 76

6.3. Security Test 86

6.4. Robustness 90

Chapter Seven.. 91

Conclusions 92

7.1. Overview 92

7.2. Analystic Results 92

7.3. Future Works 95

References.. 96

List of Figures

Figure (2-1) Classifications of Information Hiding...................................... 14

Figure (3-1) Prisoners problem 18

Figure (3-2) Overview of Steganographic System 19

Figure (4-1) Classifications of the Steganography 36

Figure (4-2) Substitution Systems Methods... 37

Figure (4-3) Image and cover Channels... 42

Figure (4-4) Gutub's hiding algorithm flowchart.. 51

Figure (4-5) Gutub's recovery algorithm flowchart 52

Figure (5-1) Flowchart of a proposed embedding algorithm 65

Figure (5-2) Flowchart of a proposed extraction algorithm........................... 66

Figure (6-1) Shows the PSNR test for Animal 1 image 73

Figure (6-2) Shows the PSNR test for Animal 2 image 73

Figure (6-3) Shows the PSNR test for Animal 3 image 73

Figure (6-4) Shows the PSNR test for Animal 4 image 74

Figure (6-5) Shows the PSNR test for Animal 5 image 74

Figure (6-6) Shows the PSNR test for Animal 6 image 74

Figure (6-7) Shows the PSNR test for Animal 7 image 75

Figure (6-8) Shows the PSNR test for Animal 8 image 75

Figure (6-9) Shows the PSNR test for Football 1 image 75

Figure (6-10) Shows the PSNR test for Football 2 image 76

Figure (6-11) shows the payload inside Animal 1 image 77

Figure (6-12) shows the payload inside Animal 2 image 78

Figure (6-13) shows the payload inside Animal 3 image 78

Figure (6-14) shows the payload inside Animal 4 image 78

Figure (6-15) shows the payload inside Animal 5 image 79

Figure (6-16) shows the payload inside Animal 6 image 79

Figure (6-17) shows the payload inside Animal 7 image 79

Figure (6-18) shows the payload inside Animal 8 image 80

Figure (6-19) shows the payload inside Football 1 image 80

Figure (6-20) shows the payload inside Football 2 image 80

Figure (6-21-A) Cover-image for (Animal 1) with size 1024X1024 81

Figure (6-21-B) Stego-image for (Animal 1) with size 1024X1024 81

Figure (6-22-A) Cover-image for (Animal 2) with size 1024X1024 81

Figure (6-22-B) Stego-image for (Animal 2) with size 1024X1024 81

Figure (6-23-A) Cover-image for (Animal 3) with size 1024X1024 82

Figure (6-23-B) Stego-image for (Animal 3) with size 1024X1024 82

Figure (6-24-A) Cover-image for (Animal 4) with size 1024X1024 82

Figure (6-24-B) Stego-image for (Animal 4) with size 1024X1024 82

Figure (6-25-A) Cover-image for (Animal 5) with size 1024X1024 83

Figure (6-25-B) Stego-image for (Animal 5) with size 1024X1024 83

Figure (6-26-A) Cover-image for (Animal 6) with size 1024X1024 83

Figure (6-26-B) Stego-image for (Animal 6) with size 1024X1024 83

Figure (6-27-A) Cover-image for (Animal 7) with size 1024X1024 84

Figure (6-27-B) Stego-image for (Animal 7) with size 1024X1024 84

Figure (6-28-A) Cover-image for (Animal 8) with size 1024X1024 84

Figure (6-28-B) Stego-image for (Animal 8) with size 1024X1024 84

Figure (6-29-A) Cover-image for (Football 1) with size 1024X1024............ 85

Figure (6-29-B) Stego-image for (Football 1) with size 1024X1024............ 85

Figure (6-30-A) Cover-image for (Football 2) with size 1024X1024........... 85

Figure (6-30-B) Stego-image for (Football 2) with size 1024X1024............ 85

Figure (6-31) Histogram of Original Animal1.bmp 86

Figure (6-32) Histogram of Stego-Animal1.bmp.. 87

Figure (6-33) Histogram of Original Football1.bmp..................................... 87

Figure (6-34) Histogram of Stego-Football1.bmp... 88

Figure (6-35) Histogram of Original Football2.bmp..................................... 88

Figure (6-36) Histogram of Stego-Football2.bmp... 89

Figure (7-1) Shows the PSNR test on the following images : 93

Figure (7-2) shows the payload inside the following images : 94

List of Tables

Table (4-1) Represents the differences between the adjacent pixels............. 43

Table (4-2) Shows the the indicator and the hidden status inside the other channels 50

Table (5-1) Shows indicator and the hidden status....................................... 61

Table (5-2) Shows the 24-bit RGB image color space and indicator position........ 61

Table (5-3) Channel parts.. 62

Table (5-4) Hide process.. 62

Table (5-5) Shows pixels before and after hiding 68

Table (6-1) the image quality test (PSNR) 72

Table (6-2) Show Payload of data which can be embedded in different 24-bit colored bmp images.......... 77

List of Abbreviations

DCT	Discrete Cosine Transformation
HVS	Human Vision System
LSB	Least Significant Bit
MSE	Mean-Squared –Error
PSNR	Peak-Signal-To-Noise Ratio
SNR	Signal-To-Noise Ratio

Abstract

The method of steganography means the ability of hiding data inside a cover. Steganography helps to hide data in another of a different type , and thus it can guarantee a high degree of security.

Previous studies proposed many algorithms that hide text inside colored images, some of these the algorithms depend on hiding data directly in a special domain. There are other algorithms that depend on changing the image shape into another using discrete cosine functions (Transform domain techniques).

The study proposed a new improved technique that takes the advantage of the 24 bits in each pixel in the RGB images and hiding data directly in a special domain, using the two least significant bits of red channel to indicate existence of data in the other two channels which are green and blue. The number of bits which will be embedded in the right part are counted in the lift part of the channel which chosen for embedding. This algorithm is characterized by the ability of hiding larger size of data and the data were embedded inside the image randomly in a new randomization technique which gave the message a higher security and resistance against extraction by attackers.

This algorithm has been compared with other known algorithms and the new results proved the power of the new algorithm to hide and extract data.

الخلاصة

طرق فن الاختزال هي واحدة من أقدم الطرق التي استخدمت لإخفاء البيانات. أي إخفاء البيانات داخل غطاء معين مختلف، وبالتالي فإنه يمكن أن يضمن درجة عالية من الأمان.

اقترحت في العديد من الدراسات السابقة خوارزميات تم من خلالها إخفاء النصوص داخل الصور الملونة، وبعض هذه الخوارزميات اعتمدت على إخفاء البيانات في الصورة بشكل مباشر ، وهناك خوارزميات أخرى اعتمدت على تغيير شكل الصورة إلى شكل آخر باستخدام دوال جيب التمام المنفصل .

أما هذه الدراسة فقد اقترحت خوارزمية جديدة مطورة يتم من خلالها تضمين البيانات داخل الصور الملونة RGB حيث تستفيد من وجود 24 ثنائية لكل بكسل لإخفاء البيانات داخل الصورة بشكل مباشر، باستخدام ثنائيتين من الجزء الأقل أهمية من قناة اللون الأحمر لتتم الإشارة إلى مكان وجود تضمين للبيانات في القناتين الأخريين وهما الأخضر والأزرق، حيث يتم تقسيم القناة إلى قسمين و من خلال القسم الأكثر أهمية يتم إيجاد عدد الثنائيات التي ستتضمن داخل القسم الأقل أهمية من القناة، وقد امتازت هذه الخوارزمية بقدرتها على إخفاء حجم كبير من البيانات، وطريقة جديدة لإخفاء البيانات بشكل عشوائي، مما أكسبها أمنية و مقاومة أعلى ضد استخراج الرسالة من قبل المخربين.

وقد تمت مقارنة الخوارزمية المقترحة مع غيرها من الخوارزميات المعروفة وأثبتت النتائج الجديدة قوة الخوارزمية الجديدة لإخفاء واستخراج البيانات.

Chapter One

Chapter One

Introduction

1.1. Introduction

Communication process is considered the most important means that helped human growth in all fields of life where the human being sought since his existence on this earth to find ways to facilitate the process of communication and intellectual exchange between different peoples, and the oldest methods that humans used : first, drawing on the caves, then use of smoke and drums to signify a particular event, followed by the human thought developed by invention of writing through using certain symbols known as letters, afterward the telegraph was invented which helped the communication process, subsequently the radio, television, and telephone, as characterized by the previous methods for the transfer of sound and image in the same time, and finally the latest and most modern means of communication is electronic mail (e-mail) which reduced the time and effort in transferring the data and information.

The development in communication means was accompanied by the easy access to confidential public and private data. For this reason, Human did his best to find different ways for maintaining the confidentiality and integrity of data which prevent the unauthorized personnel to know them. If there is no confidentiality of data transferring, it becomes so difficult to transmit them especially the military data and data related to economic, industrial organization besides the information pertaining the institutions of finance and business. A result there is a need for information hiding which is a term that expresses the general methods and techniques used in the field of security and confidentiality of information security upon transferring them from one side to another. This is one of the most important problems that have emerged because of the various means of communications. Consequently, the most important methods used in this area was encryption that depend on the transfer of confidential data from one format to another using certain ways by the sender until it reaches to the recipient who works to restore them to their original form. Afterwards, ways of expression has evolved and varied, besides, it became well-known to a lot of vandals who can resolve the coding easily in many cases, although, some of them are still maintaining the power for data's security. Therefore the need occurs for finding new techniques to protect the data. Steganography is one of them. This term derived from a Greek terminology where the word Stegano means hidden or restricted and the word Graphy means a message , writing or drawing (Petiticales, 1999) specifically. This method was known since the Greek's Age and developed later on with the advancement of the communications' means and the emerging of the Internet which processed transferring of the digital data aiming at hiding the secret data inside other objects such as : texts, images, sounds and video in which the sender embeds the secret messages inside the (original object) where it gives the highest level of security by changing the public entity of confidential data, subsequently, for maintaining the data security, they should not be materialistic seen as well as they have to be similar to the real object after their hiding. Even attackers cannot discover this stego object upon its transferring among the Internets until reaching the extraction of the secret data from inside the object in a certain way.

The concept of steganography has considerably been given much attention in recent years in order to overcome such problems. The primary aim of steganography is to hide data in cover media such as image, text, audio and video so that others will not notice it. The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. For example, that picture of your face can conceal the plans for your company's latest technical innovation.

There are currently three effective methods in applying image steganography: least significant bit (LSB) substitution, blocking, palette modification. LSB substitution is the process of modifying the least significant bit of the pixels of the carrier image. LSB substitution method ubiquity among carrier formats and message types. LSB substitution lends itself to become a very powerful steganographic method.

1.2. Problem definition

Steganography is used to hide messages in the cover media like text, image, audio and video. We focus on images as a cover media. A algorithm is needed to determine how the message it will be embedded. This algorithm can be more or less advanced using simple or complex LSB embedding in the spatial domain.

The actual hiding process begins with embedding bits of the message into the cover image. In LSB insertion technique the message will be embedded in the least-significant bit. For increasing the embedding capacity, two or more bits in each pixel can be used to embed messages by changing the LSB of pixels in a sequential manner. Most techniques in use today are invisible to a human senses and most of it takes a gray color images as a special case. In this context there are two aspects should be considered in order to embed a text message using a color image as a cover these are :

1- How to choose the pixel for embedding.

2- Embed messages by changing the LSB of pixels in a different randomization technique.

1.3. Objectives

The main objectives of this thesis are:

1) Designs and develop a new technique to pick up the pixel for an embedding.
2) Increase the size for embedded text.
3) Give a high degree of confidentiality to resist extraction process.

1.4. Significance of the problem

The study will address a special kind of problem which is categorized under the digital image steganography problem, until now, there are no optimal technique used to solve this problem, but many suggested algorithms give us good results. It will focus on hiding the text message in the least significant bits of the pixels in a BMP image.

The study will be focused on how to choose a pixel to embed a part of the text message in it under a conditional value in order to get some results about its ability to make the message store in random way. Also after choosing the pixel it will make another condition to how to store.

In this thesis, we address modern steganography . Although the topic of steganography exists since ancient times, and many of the general assumptions still apply today. Much of the recent work in steganography is in the area of invisible digital watermarking motivated by the desire for copyright protection of multimedia on the internet.

The objective of digital watermarking is to embed a signature within a digital cover signal to signify origin or ownership. Another type of data hiding is steganography. The objective of steganography is to imperceptibly embed a significant amount of data, much more than that of a signature or serial number, in to the cover signal.

1.5. Thesis Organization

The thesis contains six chapters:

Chapter 1 provides an Introduction. Chapter 2 provides an overview of information Hiding. Chapter 3 contains the Principles of Steganography in details. Chapter 4 listing and explaining different steganography methods and also list different related works. Chapter 5 provides the proposed Algorithm in details. Chapter 6 contains the experimental results of the designed Algorithm and it's also discusses the results with other Algorithms; Finally, chapter 7 contains the conclusion, future work suggestions.

Chapter Two

Chapter Two

Information Hiding

2.1. Introduction

Information hiding was known since the ancient times used by spies, armies and statesmen where they used to hide the data inside written letters and in the context of speech. Moreover, history tells us many stories that have been used in steganography ways to hide data including a story refers back to the year 440 BC when one of the Greeks' leaders shaved one of his slaves then made a tattoo on his head which was a message stated that " your land will be occupied by another country " then left the slave until his hair grew and thus hid the letter under the hair of the slave and send him to another leader and when he arrived to the second one , he also shaved his head and read the content of the message and accordingly he protected the state from occupation (Kahn,1983).

In this regard, other stories were also reported when Harpagus wrote a message on the internal part of the rabbit's stomach and then transferred it in unsuspected way to King Cyrus of Persia who helped him to defeat the battle of King Medas against Persia (Kahn, 1983). The predesessors used wax to hide the written information on the wood boards until it reaches to the recipient who removed the wax material and read the content of the message.

During the Second World War, different liquids such as: milk, vinegar, fruit juices and urine were used for writing the secret letters on paper. When it reaches the recipients they draine or heate the message until fluid becomes dark color. As a result it facilitated reading the message content. After that, invisible inks are used for writing letters, subsequently the content of the message is extracted using heat or some chemical reactions (Febien et al, 1999).

Furthermore, the Germans invented a technique known as Microdot which was a photographic image with certain size and clarification degree, write on them by using the stitches and pin over the characters of the message since that the writing will not appear unless, the recipient putting a paper under the image for facilitating its reading, this way was developed by the progress of movies pictures and lenses that reduced the size of the secret message (Khader, 2004).

Additionally, the real evolution of steganography started since the beginning of the nineties when the companies and secret organizations used digital photos, animation and voice messages to hide their secret data.

2.2. Importance of Information Hiding

When the sender processes a message that he wants to deliver to another person, such step is not that important comparing it with delivering that message to its destination without an increase or decrease or otherwise, loss of the whole message. The same rule applies to the owners of intellectual property who is seeking to protect their property from theft or loss.

Computers and printers helped to increase the speed of data transfer and less variety such as: text, images, audio, and video inside networks which makes it easier to use this data to hide other information without the need of that can be disassembled, so steganography methods were used which can encrypt data before embedded them inside the cover for giving them the highest production degree, It should be noted that the method of steganography is not connected with encryption operation neither it is not from its requirements nor it is not considered to be a standard for measuring the power used in the degree of the information hiding due to the fact that many steganography methods are stronger than encryption techniques.

2.3. Applications of Information Hiding

There are a set of applications that use the concept of hiding data as follows:

1- Covert communications: individuals and groups need to write to each other without allowing the others to see these messages, therefore they use the method of steganography for transferring confidential and secret news, information as well as covert communications are used by the intelligence, the armies and secret organizations to prevent the spies for knowing the secret data and messages.

2- Ownership: commercial companies, film and television stations, publishing houses are characterized by a mark or trademark of their own to protect their rights of copyright and distribution of their respective owners, especially if they publish them by using the Internet, and to solve the problem of theft of trade marks devised a set of algorithms resistance to sabotage operations using watermarks.

3- Authentication: where is the process of verifying the integrity of data between sender and recipient of the processes of change that may take place upon by attackers for this purpose, devised a set of algorithms to resist modification operations.

4- Data embedding: it is the process of hiding secret information inside other data using certain algorithms, and then extracts them using the methods of steganography.

2.4. Overview on the subject

Steganography is considered as one of the modern and active science due to its importance in the field of security data during the correspondence which embed the secret message inside the cover where it can be text, image, sound or video and then extract the secret message by the recipient based on the methods used in the process of hiding that depends on the characteristics of the communication system, for example, the amount of data that can be included and extraction on the capacity of the communication channel.

There are certain criteria that must be taken into account when dealing with methods of concealment as follows:

1- Imperceptibility: the cover used in the process of concealment should not be visible neither clearly defined for the attackers, and when a process of inclusion done, it must take into consideration the selected file type for inclusion, and place of inclusion within it.

2- Payload: it is the amount of data that can be hidden inside the cover without affecting it.

3- Undetectability: it is a lack of ability to extract confidential data hidden inside the cover, except by authorized personnel only.

4- Removal Resistance: it is the inability of attackers to conduct modifications and processing on the cover, such as image processing, compression and recycling...etc.

Imperceptibility and the inability of attackers to detect hidden data depend on their percentage comparing with the size of the cover and this term is called “Signal –To-Noise Ratio” (SNR) (Marvel et al, 1999).

Standard resistance to vandalism and the size of the data together are not conditional for steganography, for example, when you hide a secret message inside the cover, the way of steganography that can take into account the volume of data that included inside the cover for their resistance to vandalism, but in the watermark, they care to resist vandalism more than the size of the data itself.

2.5. Classifications of Information Hiding

There are different classifications ways to hide data, some of them considered that the watermark is part of the steganography, and considered some of the encryption that is part of the system to hide information. Figure (2-1) is the closest classification to the subject of the study. (Al-Oqily, 2003).

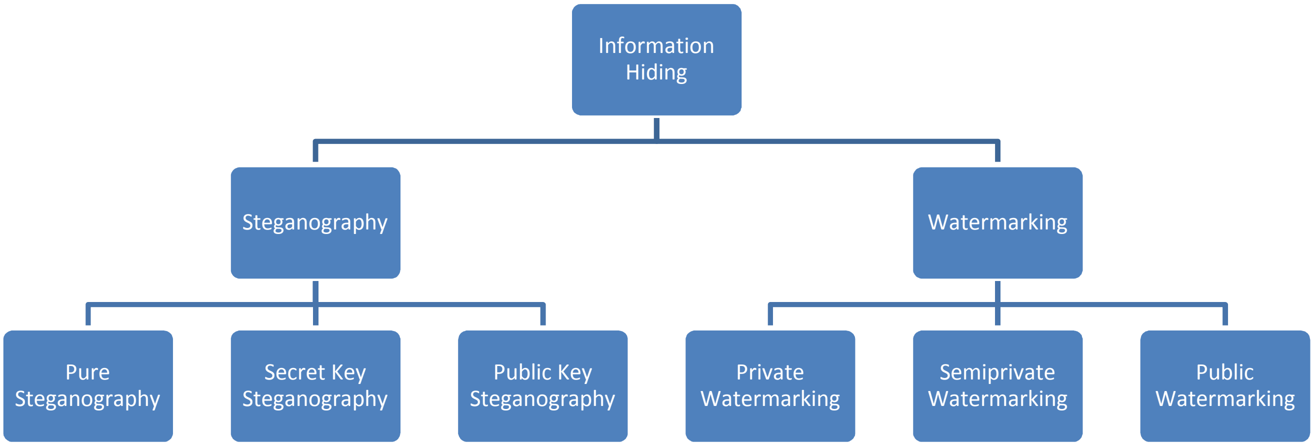


Figure (0-1) Classifications of Information Hiding

Chapter Three

Chapter Three

Principles of Steganography

3.1. Overview

What kind of methods used to protect data as they travels within the network? Besides, how can we protect these data from detection, removable or vandalism? In addition to that, how these data get to their destination without reduction or defect? And what is the reason behind the search for ways of alternative or complementary to the old ways and modern ones?

The process of encryption methods is used to protect data which based on the use of symbols, besides, codes, and the use of complex mathematical methods for converting the data into another picture that is difficult to read , except by the concerned recipients, (Who is informed in a pre-code decoder) and encryption for military purposes and spying has long history, and it is still currently being used to protect trade secrets as well as transferring data securely over the Internet. Despite what is provided by the encryption methods in the field of information security, but it has not given the required security level of the data, as there are those who are looking for ways harder to crack encryption. Moreover, there are those who look for a mechanism to break the encryption, because the text can distinguish it from the encrypted text is not encrypted, making it easier for attackers to conduct frequent experiments possibility to get encrypted data, because the use of encryption in a certain way repeatedly to help attackers dislodge by repeated experiments, which was invited to look for alternative ways more adaptable security and hide in the data, and the methods used in this area, which is the subject of our study in this research is steganography which is an old method, but it coincided with the rapid progress of communications used to hide information inside other data, what is the principle of steganography? And what is different from the encryption technique?

Science is the steganography a science mission in the field of security and concealment of information, which is different from the encryption, but complement it, because to hide the data using one of the ways the steganography reduces the chance to discover hidden data on terrorists, and may have the opportunity non-existent because it gave another layer to protect the data through the development of as text, image, sound, video and then hide data inside the lid produces new figure contains confidential data, and is not aware of the naked eye to ensure that are moving within the network, and is not to extract confidential data in the event was discovered by attackers, but it can be integration between the encryption process and the process of steganography to give it a higher degree of protection besides, weakening the opportunity of discovering the data by the attackers where the sender encrypts the data before embedded into the cover, then the recipient to extract and decrypt data.

3.2. Prisoners problem

For understanding the steganography, it is necessary to clarify the problem of prisoners proposed by the researcher (Simmons, 1983) where the problem includes two prisoners are named Alice and Bob who are jailed in separated rooms and between them Wendy who works as an observer on them and mediator for the transfering of confidential communications between them, without knowing the content, or trying to find out it content and change it before transmitting , This observer can be an example of the observer active or passive, or malicious, and determine the type of controller is linked to significantly complicate the steganography and figure (3-1) illustrates this as follows:

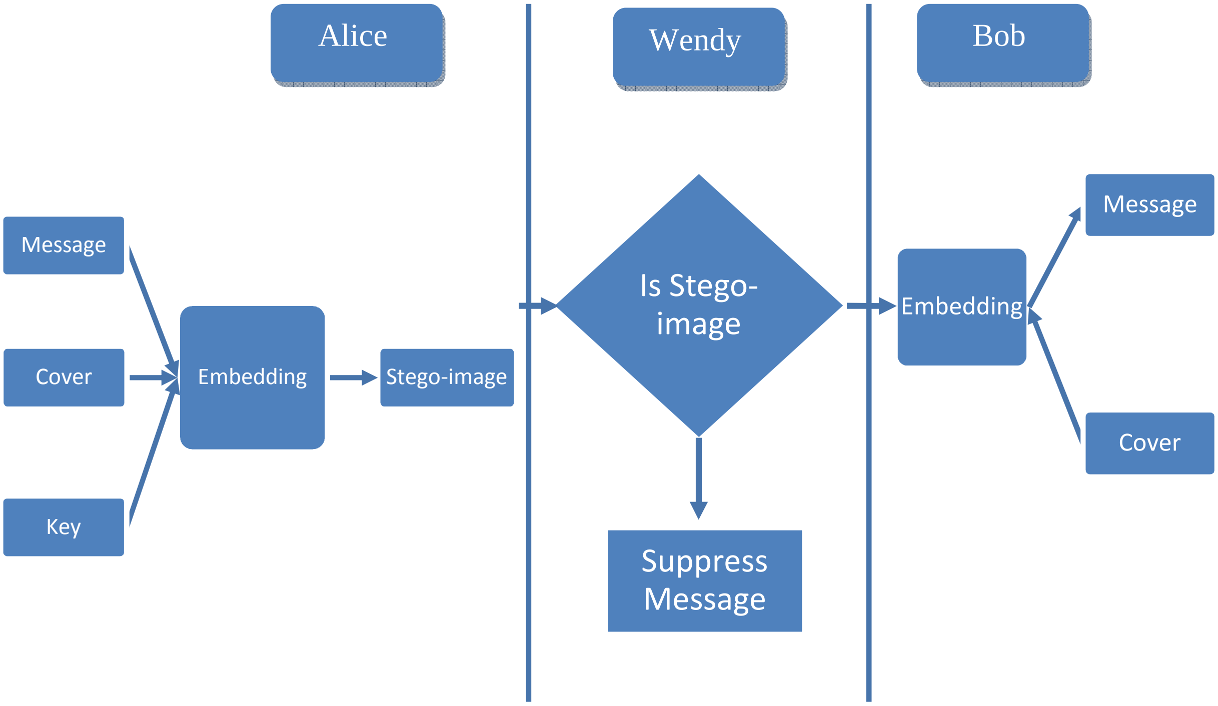


Figure (0-2) Prisoners problem

3.3. Steganography Terminology

Steganography system is divided into two operations as detailed below:

1- Embedding process: from which it can choose the cover then put secret messages included using the stego key that contains the secret message Stego Cover.

2- Extraction process: From which to extract the secret message using the secret key, and can be watched through the lid are moving between the sender and the recipient by the attackers who have no right to extract the secret message and the figure (3-2) illustrates this:

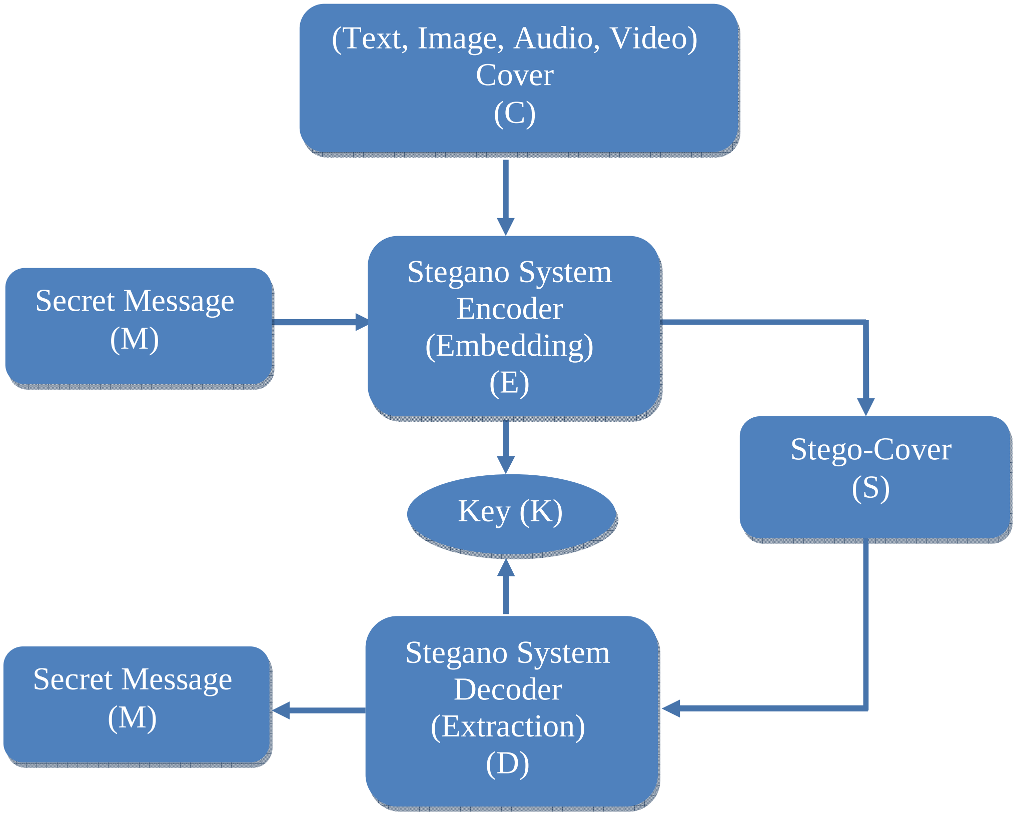


Figure (0-3) Overview of Steganographic System

Figure (3-2), noted the following:-

1- Secret Message (M): Confidential data to be hidden within other data such as hide the text within the image.

M: It indicates data to be hidden.

m: It indicates secret message can be represented by binary system.

L (m): It indicates secret message length.

m_i: it presents bit from the secret message (m).

$1 \leq i \leq L(m) \qquad m_i \in M$

2- Cover (C) : used to hide the secret message (M).

C: It refers to the covers that are used to hide data such as :

text, image, sound, animation.

C: It refers to the cover of the selected image which represents a set of pixels and for each one of them has certain value.

Ci: It refers to one of the pixels.

L (Ci): It is the cover size $1 \leq i \leq L(c)$

In the case of binary representation- $C_i = 0$ OR 1

In the case of Gray Scale Image : $0 \leq Ci \leq 255$

And for each element of the cover C_i an index which represents the element's location inside the cover and the code C_{ij} is used to refer to the element's index inside the cover.

3- Key (K): Is used to hide the secret message (M) inside the cover (C) is called (Stego Key) as :

K: refers to the set of stego-key.
k : refers to one of these keys (methods).

4- Stago Cover(S) refer to System outputs of Steganography which is the cover (C) after hiding the secret message (M) inside it as :

S: refers to the set of covers that contain the data.

s: refers to the secret cover. $s \in S$

L (s): is the size of the secret Cover.

5- Embedding (E): It is the process carried out by the sender to hide the secret message (M) inside the cover (C) as the code (E) refers to the embedding process,the result of this process is to cover the secret (S).

6- Extraction (D): It is the process done by the recipient to extract the secret message (S) which its code is (D).

7- Attackers are the individuals who do not have the right to see the secret message (M) where they may have the secret cover (S) but they cannot be able to extract the data from the cover.

8- Embedder (E): is the person who done embedding.

9- Extractor (D): is the person who done the extraction operation.

3.4. Steganography Goals

The main goals are :

1- To avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised , then this goal is defeated (Katzenbeisser and Petitcolas,2000).

2- To hide a message inside another harmless message in a way that does not allow any attackers to detect that there is a second secret message present (Johnson, 1998).

3- Giving the highest degree of protection for confidential data.

3.5. Steganography Types

As shown in figure (2-1) Steganography is divided into three main types, these types are described in the following sections :

3.5.1 Pure Steganography

Steganography which does not require any previous information between the sender and the recipient is called pure steganography which also does not need a (stego-key) in the embedding neither in the extraction process. The sender in this case depends on ambiguity in protection of the secret data which is considered the minimum security level. The descriptions of the embedding and extraction operations are as follows:

- The embedding process E: C,M→ S
- The extraction process D: C→ M

Note that the two processes do not need a secret key, and that is means that both sender and recipient can reach to the embedding and extraction algorithms, therefore, the steganography consists from the following: the original cover, the secret message, the embedding and extraction processes besides the secret cover). In this form the attacker Wendy does not know the method used by Alice and Bob in hiding the information which is considered a bad hypothesis called the security through the ambiguity. Moreover, the pure steganography does not need any secret information between the sender and the recipient. This means that the Wendy observer can get the algorithms used by Alice and Bob and thus the ability to extract the secret message easily (Katzenbeisser and Petitcalas, 2000).

3.5.2 Secret Key Steganography

The Secret key steganography depending on a secret information which is called a secret key. A person who has this secret key can get a secret message from the stego-image, Both sender and receiver must have the same secret key, so the sender chose a cover then embed the secret message in it by using a secret key which must be known for receiver to obtain the secret message.

$$G = (C, M, K, E_k, D_k)$$

$$E_K : C, M, K \rightarrow S$$

$$D_K : S, K \rightarrow M \quad \Rightarrow \quad D_k(E_k(c, m, k), K) = m \quad for \ m \epsilon M, k \epsilon K$$

Where :

G : steganography system
C : cover
M : secret message
K : secret key
S : stego-image
E_K *: embedding process by secret key*
D_K *: extracting process by secret key*

The securiry of this type depends on a secret key not in the algorihm which used, the security for this type will be very weak when a secret key known , because both Alice and Bob guess that Wendy know the steganography algorithm but he does not know the secret key . (Khader, 2004).

3.5.3 Public Key Steganography

The concept of the Public Key is derived from the Public Key in Cryptographic processes where this method upon use gave the highest degree of protection more than the usage of the private key which is ineffective one.

The above mentioned method depends on two keys: (K_e , K_d) public key and secret key, so the sender embedded the secret message by using a public key (K_e) then the receiver will get the secret message by using a secret key (K_d). The following operations clarify the embedding and extraction:

- Embedding process : $E : C , M , K_e \rightarrow S$
- Extracting process : $D : S , K_d \rightarrow M$

The public key is available for each one while the private key remains secret between Alice and Bob , and there is a relationship between the two keys $(K_e (K_d (m)) \rightarrow M)$ so the sender does a certain process on public key to see the private key $(P , K_e \rightarrow K_d)$.

(P) Indicates the operation done on the public key for knowing the private key.

3.6. System Security of Steganography

System security of steganography consists of 3 parts, Alice and Bob represent the sender and recipient sides where the third side is the observer Wendy, where each of Alice and Bob attempts to hide their secret data by using modern technology to hiding information also Wendy attempts to discover secret data by using methods and techniques which is called steganalysis to attack the security system by supposing that there is a secret message inside the cover or disabling secret message as much as Wendy can. Therefore, the general objective of the steganography is to prevent attackers from obtaining any information about this method because if they any information, they will reach to the secret data resulting that the system is unsecure. (Etting, 1998)

There must be two basic conditions to guarantee steganography as follows:

1- The secret key must remain unknown for the attackers.

2- The original cover should remain also unknown for the attackers. (Zollner et al, 1998).

For securing steganography algorithm, it must have four conditions (Katzenbeisser and petitcolas, 2000):

1- The secret message is embed inside the cover by using public algorithm and recognized secret key to the sender and recipient.

2- The individuals who know the secret key are themselves who are able to extract the entire message.

3- If attackers are able to discover the secret message inside a certain cover, they should not extract it and if they succeeded in extracting part of it, they must not get the entire whole message.

4- Non-application of the calculations to discover secret message.

3.7. Type of Attackers

The attacker is the third party of the communication process by using the steganography. Wendy who represent the observer on Alice and Bob to keep them away from runaway, and informing each other about the secret plans and preventing the message from receiving it or analyzing it for knowing its content or sending it after saving it. Therefore, it is called the Passive or Active or malicious observer.

- If he represents the passive observer, he will decide to send the message or preventing its arrivals to the recipient and attempting to detect the secret message.
- If he represents the active observer, he will try to modify the message.
- If he represents the malicious observer, he will try to change the message and putting obstacles on the correspondence for any message that he receives, Thus resulting a loss of the message content.

Thus Alice and Bob need to a method to resist the attacking operations by Wendy, whereas the algorithms of steganography is complicated, the observer's mission will become more difficult which needs from his side Conclusions and viewpoints to decrypt the algorithms of steganography.

3.7.1 Passive Attacker

The passive attacker can detect the existence of a secret message by using the discrete Laplace operator (Katzenbeisser and Petitcolas, 2000). By this operator it is possible to detect secret messages in grayscale images.

	(x+1,y)	
(x,y-1)	**(x,y)**	**(x,y+1)**
	(x-1,y)	

$$\blacktriangledown^{2}\, p(X,y)=p(x+1,y)+p(x-1,y)+p(x,y+l)+p(x,y-1)-4p(x,y) \qquad (3\text{-}1)$$

Since we can expect neighboring pixels to have a similar color for pixel p(x, y), the histogram of

$\blacktriangledown^{2}P(x, y)$ is tightly clustered around zero for original image, since the embedding process adds noise to the original so using this equation by attacker does not prove the existence of a secret, but it will provide strong evidence that the picture was subject to modification.

3.7.2 Active Attacker

An active attacker, who is not able to extract or prove the existence of a secret message, thus can simply add random noise to the transmitted cover and so try to destroy the information. In the case of digital images, an attacker could also apply image processing techniques or convert the image to another file format. All of these techniques can be harmful to the secret communication. Another practical requirement for a steganography system, therefore is robustness. A system is called robust if the embedding information cannot be altered without making drastic changes to the stego-object. The below two equations used to authenticate if a steganography system resisting for robustness:

$$D_k(P(E_k(c,m,k)=D_k(E_k(c,m,k),k)=m \qquad (3.2)$$

$$D\ (P(E\ (c,m)))=D(E(c,m))=m \qquad (3.3)$$

Where :

P: means any cover processing

Equation (3-2) is used upon usage of the secret key in embedding process.

Equation (3-3) is used upon usage of pure steganography system.

Other operations may happen between the sender and the recipient to assure reaching the same cover. One of them is called authentication which indicates the agreement between the sender and the recipient about certain value of the image where each one of them makes sure of this image upon sending and receiving during the extraction of the secret message to ensure delivering of the same cover. There are also algorithms resistant for attacking operations partially such as: DCT, it is possible to conduct the same modification operations done by the attackers to return the cover to its original shape before extraction operation.

3.7.3 Malicious Attacker

He is the one who sends the secret message to the recipient after changing the cover or the content where the recipient cannot make sure from the accuracy of the secret message and to avoid malicious observer, there should be security algorithms resistant for attacking operations and more secure.

3.8. Steganalysis

The objective of steganalysis System done by attackers is detecting the steganography operations besides other targets for this operation reflecting in the following:

1- Deactivation: It is preventing the delivery of the secret message to its owner.

2- Extractions: It is the attempt to extract the secret message.

3- Confusion: It is the operation of replacing the cover with another one for deceiving the recipient about the secret message.

There are other detentions to this operation including the following:

- The art of detecting the secret message inside the cover. (Etting, 1998)
- It is a technique to determine the hiding message then attempting to extract it from the cover. (Joanson and Jajudia, 2001)

The steganography system consists from several contents which the attackers might reach to some of them to conduct analysis on them as follows:

1- Stego-only attack : only the stego-object is available for analysis.

2- Known cover attack : the original cover-object and stego-object are both available for analysis.

3- Known message attack : at some point , the hidden message may become known to the attacker . Analyzing the stego-object for patterns that correspond to the hidden message may be beneficial for future attacks against the system. Even with message, this may be very difficult and may even be considered equivalent to the stego-only attack.

4- Chosen stego attack : The steganography tool (algorithm) and stego-object are known.

5- Chosen message attack : The steganalyst generates stego-object from some steganography tool or algorithm from a chosen message. The goal in this attack is to determine corresponding patterns in the stego-object that may point to the use of specific steganography tool or algorithms.

6- Known stego attack : The steganography algorithm (tool) is known and both the original and stego-object are available.

3.9. Kerckhoff Principles

Kirchhoff suggested a set of principles that must be available during the encryption process until the process as required and correct, since the encryption process involved with the process of steganography in the security and integrity of the data, you must observe these principles when using the steganography process, and these principles are: (Rabah, 2004)

1- The process of extracting the secret message must be clear and easy for the receiver and scalable mechanism to extract.

2- The secret key must be easy to handle and store.

3- Possibility of transfer encoded text using the Telegraph.

4- The possibility of transfer the system easily.

5- Apply the system must be easy, since it does not require many rules or mental effort.

3.10. Steganography System Security

To increase the security of steganography methods it should have a high degree of similarity between the original cover and the cover which contain the secret message Stego-Image, and for this purpose there are two basic methods used to prove the security of steganography system , these methods are :

1- Similarity function.

2- Entropy function.

3.10.1 Similarity function

The embedding process is defined in a way that a cover and the corresponding stego-object are perceptually similar. Formally, perceptual similarity can be defined via similarity function:

Definition 2.3 (Katzenbeisser and Petitcolas, 2000): (Similarity function) Let C be a nonempty set. A function

sim: $C^2 \rightarrow [-\infty,1]$ is called similarity function on C, if for x,yϵC

sim (x,y) = l ⇔ x = y

For x ≠ y, *sim*(x,y) < 1

In the case of digital images the correlation between two images can be used as a similarity function. Therefore most practical steganographic systems try to fulfill the condition . *sim (c,E(c,m))* ≈1 for all *m ϵ M* and c ϵ C.

$$r = \frac{\sum(\mathrm{x_i} - \bar{\mathrm{x}})(\mathrm{y_i} - \bar{\mathrm{y}})}{\sqrt{\sum(\mathrm{x_i} - \bar{\mathrm{x}})^2}\ \sqrt{\sum(\mathrm{y_i} - \bar{\mathrm{y}})^2}} \qquad (3.4)$$

Where *x* is the cover image, *y* is the stego-image, $\bar{\mathrm{x}}$ is the mean of the $\mathrm{x_i}$'s, $\bar{\mathrm{y}}$ the mean of the $\mathrm{y_i}$'s. if the value of *r* is near l then the vectors *x* and *y* is highly correlated, and if it near 0 indicates that x and y is uncorrelated (Norusis, M..l. 1982).

For every communication process, a cover is randomly chosen. The sender could also look through the database of usable covers and select one that the embedding process will change the least.

Such a selection process can be done via a similarity function *sim*. In the encoding phase, the sender chooses a cover c with property

$$c = \max_{x \in C} sim\big(x, E(x,m)\big) \qquad (3.5)$$

The sender could select one, best suitable for communication. Such a technique, called selection method of invisibility (Katzenbeisser and Petitcolas, 2000).

3.10.2 Entropy function

An information-theoretic model for steganography was proposed by Cachin (Cachin, 1998) which gave a definition of the security of the steganographic systems.

The main idea is to refer to the selection of a cover as a random variable *C* with probability distribution *Pc*. The embedding of a secret message can be seen as a function defined in *C*, let *Ps* be the probability distribution of $E_k(c, m, k)$, that is the set of all stego-objects produced by the steganographic system. If a cover *c* is never used as stego-object, then *Ps(c) =0*. In order to calculate *Ps*, probability distribution on K and M must be imposed. Using the definition of relative entropy $U(P_1 \parallel P_2)$ between two distribution P_1 and P_2 are defined on the set *n*,

$$U(P1 \parallel P2) = \sum_{n=0}^{255} Pc(n)\, log_2 \frac{P1(n)}{P2(n)} \qquad (3.6)$$

Which measure the inefficieney that the distribution is P_2 where the true distribution is P_1. The impact of the embedding process on the distribution *Pc* can be measured. Specifically, we define the security of a steganography system in terms of $U(P_1 \parallel P_2)$.

3.11. Invisibility of Steganography

In data hiding, we have two primary objectives, the embedded data must be imperceptible to the cover, including the observer's resources such as computer analysis, and it should have maximum payload possible. It is difficult to quantify how imperceptible embedded data is. In the case of image steganography, the typical observer's detection resources include the human vision system (HVS) and, potentially, computer analysis. For most of the methods presented in the previous section using imagery, the imperceptibility of the embedded data is indicated by illustrating the original image and its counterpart with embedded data so that their visual differences, if any, can be determined. Additionally the mean-squared-error (MSE) (2.8) or peak-signal-to-noise ratio (PSNR) (2.9) between the original and stegoimage may be presented. The original image's pixels are represented as X_{ij} and the stegoimage pixel as $\bar{X}_{ij}$. The variable L reflects the peak signal level (L=255 for grayscale images) (Kutter M. and Petitcolas F. 1999).

$$MSE = \left[\frac{1}{N * N}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2 \qquad (3.7)$$

$$PSNR = 10 \ \log_{10} \frac{L^2}{MSE} \ db \qquad (3.8)$$

Where:

X_{ij} is the original image pixels

$\bar{X}_{ij}$ is the secret image

L = 255 When using the gray image.

Chapter Four

Chapter Four

Related works

4.1. Introduction

In the recent years, several of the steganography techniques have been suggested where most of them on substitution system which working on replacing part of the original cover by the secret message through the highest degree of payload but it is not resistant to attacking processing , then different methods occurred to resist the attacking processing however they could not hide large amounts of data.

There are numerous classifications of the steganography where some of them depend on the used cover in embedding processing besides, there are many standards which should be taken into consideration in classifying the technologies used to hide the information by using the steganography including: (Possibility of loading on the cover directly or using the original key between the sender and the recipient or using statistical equations …..). Figure (4-1) shows these classifications: (Katzenbeisser and Petitcalas, 2000)

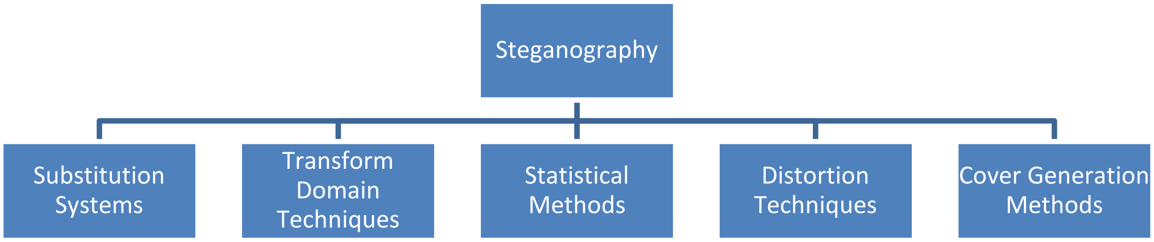


Figure (0-1) Classifications of the Steganography

4.2. Substitution systems

This kind of systems depends on hiding the secret message by one of the following: Last significant bit, replacing part of the original cover by the secret message without affecting it. After that, the data is extracted from the site that was replaced.

The following Figure (4-2) shows some of the methods which use the substitution systems.

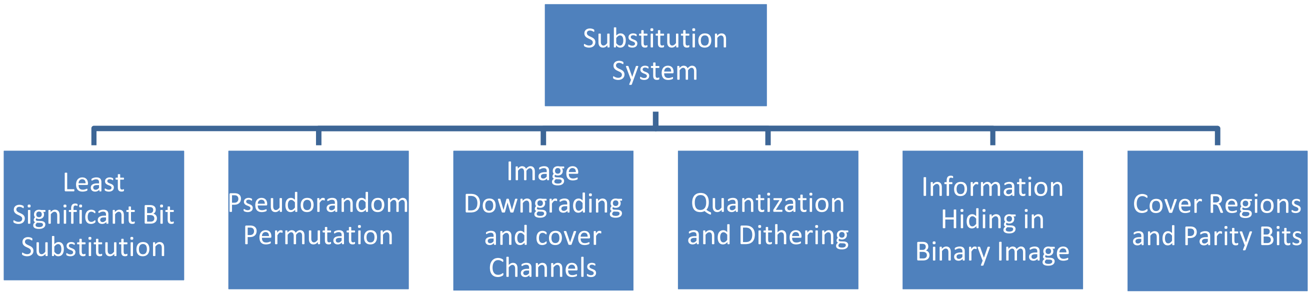

Substitution System
Least Significant Bit Substitution
Pseudorandom Permutation
Image Downgrading and cover Channels
Quantization and Dithering
Information Hiding in Binary Image
Cover Regions and Parity Bits

Figure (0-2) Substitution Systems Methods

4.2.1 Least Significant Bit (LSB):

It is mainly common used method in which through it the least duality is replaced in each byte where it is considered the simplest method leading to other more complex methods by dividing the cover into primary elements (Katzenbeisser and Petitcalas, 2000) and to extract the secret message the least important site will be selected from each element, the two algorithm (4.1) and (4.2) show the Embedding Processing, Extraction Processing respectively. (Katzenbeisser, 2000)

Algorithm 4.1 : Embedding Processing : Least Significant Bit Substitution

```
For I = 1,……..L(c) do
Si ← Ci
End for
For I = 1,……..L(c) do
Compute index ji where to store ith message bit
Si ←   Ci ↔ Mi
End for
```

Algorithm 4.2 : Extraaction Processing : Least Significant Bit Substitution

```
For I = 1,……..L(c) do
Compute index ji where to store ith message bit
Si ← LSB(Ci)
End for
```

In order that the recipient, he collects a series of the binaries which are located at the end of each point, the recipient has to know the indices where the data are embedded inside it. This means that the load of should equal to one of the cover elements but its load is less than the cover elements number, it means the end of the secret message before reaching to the last element included in it. It means that, the elements were not used in embedding processing which resulted in dividing the cover into two parts: modified section (the data were embedded inside it where the other one is unmodified (It is not used in embedding processing), for solving this problem, it is suggested that the embedding processing is to be distributed on the entire cover and not on its starting where the space for data includes the whole cover and the replacement is done randomly.

Algorithm processing principal

The gray-scale consists of a group of pixels and each pixel has 8 bits starting by most and ending by least which means transferring the intended secret message to be hidden to binary image pixels.

Most	8	7	6	5	4	3	2	1	Least

Pixel

Embedding Processing

1. Adding one binary image to hide inside the site which is least from each point.

2. The points are transferred into to another image which includes the secret message (Stego_Image).

Extraction Processing

1. Extraction each binary image from each point.
2. Collecting the series of binary images to get the hidden message.

This algorithm is distinguished by the highest storage capacity which reaches to 32kbyte inside an image measured 512×512 of the Gray-Scale where the difference between the original and secret images is very little due to modifying the last binary image in each point.

One of this algorithm disadvantages: losing the secret message upon making any attacking processing by the attackers where they detect the data inside the secret message because of it is easily to extract it.

4.2.2 PSEUDO-RANDOM PERMUTATIONS

In this algorithm distributing the secret message is inside the cover randomly, besides finding the Index for each element inside the processed embedding processing while the extraction processing depends on the Seed principle meaning repetition of the random values upon their execution for ensuring the message values. This algorithm works on increasing of the complicated processing on the attackers because, but it does not ensure the arrangement of the secret message the same as the original one.

The above processing caused the problem of collision meaning that choosing any points for more than once. It means repetition adding binary image from the message inside the site (the element) as one of the cover which resulting in distortion of the message due to changing some of the values where more load of the message; the possibility of the collision will increase.

To solve the collision in this algorithm vector will be added in which each element index of the cover will be clarified. After that it is embedded and another binary image is to be selected reaching to the end of the message.

The collision problem can be solved through usage of algorithm number (4.3) suggested by Aure Tumoas dated 1996 in which the embedding seat will be located without repetition or collision. This algorithm is used when the cover is a digital image with the two dimensions X and Y dividing the secret key into three keys K_1, K_2, K_3 then the embedding site will be computed giving new value each time.

Algorithm 4.3 : Computing the index ji using Pseudorandom Permutation

```
$v \leftarrow i . div . X$
$u \leftarrow i . mod . X$
$v \leftarrow (v+h_{k1}(u)) . mod . Y$
$u \leftarrow (u+h_{k2}(v)) . mod . X$
$v \leftarrow (v+h_{k3}(u)) . mod . Y$
$ji \leftarrow vX + u$
```

For extraction of data from the site where the embedded processing done, it is a must to know the keys K_1, K_2, K_3 where this algorithm needs the previous used one in each embedding binary image of the secret message which resulted in increasing of the necessary time to implement this Algorithm as the following example:

Indexes: 1 2 3 4 5

Binary images: 00011101, 01000111, 000110, 11000010, 11010110

Secret Message: 0, 1, 1, 0, 1

Embedding Processing as follows:

1. Selecting the first pixel of the image randomly for embedding the first binary image from the message vector (B).

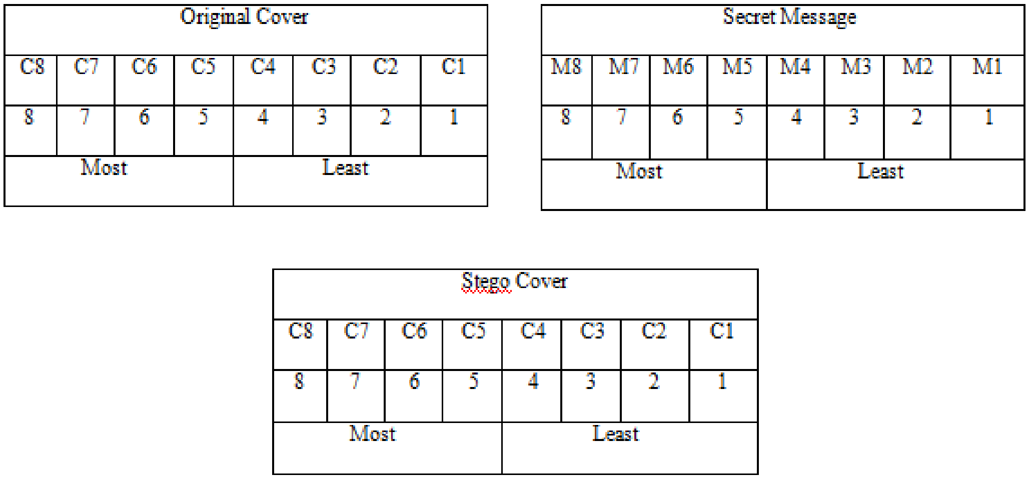
2. Selecting new pixel of the image randomly for embedding new binary image from the message vector (B) by choosing new element which will be embedded inside the binary image of the secret message and adding its site to the vector (B).

Extraction Processing

For ensuring the right series of the message, the same processing will be repeated at the end of each point by using SEED principle to obtain the same random values.

4.2.3 Image Downgrading and cover Channels

It is a special case of the replacing systems of the original image as cover in the same time. For performing the embedding processing by using this method, the secret and original messages have the same dimension where the sender replaced the least part or (for binary images from each point) with the most higher part of the secret message (for binary images from each point). Figure (4-3) Regression Technique and the secret messages show that:



Original Cover							
C8	C7	C6	C5	C4	C3	C2	C1
8	7	6	5	4	3	2	1
Most				Least			

Secret Message							
M8	M7	M6	M5	M4	M3	M2	M1
8	7	6	5	4	3	2	1
Most				Least			

Stego Cover							
C8	C7	C6	C5	C4	C3	C2	C1
8	7	6	5	4	3	2	1
Most				Least			

Figure (0-3) Image and cover Channels

In figure (4-3), the highest part of the original image will be merged with its similar of the secret message for obtaining the secret cover where the recipient extracts the least part from each point to get the secret message, in spite of the fact, such method is unsecure in the required way, however, it is sufficient to send a rough estimate for the secret message (the secret image). (Katzenbeisser and Petitcalas, 2000).

4.2.4 Quantization and Dithering

Each pixel of the digital image has a certain value representing the colored density (the colored degree) where the adjacent pixels are convergent in the colored density. This Algorithm depends on finding the deference between each two adjacent pixels as in the following equation: (Katzenbeisser and Petitcalas, 2000).

$$\Delta i + Q(X_i - X_{i-1}) \text{ ---------------- } (4.1)$$

The following Table (4-1) represents the differences between the adjacent pixels between the sender and the recipient.

Δi	-4	-3	-2	-1	0	1	2	3	4
M	0	1	0	1	1	1	0	0	1

Table (0-1) Represents the differences between the adjacent pixels

For embedding the secret message inside the cover, the difference between each two adjacent points based on the equation (3-1) where a table to be prepared representing the differences as in the table (4-1), for example, if the difference equals -4 , the embedding value is 0, but if the difference is (-3), the embedding value is (1) where the extraction process is done according to the values table of the differences comparing it with the table representing the secret key then extraction of opposite value as in the following examples:

Example :

Embedding Process

Original Image Values				Secret Key						Stego image Values			
90	90	92	90	Δi	-2	-1	0	1	2	90	90	92	91
93	92	90	90	m	1	0	0	1	0	93	91	90	90
89	88	90	91							88	88	90	91
93	91	91	93							93	91	91	93

Secret Message Values								
A	0	1	0	0	0	0	0	1

Extraction Processing

Stego image values and the secret keys are the inputs for this process.

Secret Key						Stego image Values			
Δi	-2	-1	0	1	2	90	90	92	91
M	1	0	0	1	0	93	91	90	90
						88	88	90	91
						93	91	91	93

In the extraction processing, the difference between adjacent points is specified, then comparing the difference value with the table and extraction the secret message with knowing that , the difference between the first two points is 0 and the value is also is 0 and so forth.

4.2.5 Cover-Regions and Party Bits

This method depends on dividing the original cover into a group of equal parts then embedding binary image in each one of them and in the same time, the cover is divided to equal parts similar to the load of the secret message according to the following formula:

$$P(I) = \sum LSB(C_i) \ . \ \mathrm{mod} \ . \ 2 \quad \text{----------------} \ \mathit{(4.2)}$$

The equation (4.2) finds out the value the values of LSB as (the last binary image from each pixel) then finds its results by dividing it into 2 which is (0) that will be embedded where LSB its result is identical to P(I). After that the equation (4.2) will be applied on each part of the image which represents the secret message result.

Regardless, that such method does not resist the attacking processing with least storage capacity but it gives a high degree of the similarity between the original and the secret images as the sender who is the one that specifies the modification location inside the part. (Katzenbeisser and Petitcalas, 2000)

4.2.6 Information Hiding In Binary Image

The binary image consists of two colors only which are the white and black where the pixel with value (1) has the white color and the pixel with value (0) has the black color. As example of this kind of replacement is suggested by the two scientists Koch and Zaho as they indicated that the embedding process is done through dividing the binary image to a group of blocks (B_i) then, the value (1) will be embedded inside the block (1), if the percentage of the white color for hiding the value is $P_1(B_i) > 50\%$ and (0) if the percentage of the black color for hiding the value $P_0(B_i) > 50\%$ where the required color percentage will be increased by using the change indicator (λ).

$$P1\ (Bi) < R0\ (Bi) - 3\lambda \text{ ---------------- } \mathit{(4.3)}$$

$$P1\ (Bi) < R0\ (Bi) + 3\lambda \text{ ---------------- } \mathit{(4.4)}$$

In case that the points which will be modified affecting the image, the block remains (Bi) is unused and invalid.

For extraction of data from the binary image, the unused images in embedding process were excluded, then, the value will be extracted from the block (1) (Bi) , if the percentage of the white color is bigger than $P_1(B_i) > 50\%$ and the value (1) is extracted, the value will be extracted from the block (1) (Bi), if the percentage of the black color is bigger than $P_0(B_i) > 50\%$ and the value (0) is extracted and the embedding and extraction Algorithm (4.4) and (4.5) are adopted in the embedding and extraction processing. (Khader, 2004).

Algorithm 4.4 : Embedding data In Binary Image:

```
For I = 1 ………. L(m)
/* test if block Bi is valid
If P1(Bi) > R1+ 3λ OR P1(Bi) < R0 - 3λ Then Continue
If ( Ci=1 and P1(Bi) < R0 ) OR ( Ci=0 and P1(Bi) > R1 ) Then
Mark Block Bi unusable, i.e. modify Block so that
Either P1(Bi) < R0 - 3λ OR P1(Bi) > R1 + 3λ
Continue
```

```
End if
Break
/* Embed Secret Message bit in Bi */
If Ci = 1 Then
Modify Bi so that P1(Bi) > R1 and P1(Bi) < R1+ λ
Else
Modify Bi so that P0(Bi) < R0 and P0(Bi) < R0+ λ
End if
End for
```

Algorithm 4.5 : Extraction data from Binary Image

```
For I = 1 ………. L(m)
/* test if block Bi is valid
If P1(Bi) > R1+ 3λ OR P1(Bi) < R0 - 3λ Then Continue
Break
/* Extract Secret Message bit From Bi */
If P1(Bi) > 50% Then
Mi = 1
Else
Mi = 0
End if
End for
```

4.3. Transform Domain Techniques

The replacement methods depend on embedding the secret data inside the original cover directly spatial domain but it is effected by any modification on the original cover (or the secret data is either lost or destroyed upon implementing any handling processing on the cover by the attackers) which is not seen by the naked eye, and characterized by the possibility of high storage.

But, we sometimes, need more security in data transferring process as well as, a higher resistance degree by the used cover in hiding processing upon any change or handling by the attackers, it means that, (the cover is not effected by any modification processing, thus, the secret data remains hidden inside the cover) depending on the following factors such as: the load of transferring data, changing of the cover for frequency domain to resist the attacking processing embedding of the secret data inside the cover and changing the image points by the functions like Discrete Cosine Transformation (DCT) .

4.4. Statistical Steganography

This technique depends on implementing a group of the statistical processing to the original cover based on the secret message where the cover is divided into a set of parts that each one of them is specified to embed an element of the secret message (mi) as the modification will be executed on the opposite side of the data values equal “0”. The recipient has to distinguish between modified and unmodified parts of the cover to extract the secret message which embedded by M, the cover division C, the blocks Bi in the load of the secret message L (m) bases on the equation (4.5)

$$L(C) = B1 + B2 + \ldots\ldots\ldots\ldots B1(mi) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4.\ 5)$$

As L (C) is the cover load and L (Mi) is the secret message load.

- If mi = 1, the modification will be done on the block.
- If mi = 0, modification will not be done on the block.

Function F is used to distinguish between the cover blocks based on the following formula :

$$F(Bi) = \begin{cases} 1 \ : \ Block\ (Bi) mod\ i\ fied \\ 0 : otherwase \end{cases}$$

The researcher in this field has to find (Hypothesis- Testing Function which is a statistical operations implemented on the points of each block for distinguishing between the modified and unmodified blocks where this function covers a certain value, if the block is modified and (0) value, if the block is unmodified. (Katzenbeisser and Petitcalas, 2000).

4.5. Distortion techniques

the Steganography techniques depend on embedding the data inside the cover (distortion the cover) by using one of the replacement methods and the secret data is extracted by the comparison between the original and secret covers (the distorted) where the difference degree between them the secret data, it means that, the method needs the original cover for extracting the secret data (the secret key is the original cover).

4.6. Cover Generation Techniques

In the previous technologies, the selecting of the cover was done randomly, and then the secret message was embedded inside the cover, but in this technology, special covers are generated for the Steganography system for correspondence of the secret message.

Find below the description of Gutub's pixel indicator and Ghosal's New Pair Wise Bit algorithms which are part of the modern studies in this field.

4.7. Gutub's Pixel Indicator Algorithm

This algorithm is invented by researchers Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi. It embeds the secret data directly on the cover spatial domain based on RGB image as a cover for secret data where the pixel indicator technique uses the least two significant bits of one of the channel from Red, Green and Blue as an indicator for existence of data in the other two channels. The indicator channels are chosen in sequence, with Red being the first in the first pixle while Green is channel 1 and Blue is the channel 2. In the second pixel, Green is the indicator, while Red is channel 1 and Blue is channel 2. In third pixel Blue is the indicator, while Red is channel 1 and Green is channel 2. (Gutub, 2008)

The following table (4-2) shows the relation between the indicator and the hidden status inside the other channels:

Indicator	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2 bits of hidden data
10	2 bits of hidden data	No hidden data
11	2 bits of hidden data	2 bits of hidden data

Table (0-2) Shows the the indicator and the hidden status inside the other channels

The hiding algorithm is flowcharted in Figure (4.5). The recovery algorithm is flowcharted in Figure (4.6) and it will stop based on the length of the secret message, which is stored in the first 8 bytes of the cover image.

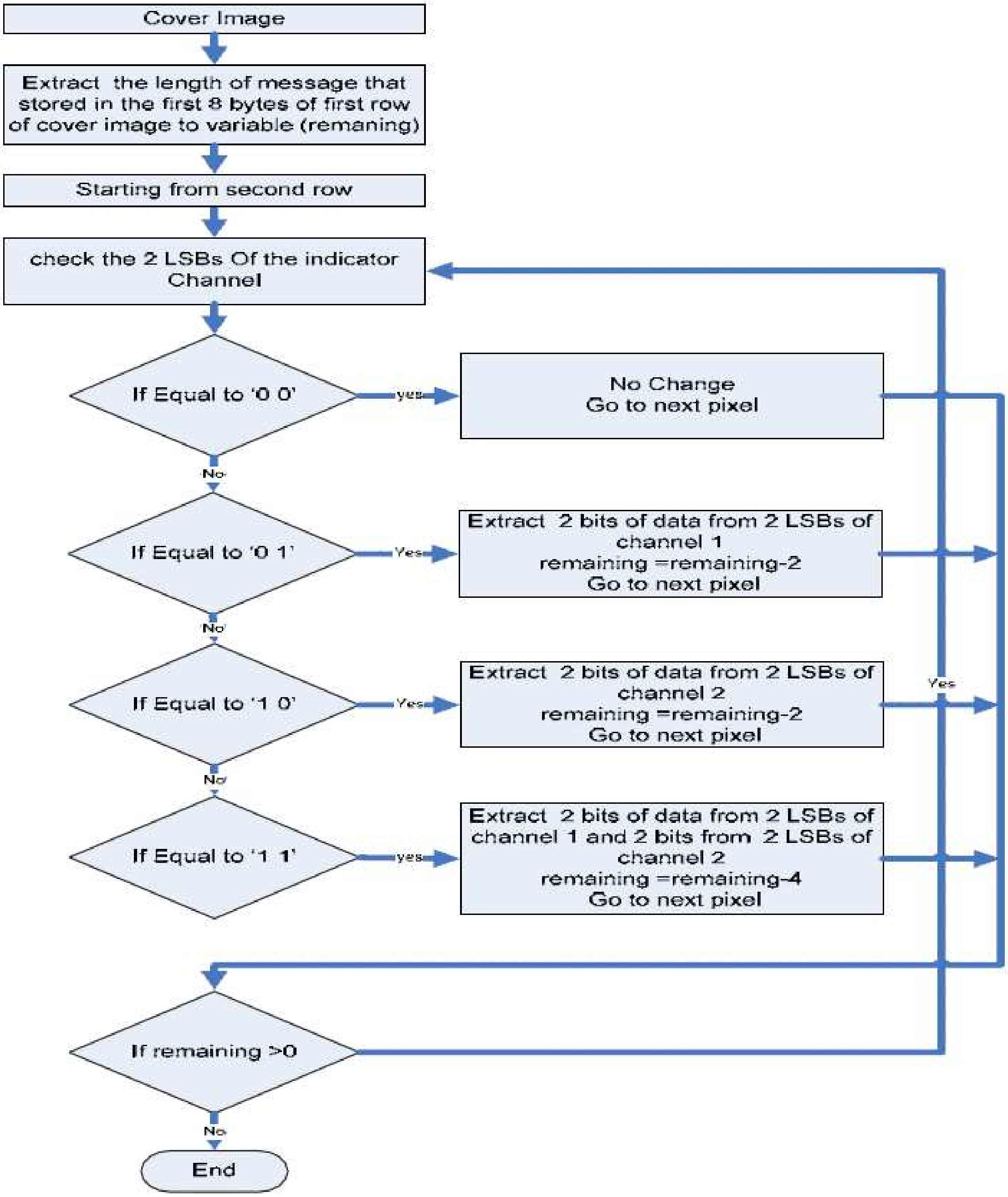

Cover Image
Extract the length of message that stored in the first 8 bytes of first row of cover image to variable (remaning)
Starting from second row
check the 2 LSBs Of the indicator Channel
If Equal to '0 0'
yes
No Change
Go to next pixel
No
If Equal to '0 1'
Yes
Extract 2 bits of data from 2 LSBs of channel 1
remaining =remaining-2
Go to next pixel
No
If Equal to '1 0'
Yes
Extract 2 bits of data from 2 LSBs of channel 2
remaining =remaining-2
Go to next pixel
No
If Equal to '1 1'
yes
Extract 2 bits of data from 2 LSBs of channel 1 and 2 bits from 2 LSBs of channel 2
remaining =remaining-4
Go to next pixel
Yes
If remaining >0
No
End

Figure (0-4) Gutub's hiding algorithm flowchart

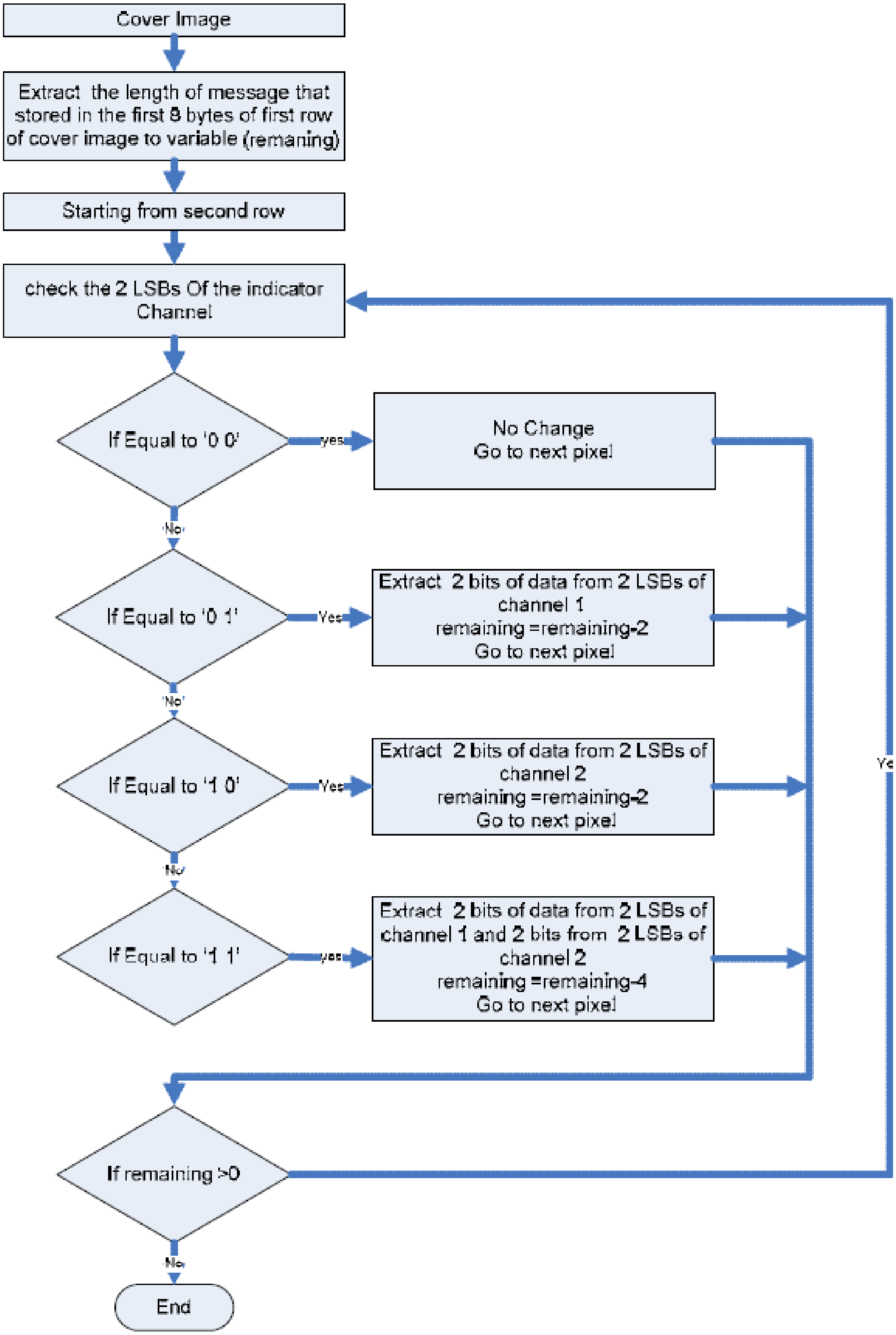

Cover Image
Extract the length of message that stored in the first 8 bytes of first row of cover image to variable (remaning)
Starting from second row
check the 2 LSBs Of the indicator Channel
If Equal to '0 0'
yes
No Change
Go to next pixel
No
If Equal to '0 1'
Yes
Extract 2 bits of data from 2 LSBs of channel 1
remaining =remaining-2
Go to next pixel
No
If Equal to '1 0'
Yes
Extract 2 bits of data from 2 LSBs of channel 2
remaining =remaining-2
Go to next pixel
No
If Equal to '1 1'
yes
Extract 2 bits of data from 2 LSBs of channel 1 and 2 bits from 2 LSBs of channel 2
remaining =remaining-4
Go to next pixel
If remaining >0
Ye
No
End

Figure (0-5) Gutub’s recovery algorithm flowchart

This algorithm is characterized by the data load which can be classified inside the cover but, it is weak from the security level where, the indicator chossen sequentially. Also, the algorithm uses fixed no of bits per channel (2 bits) to store data and the image may get distorted if more bits are used per channel.

4.8. Ghosal's New Pair Wise Bit Algorithm

This Algorithm is invented by researcher Ghosal proposed a seganographic method works by considering the three channels (viz. red, green and blue) of each pixel of the cover image one by one up to the (maximum, if desire) last pixel and calculating the number of ones and zeroes in the red channel. Then, calculate the absolute difference value of the number of zeroes and number of ones which is again divided by the total embedding channel numbers viz. green and blue which is 2 for a 24 bit color image. The resultant number of bits of the hidden data is embedded on the LSB part (in bit range of 0-3) of the green and blue bytes (channels) of each pixel of the cover image respectively. (Ghosal, 2011).

Embedding Procedures :

Step 1: Load the 24-bit color image as cover.

Step 2: Load the data (usually, text or image) which is to be embedded.

Step 3: Consider the Red, Green and Blue channels of pixels starting from the first to a maximum of the end pixel to hide the secret information in the cover. That means, only the requisite number of pixels is needed from the cover which can hide the entire secret information.

Step 4: Calculate the number of 1’s and number of 0’s in the Red channel of each pixel.

Step 5: Calculate the absolute difference value of number of 1’s and 0’s in red channel.

Step 6: Divide the difference value results by the number of channels to be embedded in a pixel which is 2 for a 24 bit color image.

Step 7: Now, the resultant number of bits of the embedding size is to be embedded till a specified number of pixels and then data is to be embedded on the LSB (up to 3rd bit position) part of the Green and Blue bytes of each pixel of the cover image where the Red channel will act as an indicator.

Step 8: The final stego image is to be produced.

Extracting Procedures :

Step 1: Load the 24-bit color stego- image.

Step 2: Consider the Red, Green and Blue channel of pixels starting from the first of the stego-image to a maximum of the end pixel.

Step 3: Calculate the number of 1’s and 0’s in the Red channel of each pixel.

Step 4: Calculate the absolute difference value of number of 1’s and number of 0’s in red channel.

Step 5: Divide the difference value results by 2 in the same manner.

Step 6: Now, the resultant number of bits of the size data is to be extracted by traversing a specified number of pixels and depending on the size of the hidden data, the requisite secret data is to be extracted from the LSB part of the Green and Blue channels of each pixel of the stego image where the Red channel will act as an indicator.

Step 7: Now, the hidden data will be extracted from the stego image.

For example of how the above method works. Let we assume, the bit pattern (R, G and B) for two consecutive pixels of a 24-bit color image is as shown below:

11111010 00010111 10000010 00010001 00110011 10101010

Now, if we want to embed a character 'B' (has the binary value 01000010), we need to follow the above method. So, as per our method the number of one's in Red byte is 5 and number of 0's in Red byte is 3. So, the absolute difference value is (6-2) =4. Dividing the above results by 2 yields =4/2=2. So, bit embedded on the LSB part of the green byte is 2 and bit embedded on the LSB part of the blue byte is also 2. Also, for the second R byte the number of one's is 6 and number of zeroes is 2. So, the absolute difference results value is = (2-6) = 4. Dividing the above results value by 2 yields =4/2=2. So, bit embedded on the LSB part of the green byte is 2 and bit embedded on the LSB part of the blue byte is also 2.

Now, the bit stream of the stego image will be as shown below:

11011010 000101**0**1 100000**0**0 11111001 00110**00**0 10101010

So, by replacing only 4 bits in 4 numbers of selected bytes, we can hide the binary string 01000010.

This algorithm is characterized by the data load which can be classified inside the cover and where the distortion is very less and usually quite tough to find out any differences by human eyes. but, it is weak from the security level where, data is to be embedded on the LSB (up to 3rd bit position) part of the Green and Blue bytes of each pixel of the cover image where the Red channel will act as an indicator.

4.9. Analytical study of the previous techniques

Throughout study to the steganography techniques we found that there are some advantages and dis advantges of those techniques such as:

- Substitution systems domain techniques are the best of algorithms in terms of the data load while it is difficult to discover and unaware sensory by the human beings where the cover can be text, image, sound or animation but, it is not resistant to the robust operations.
- Transform domain techniques are the best of algorithms in terms of security and resistance to attacks but, they cannot store hidden data inside RGB images with big load which is considered very little comparing it with replacement algorithms. Consequently, the images are considered the only cover for this type of algorithms.

- Statistical steganography is considered the most algorithms complexity because it is difficult to be detected by the attacker, but it is hard to be applied since that it needs a theory for distinguishing between modified and non- modified blocks.
- Distortion techniques are distinguished to be easily applied but, it is the least security algorithms because, it requires the original cover to extract the secret data through comparing them with the secret cover.
- Cover generation techniques cannot store the data inside any cover but, they can be stored inside special covers which gives at the beginning higher security where they become the least security after a while due to recognition of the approved covers that used in the data embedding processes.

Chapter Five

Chapter Five

Proposed Algorithm

5.1. Overview

Start research in this area from the beginning of the eighties when the researcher Simmons represents a model for the concept of steganography by explaining of the prisoners problem that have been described previously in Chapter 3 of this thesis, and then a varied ways of embedding secret data inside of the cover have been suggested through a series of studies that depends on two methods for hiding the secret data, these are :

1- Embedding data inside cover using a spatial domain.

2- Embedding data inside cover using a transform domain.

5.2. The Proposed Model

A good approach to image steganography should aim at concealing the highest amount of data possible in a cover image. The least significant bit scheme is one of the simplest and easily applicable data hiding methods, which directly embeds bits of secret data in the least significant bits of each image pixel. Variations of this technique rely on optimally replacing carefully chosen pixel bits with message bits to improve the image quality and to provide larger hiding capacity.

Images are the most widespread carrier medium used as they can offer high hiding capacity. However, altering the least significant bits of 8-bit images would produce poor quality stego-images. Therefore, 24-bit RGB color images are preferable as their color values can be directly modified without noticeable degradation in image quality.

The proposed technique will be used to hide text message in BMP image with 24-bit color depth, the text message is converted to binary representation and after that embedded it in cover-image using a spatial domain. The proposed model represents a new technique for hiding text message inside digital images in a new randomization manner.

This technique divided it to two algorithms:

1- Embedding algorithm: for sender.

2- Extraction algorithm: for receiver.

5.2.1 Embedding Algorithm

Input : Secret Message , Cover-image.

Output : Stego-image.

Embedding algorithm steps :

1- Convert the text message to binary representation.

2- Calculate the Length of Message.

3- Store the message length into first 8 red bytes (in first 8 pixels of image in using two bits from LSB of red channel).

4- Finds Allocation for embedding data inside image by testing the pixel to make a decision to embed a part of text message or not by an Indicator starting from pixel number nine. The following table (5-1) shows the relation between the indicator and the hidden status inside the other channels in pixel:

Red Indicator	**Green**	**Blue**
00	No hidden data	No hidden data
01	No hidden data	hidden data
10	hidden data	No hidden data
11	hidden data	hidden data

Table (0-3) Shows indicator and the hidden status.

5- After choosing the pixel for embedding the first byte will be an indicator (Red channel) and other two channels (green, blue) to hide inside these two channels or one of them depending on the value of indicator . The following table 5-2 shows the 24-bit RGB image color space and indicator position:

8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
Red *channel*								Green *channel*								Blue *channel*							
8-bit								8-bit								8-bit							
24-bit pixel																							

Table (0-4) Shows the 24-bit RGB image color space and indicator position

6- Indicator selection will stop once the message stored in the image. it depends on a counter which holds the length of message. in each selection this counter will decrease.

7- If the channel choosing to embed the data in it, then the channel will divided into two parts , least significant part and most significant part, each part consists of four bits by process (Hide): table 5-3 illustrate this:

8	7	6	5	4	3	2	1
Most significant part				least significant part			
Channel which is chosen for embedding							

Table (0-5) Channel parts

The most significant part used to determine the number of bits in least significant part which it will modify to enter the hiding data in it.

8- Calculate the number of zero's in the most significant part :

9- Hide process will done by :

A- If the number of zero's = 4 or 0 then one bit of least significant part will use to hide one bit of secret message.

B- If the number of zero's = 2 then two bits of least significant part will use to hide two bits of secret message.

C- If the number of zero's = 3 or 1 then three bits of least significant part will use to hide three bits of secret message . table 5-4 illustrate this :

Number of Zero's In Most significant part	Number of bit To Embedded in Least significant part
4 OR 0	1 bit
2	2 bit
3 OR 1	3 bit

Table (0-6) Hide process

5.2.2 Extraction Algorithm

Input: Stego-image.

Output: Secret Message.

Extraction Algorithm Steps :

1- Extract the message length from first 8 red bytes (in first 8 pixels of image by using two bits from LSB of red channel)

2- Store the message length into variable (STOP)

3- Finds allocation for extracting data from image by testing the pixel to make a decision to extract a part of secret message or not by an Indicator starting from pixel number nine.

4- After choosing the pixel for extracting, the first byte will be an indicator (Red channel) and other two channels (green, blue) will be channels 1 and 2. These two channels or one of them will be used to extract a part of secret message depending on the value of indicator.

5- Indicator selection will stop once the stop counter value will be zero. Stop a counter which holds the length of message. And in each selection this counter will decrease.

6- If the channel choosing to extract the data, then the channel will divided into two parts , Least significant part and Most significant part, each part consists of four bits by process (Extract).

7- Calculate the number of zero’s in the most significant part :

8- Extract process will done by :

   A- If the number of zero’s = 4 or 0 then one bit of least significant part will use to extract one bit from secret Message.

B- If the number of zero’s = 2 then two bits of least significant part will use to extract two bits from secret message.

C- If the number of zero’s = 3 or 1 then three bits of least significant part will use to extract three bits from secret message .

Figure (5-1) illustrates the flowchart of embedding algorithm and Figure (5-2) illustrates the flowchart of extraction algorithm.

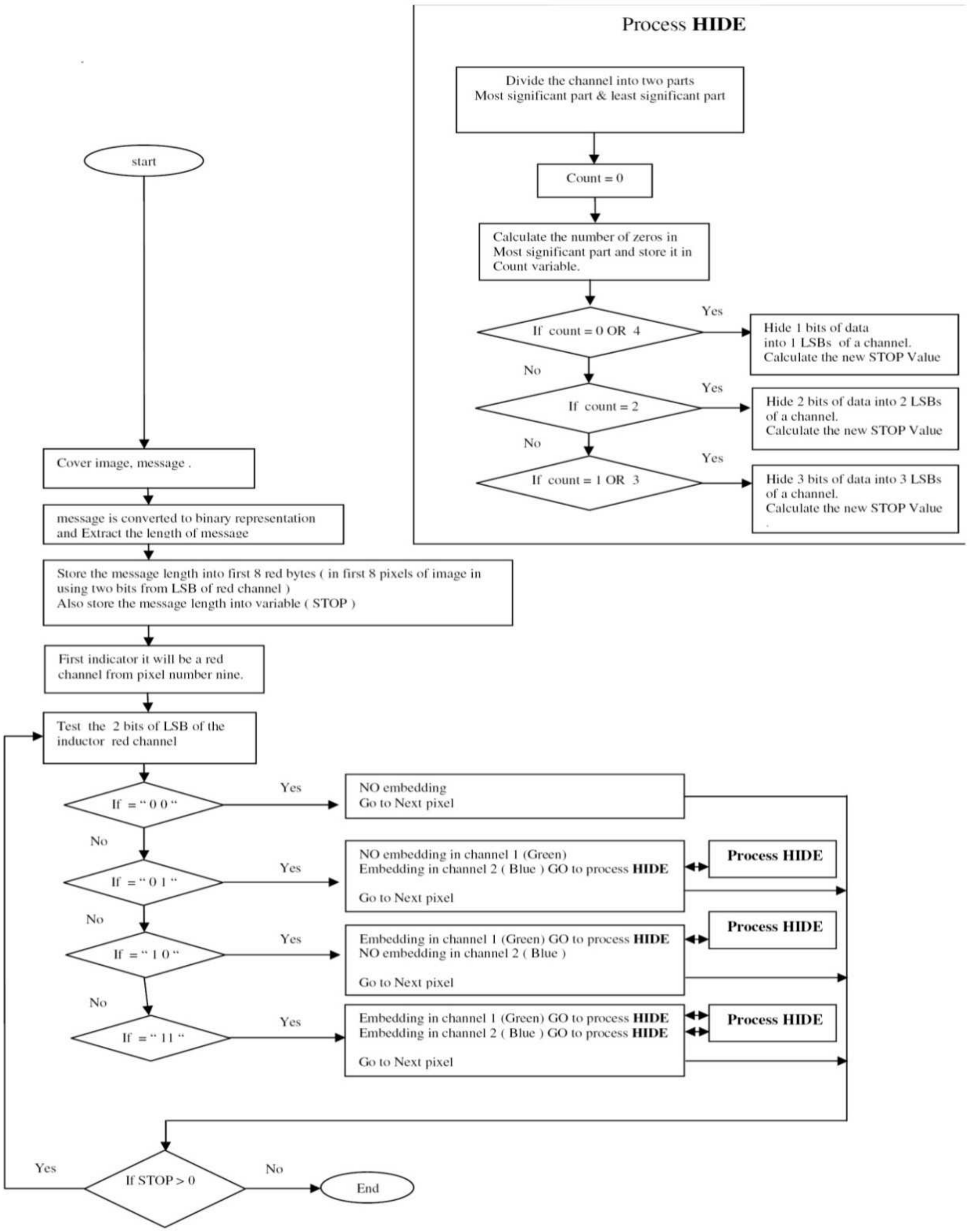

Process HIDE
Divide the channel into two parts
Most significant part & least significant part
Count = 0
Calculate the number of zeros in Most significant part and store it in Count variable.
If count = 0 OR 4
Yes
Hide 1 bits of data into 1 LSBs of a channel.
Calculate the new STOP Value
No
If count = 2
Yes
Hide 2 bits of data into 2 LSBs of a channel.
Calculate the new STOP Value
No
If count = 1 OR 3
Yes
Hide 3 bits of data into 3 LSBs of a channel.
Calculate the new STOP Value
start
Cover image, message .
message is converted to binary representation and Extract the length of message
Store the message length into first 8 red bytes (in first 8 pixels of image in using two bits from LSB of red channel)
Also store the message length into variable (STOP)
First indicator it will be a red channel from pixel number nine.
Test the 2 bits of LSB of the inductor red channel
If = " 0 0 "
Yes
NO embedding
Go to Next pixel
No
If = " 0 1 "
Yes
NO embedding in channel 1 (Green)
Embedding in channel 2 (Blue) GO to process HIDE
Go to Next pixel
Process HIDE
No
If = " 1 0 "
Yes
Embedding in channel 1 (Green) GO to process HIDE
NO embedding in channel 2 (Blue)
Go to Next pixel
Process HIDE
No
If = " 11 "
Yes
Embedding in channel 1 (Green) GO to process HIDE
Embedding in channel 2 (Blue) GO to process HIDE
Go to Next pixel
Process HIDE
Yes
If STOP > 0
No
End

Figure (0-6) Flowchart of a proposed embedding algorithm

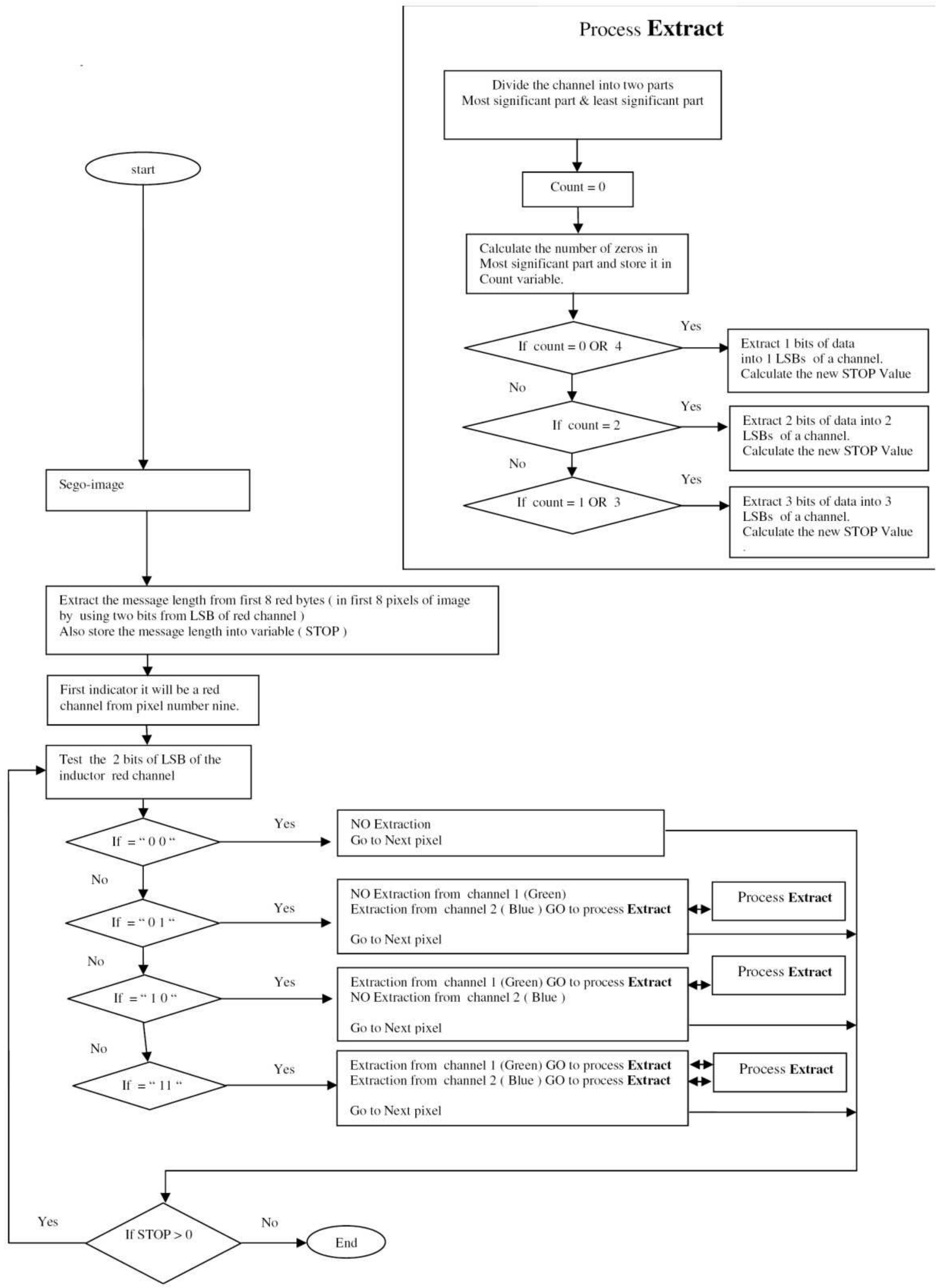

Process Extract
Divide the channel into two parts
Most significant part & least significant part
Count = 0
Calculate the number of zeros in Most significant part and store it in Count variable.
If count = 0 OR 4
Yes
Extract 1 bits of data into 1 LSBs of a channel. Calculate the new STOP Value
No
If count = 2
Yes
Extract 2 bits of data into 2 LSBs of a channel. Calculate the new STOP Value
No
If count = 1 OR 3
Yes
Extract 3 bits of data into 3 LSBs of a channel. Calculate the new STOP Value
start
Sego-image
Extract the message length from first 8 red bytes (in first 8 pixels of image by using two bits from LSB of red channel)
Also store the message length into variable (STOP)
First indicator it will be a red channel from pixel number nine.
Test the 2 bits of LSB of the inductor red channel
If = " 0 0 "
Yes
NO Extraction
Go to Next pixel
No
If = " 0 1 "
Yes
NO Extraction from channel 1 (Green)
Extraction from channel 2 (Blue) GO to process Extract
Go to Next pixel
Process Extract
No
If = " 1 0 "
Yes
Extraction from channel 1 (Green) GO to process Extract
NO Extraction from channel 2 (Blue)
Go to Next pixel
Process Extract
No
If = " 11 "
Yes
Extraction from channel 1 (Green) GO to process Extract
Extraction from channel 2 (Blue) GO to process Extract
Go to Next pixel
Process Extract
Yes
If STOP > 0
No
End

Figure (0-7) Flowchart of a proposed extraction algorithm

5.2.3 Example

- **Secret Massage : 0000 1111, 1001 1111,**
- **Embedding algorithm**

- Convert the text message to binary representation.
- Calculate the length of message = $(16)_{10} = (00000000\ \ 00010000)_2$
- Store the message length into first 8 red bytes (in first 8 pixels of image by using two bits from LSB of red channel).
- Store the message length into variable STOP.
- Finds allocation for embedding data into image by testing the pixel to make a decision to hide a part of secret message or not by an Indicator starting from pixel number nine.
- If the channel choosing to hide the data, then the channel will divided into two parts , Least significant part and Most significant part, each part consists of four bits by process hide.
- Calculate the number of zero's in the most significant part :
- Hide process will done by :
  - If the number of zero's = 4 or 0 then one bit of least significant part will use to hide one bit of secret message.
  - If the number of zero's = 2 then two bits of least significant part will use to hide two bits of secret message.
  - If the number of zero's = 3 or 1 then three bits of least significant part will use to hide three bits of secret message .

- Indicator selection will stop once the stop counter value will be zero. Stop a counter which holds the length of message. In each selection this counter will decrease.
- The table 5-5 illustrates this :

No	Before Hide			Y/N	After Hide			Binary Representation before hide			Binary Representation after hide		
	pixel				pixel			pixel			pixel		
	R	G	B		R	G	B	R	G	B	R	G	B
9	31	93	154	Y	31	92	152	0011 1111	0101 1101	1001 1010	0011 1111	0101 1100	1001 1000
10	32	94	161	N	32	94	161	0010 0000	0101 1110	1010 0001	0010 0000	0101 1110	1010 0001
11	34	93	154	Y	34	95	154	0010 0010	0101 1101	1001 1010	0010 0010	0101 1111	1001 1010
12	37	95	154	Y	37	95	155	0010 0101	0101 1111	1001 1010	0010 0101	0101 1111	1001 1011
13	39	97	161	Y	39	98	161	0010 0111	0110 0001	1010 0001	0010 0111	0110 0010	1010 0001
14	40	97	164	N	40	97	164	0010 1000	0110 0001	1010 0100	0010 1000	0110 0001	1010 0100
15	36	96	162	N	36	96	162	0010 0100	0110 0000	1010 0010	0010 0100	0110 0000	1010 0010
16	39	99	162	Y	39	99	163	0010 0111	0110 0011	1010 0010	0010 0111	0110 0011	1010 0011

Table (0-7) Shows pixels before and after hiding

- Notes that hide process it will be in least Significant part, and it will embedded 1 or 2 or 3 bits , so in previous example the number of bits embedded in each pixel as shown below :

P9	P10	P11	P12	P13	P14	P15	P16
4(2)	0	2(1)	2(1)	4(2)	0	0	4(1)

Which means that in previous example in 8 pixels we can hide 16 bits.

- **Extraction algorithm**

- Extract the message length from first 8 red bytes (in first 8 pixels of image by using two bits from LSB of red channel).

- Calculate the length of message = $(00000000\ \ 00010000)_2 = (16)_{10}$
- Store the message length into variable STOP.
- Finds allocation for extracting data from image by testing the pixel to make a decision to extract a part of secret message or not by an Indicator starting from pixel number nine.
- If the channel choosing to extract the data, then the channel will divided into two parts , Least significant part and Most significant part, each part consists of four bits by process extract.
- Calculate the number of zero's in the most significant part :
- Extract process will done by :
  - If the number of zero's = 4 or 0 then one bit of least significant part will use to extract one bit from secret message.
  - If the number of zero's = 2 then two bits of least significant part will use to extract two bits from secret message.
  - If the number of zero's = 3 or 1 then three bits of least significant part will use to extract three bits from secret message .
- Indicator selection will stop once the stop counter value will be zero. Stop a counter which holds the length of message. In each selection this counter will decrease. The table (4-4) illustrates that.
- The bits embedded in each Will extracted from each pixel in example as shown below:

P9	P10	P11	P12	P13	P14	P15	P16
0000	0	11	11	1001	0	0	1111

So the secret message will be: 0000 1111, 1001 1111

Chapter Six

Chapter Six

Experimental Results

This chapter includes characteristics of proposed algorithm as well as comparing them with the characteristics of known ones. In this regard, the programming language is used v.b.net version 2005 and also MATLAB, Version R2009a, It supported possibility of image processing indicating loading and analysis of the image besides changing it from one formula to another one by using a group of orders under the Image Processing Tool Box (Chapman, 2002). Proposed algorithm was applied on several of 24-bit colored bmp images for the purpose of the algorithm efficiency validation where it is processed on computer with AMD Athlon^{tm} 64 X2 dual core processor operating on frequency of 3.00 GHz and RAM equals 2.5 GB.

6.1. The Image Quality Test

This test measures the image quality through the comparison between the original image and the Stego image, It estimates the secret data percentage to the image percentage, taking into account that the typical value is 45 (Na-1,2004) and the table (6-1) shows the results through Equation (3.8) (Peak-Signal-to-Noise-ratio).

image	Image Size	Gutub Pixel Indicator Algorithm	Ghosal's New Pair Wise Bit Algorithm	Proposed Algorithm
Animal 1	1024×1024	57.94	56.33	57.96
Animal 2	1024×1024	58.10	56.68	58.20
Animal 3	1024×1024	58.11	56.17	58.32
Animal 4	1024×1024	57.81	55.81	57.91
Animal 5	1024×1024	57.90	57.02	57.93
Animal 6	1024×1024	57.90	56.50	57.95
Animal 7	1024×1024	57.73	56.29	57.94
Animal 8	1024×1024	57.74	56.92	57.86
football 1	1024×1024	57.96	55.86	58.02
football 2	1024×1024	57.50	47.40	57.90

Table (0-8) the image quality test (PSNR) .

We find out through the results that proposed algorithm is more satisfied experimental out comes than Gutub pixel indicator algorithm and Ghosal's new pair wise bit algorithm due to non-existence of difference between the original image and the secret one.

Figures (6-1),(6-2),(6-3),(6-4),(6-5),(6-6),(6-7),(6-8),(6-9) and (6-10) show image quality by comparing between the original images after embedding of the secret data inside it by using PSNR on the following images (Animal 1, Animal 2, Animal 3, Animal 4, Animal 5, Animal 6, Animal 7, Animal 8, Football 1 and Football 2).

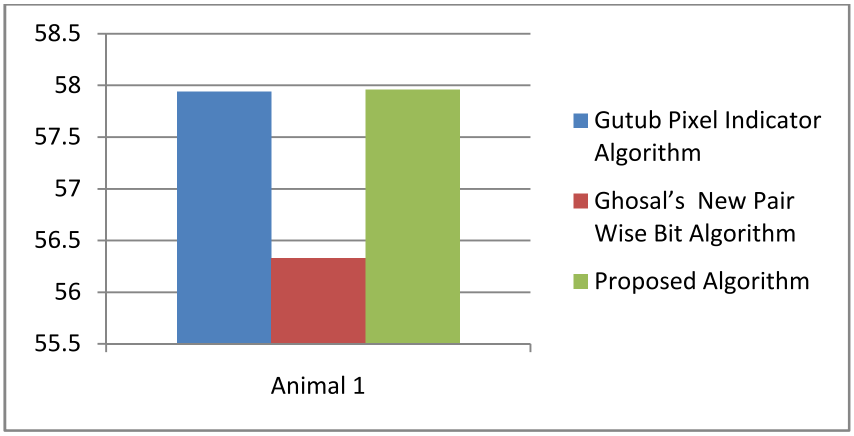


Figure (0-8) Shows the PSNR test for Animal 1 image

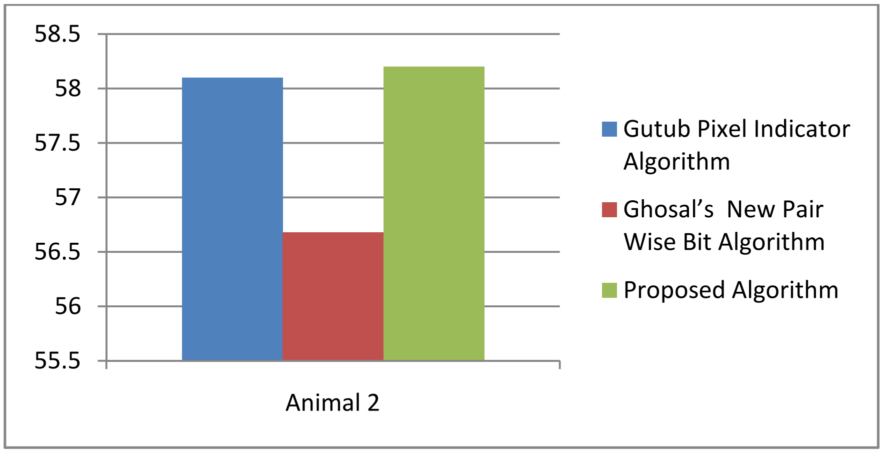


Figure (0-9) Shows the PSNR test for Animal 2 image

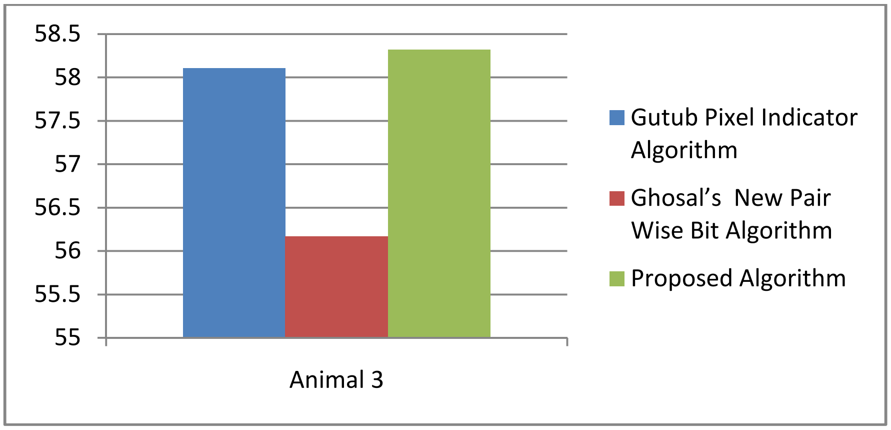


Figure (0-10) Shows the PSNR test for Animal 3 image

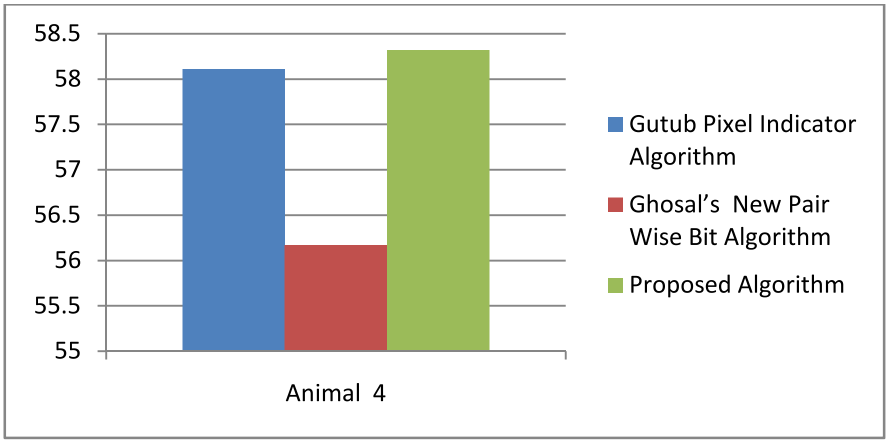


Figure (0-11) Shows the PSNR test for Animal 4 image

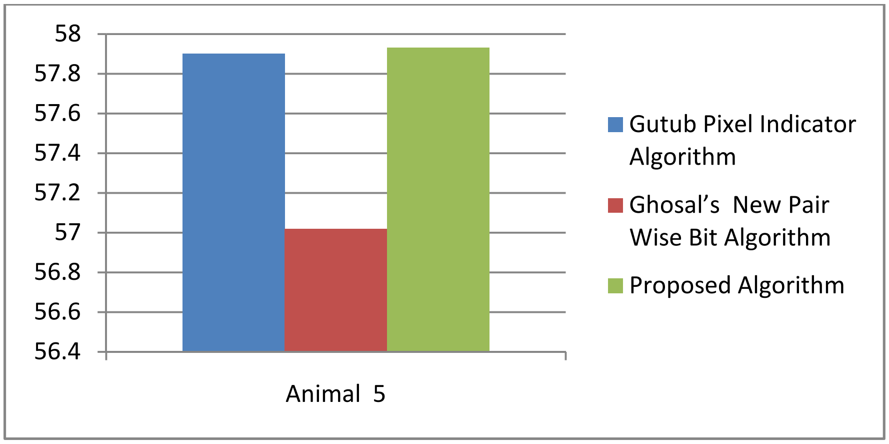


Figure (0-12) Shows the PSNR test for Animal 5 image

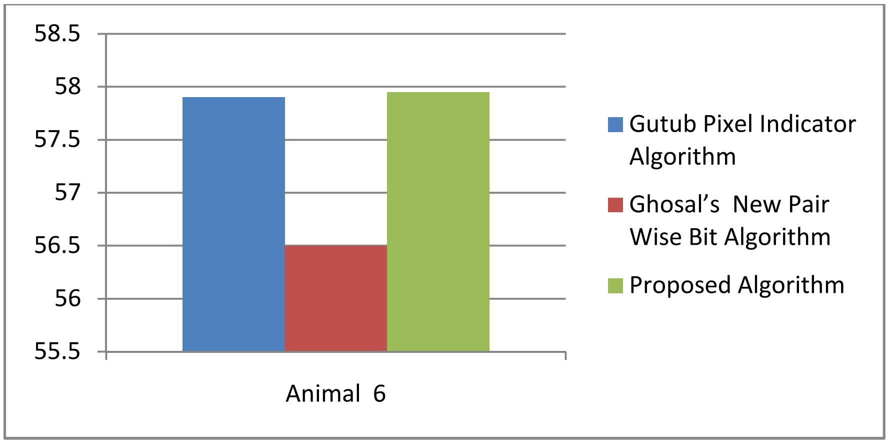


Figure (0-13) Shows the PSNR test for Animal 6 image

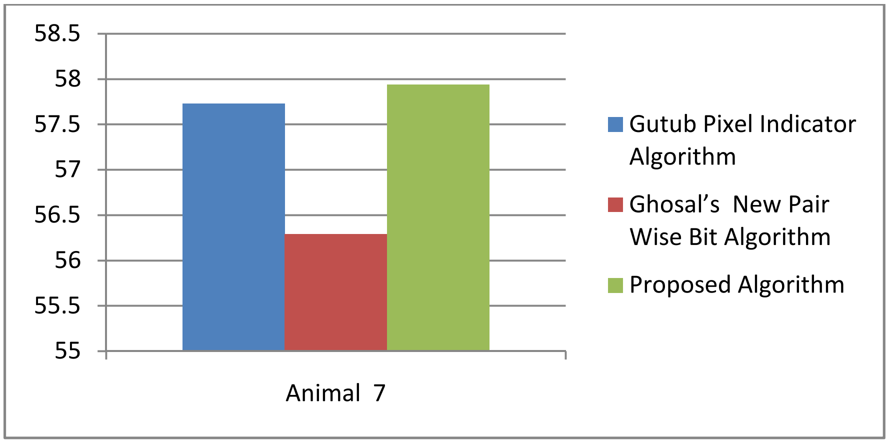


Figure (0-14) Shows the PSNR test for Animal 7 image

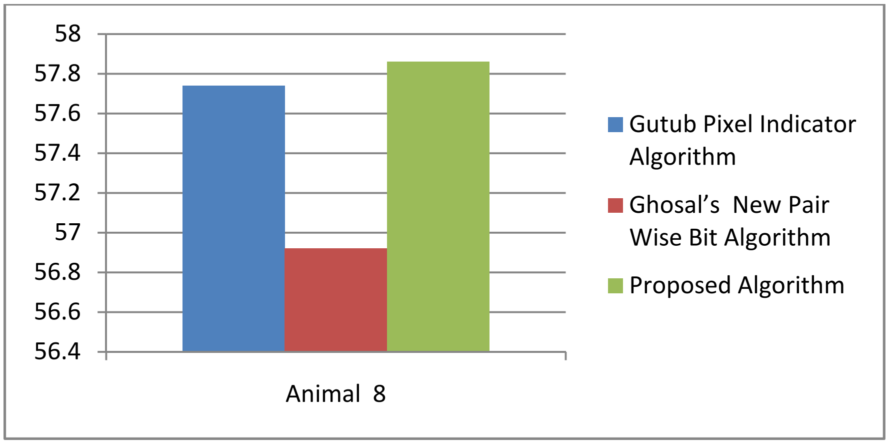


Figure (0-15) Shows the PSNR test for Animal 8 image

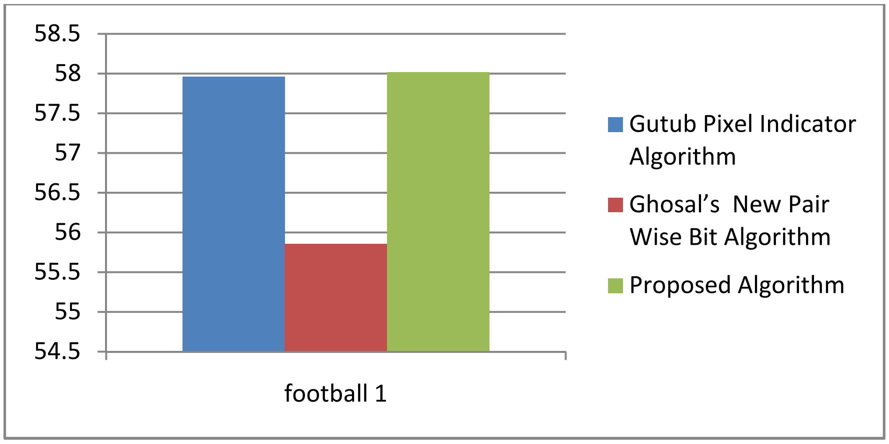


Figure (0-16) Shows the PSNR test for Football 1 image

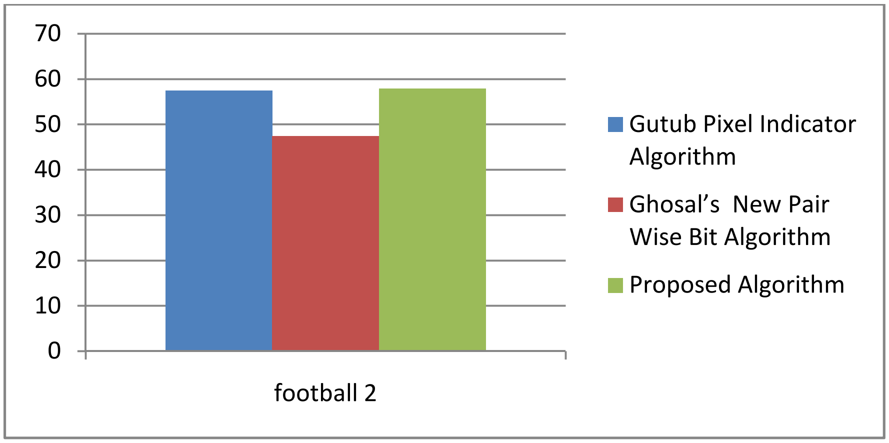


Figure (0-17) Shows the PSNR test for Football 2 image

6.2. Payload

The table (6-2) shows the data load which can be embedded inside different loads of the images by using proposed algorithm, Gutub pixel indicator and Ghosal's new pair wise bit algorithm with Bits estimated load.

This table shows that the data load which are embedded by using the proposed algorithm is bigger than the Gutub pixel indicator algorithm due to the reason that the proposed one can be embedded once or twice or three times in each channel while Gutub pixel indicator algorithm can be embedded once or twice times in each channel.

The table also shows some of approximate regarding the data load by using proposed algorithm and Ghosal's new pair wise bit algorithm for the reason that both of them can embed data reaching to 3 bits in each channel as maximum and one as minimum.

image	Image Size	Size of data By using Gutub Pixel Indicator Algorithm	Size of data By using Ghosal's New Pair Wise Bit Algorithm **Hiding Capacity (Bits)**	Size of data By using Proposed Algorithm **Hiding Capacity (Bits)**
		Hiding Capacity (Bits)	**Hiding Capacity (Bits)**	**Hiding Capacity (Bits)**
Animal 1	1024×1024	1572900	1692178	1692976
Animal 2	1024×1024	1575400	1869612	2087466
Animal 3	1024×1024	1559408	1782850	1869408
Animal 4	1024×1024	1588042	2762380	2789042
Animal 5	1024×1024	1572370	1456352	1572900
Animal 6	1024×1024	1521180	1665308	1671486
Animal 7	1024×1024	1583486	1811022	1833746
Animal 8	1024×1024	1562746	1413360	1542042
football 1	1024×1024	1552376	1646528	1648308
football 2	1024×1024	1462316	3144172	3052960

Table (0-9) Show Payload of data which can be embedded in different 24-bit colored bmp images

Figures (6-11),(6-12),(6-13),(6-14),(6-15),(6-16),(6-17),(6-18),(6-19) and (6-20) show Payload of data which can be embedded inside images (Animal 1, Animal 2, Animal 3, Animal 4, Animal 5, Animal 6, Animal 7, Animal 8, Football 1 and Football 2).

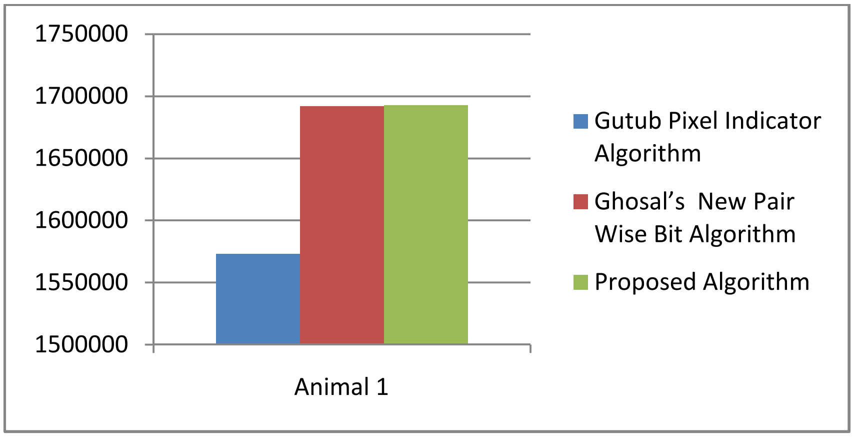


Figure (0-18) shows the payload inside Animal 1 image

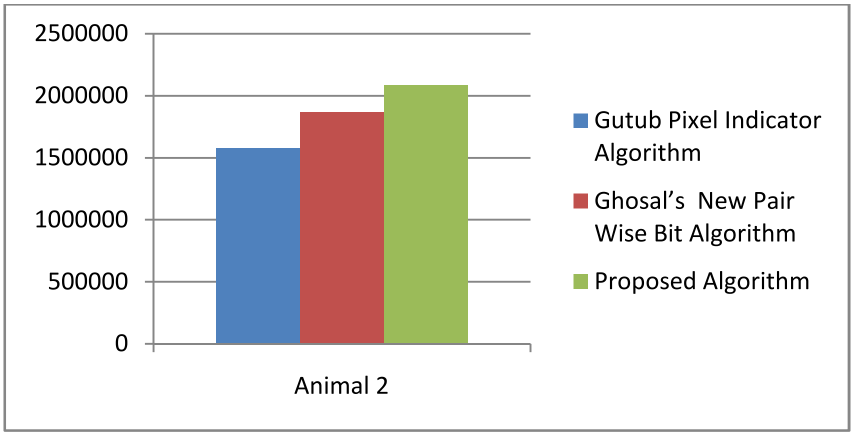


Figure (0-19) shows the payload inside Animal 2 image

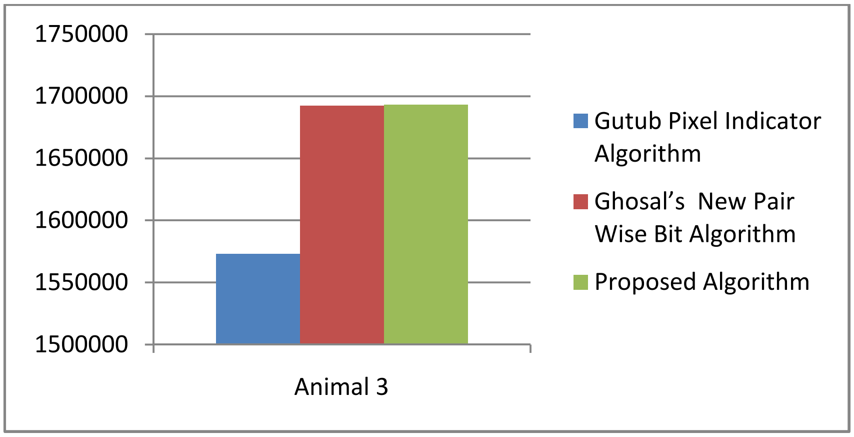


Figure (0-20) shows the payload inside Animal 3 image

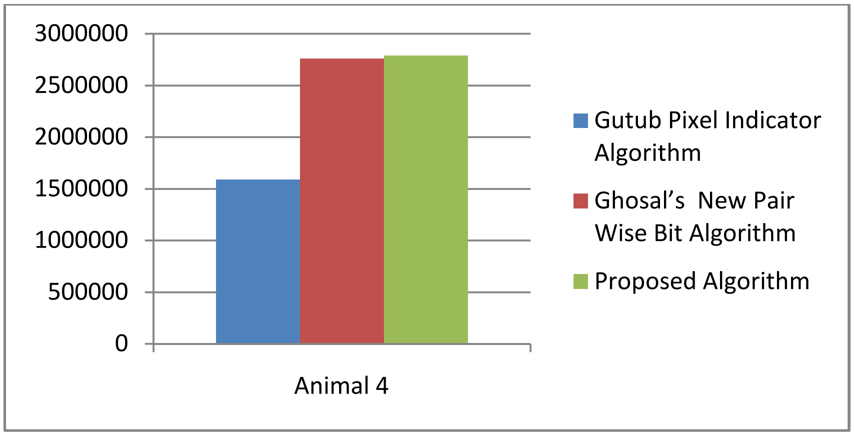


Figure (0-21) shows the payload inside Animal 4 image

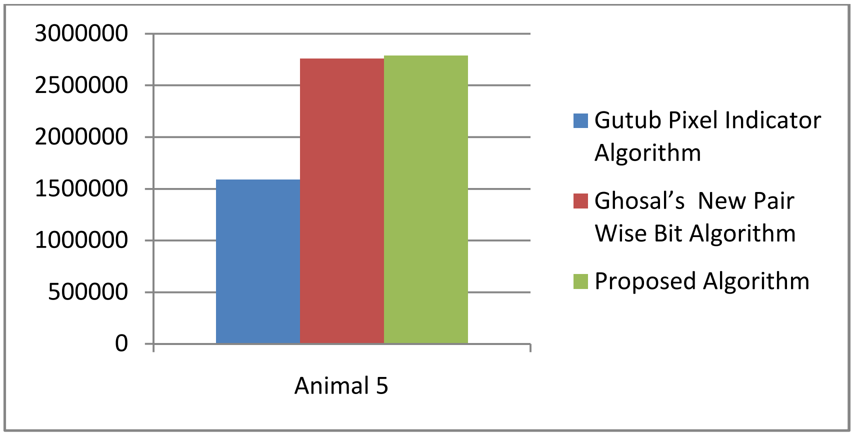


Figure (0-22) shows the payload inside Animal 5 image

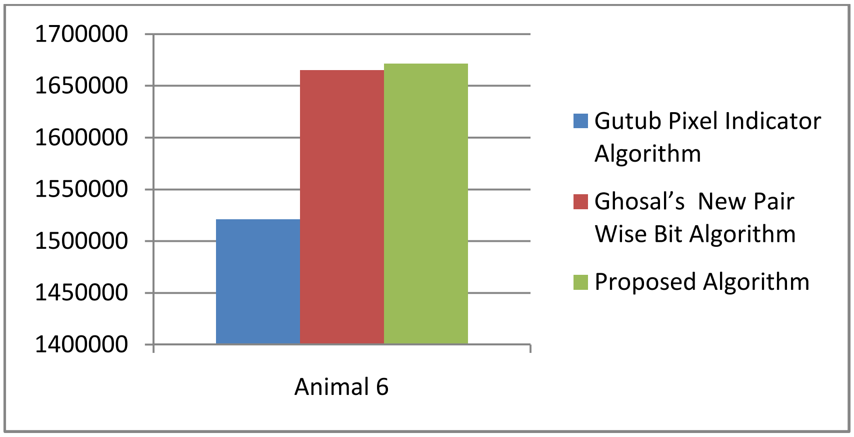


Figure (0-23) shows the payload inside Animal 6 image

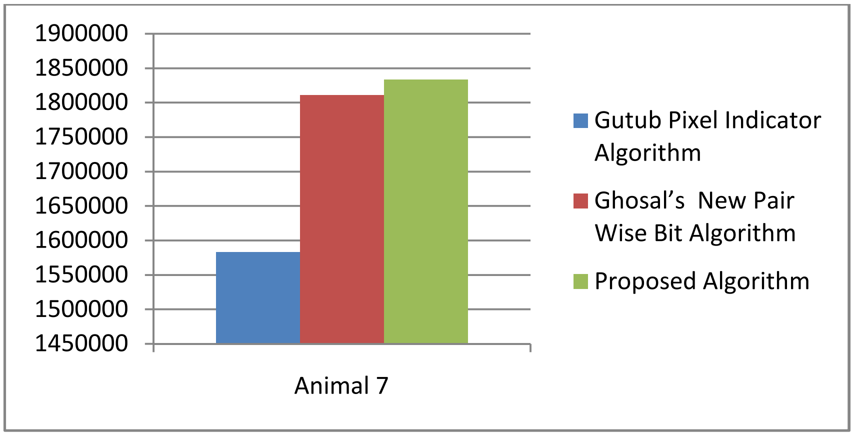


Figure (0-24) shows the payload inside Animal 7 image

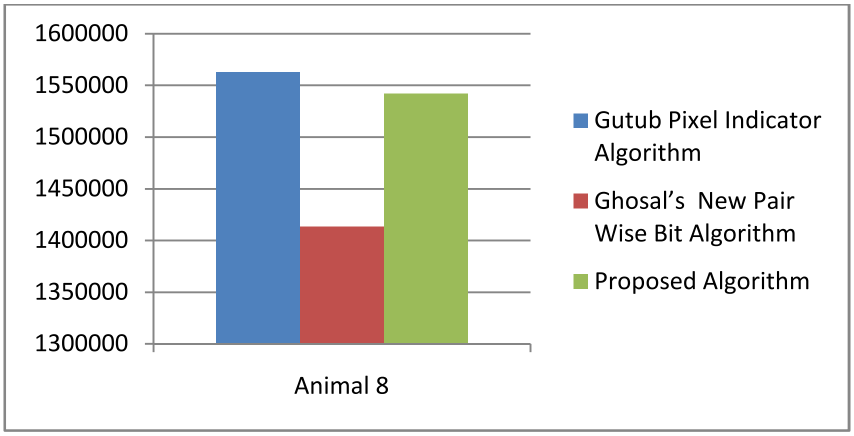


Figure (0-25) shows the payload inside Animal 8 image

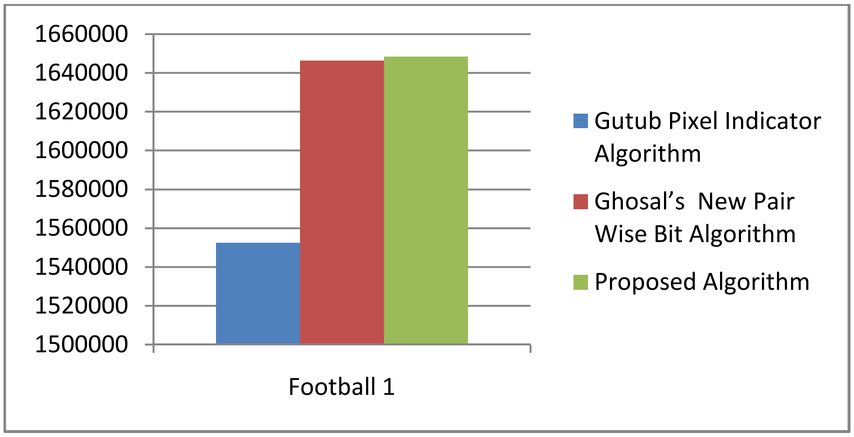


Figure (0-26) shows the payload inside Football 1 image

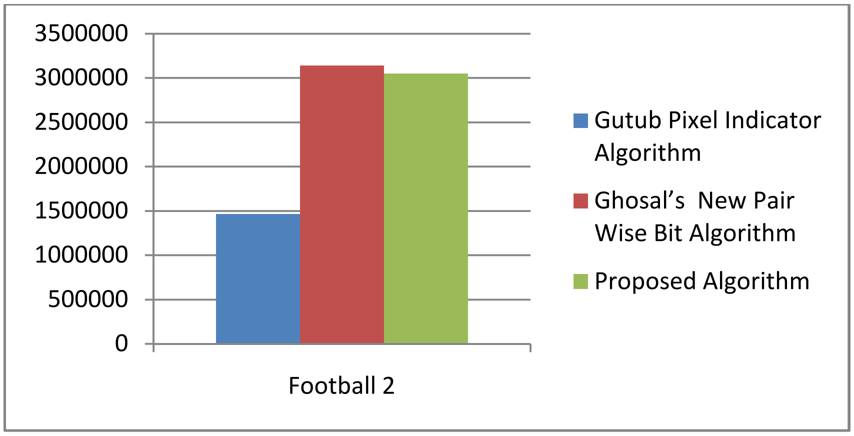
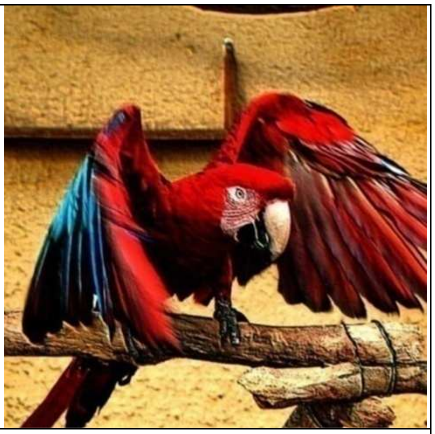
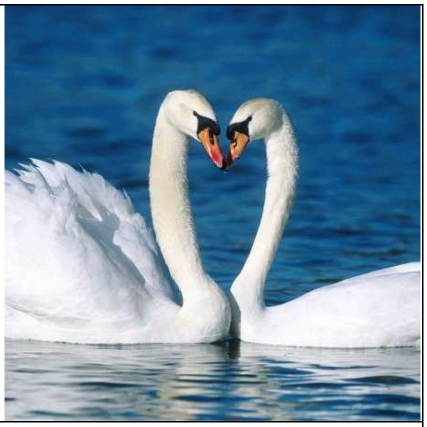


Figure (0-27) shows the payload inside Football 2 image

Figures (6-21-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 1) picture by proposed algorithm.

	
Figure (0-28-A) Cover-image for (Animal 1) with size 1024X1024	Figure (00-29-B) Stego-image for (Animal 1) with size 1024X1024

Figures (6-22-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 2) picture by proposed algorithm.

	
Figure (0-30-A) Cover-image for (Animal 2) with size 1024X1024	Figure (0-31-B) Stego-image for (Animal 2) with size 1024X1024

Figures (6-23-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 3) picture by proposed algorithm.

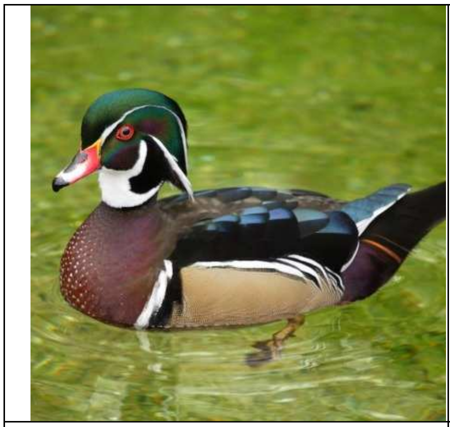


Figure (0-32-A) Cover-image for (Animal 3) with size 1024X1024	Figure (0-33-B) Stego-image for (Animal 3) with size 1024X1024

Figures (6-24-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 4) picture by proposed algorithm.

Figure (0-34-A) Cover-image for (Animal 4) with size 1024X1024	Figure (0-35-B) Stego-image for (Animal 4) with size 1024X1024

Figures (6-25-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 5) picture by proposed algorithm.

Figure (0-36-A) Cover-image for (Animal 5) with size 1024X1024	Figure (0-37-B) Stego-image for (Animal 5) with size 1024X1024

Figures (6-26-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 6) picture by proposed algorithm.

Figure (0-38-A) Cover-image for (Animal 6) with size 1024X1024	Figure (0-39-B) Stego-image for (Animal 6) with size 1024X1024

Figures (6-27-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 7) picture by proposed algorithm.

Figure (0-40-A) Cover-image for (Animal 7) with size 1024X1024	Figure (0-41-B) Stego-image for (Animal 7) with size 1024X1024

Figures (6-28-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Animal 8) picture by proposed algorithm.

Figure (0-42-A) Cover-image for (Animal 8) with size 1024X1024	Figure (0-43-B) Stego-image for (Animal 8) with size 1024X1024

Figures (6-29-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Football 1) picture by proposed algorithm.

Figure (0-44-A) Cover-image for (Football 1) with size 1024X1024	Figure (0-45-B) Stego-image for (Football 1) with size 1024X1024

Figures (6-30-A,B) shows Cover-image, Stego-image after embedding 2120 byte inside (Football 2) picture by proposed algorithm.

Figure (0-46-A) Cover-image for (Football 2) with size 1024X1024	Figure (0-47-B) Stego-image for (Football 2) with size 1024X1024

6.3. Security Test

This test depends on the comparison between the original image and the image after embedding of data inside through the following statistical tool Histogram, The degradation of the quality of images can also be visually noticed by applying the histogram analysis. In statistics, a histogram is a graphical display of tabulated frequencies, shown as lines. It shows what proportion of cases fall into each of several categories: it is a form of data binning. So, we have compared the histogram of three different images (Animal 1, Football 1 and Football 2) where the histogram is calculated for R, G and B channel separately. Here, Figure (6-31), Figure (6-32), Figure (6-33), Figure (6-34), Figure (6-35) and Figure (6-36) shows three different comparison results of histograms of Animal1.bmp, Football1.bmp and Footbal2.bmp with their stego-images.

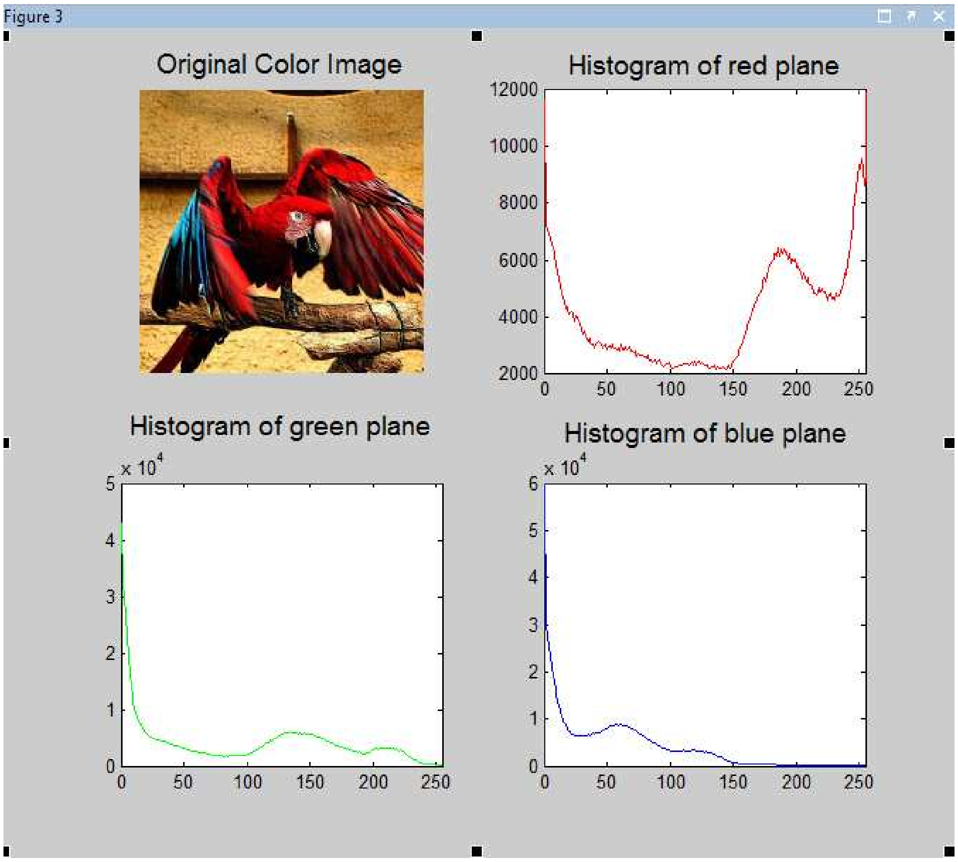


Figure (0-48) Histogram of Original Animal1.bmp

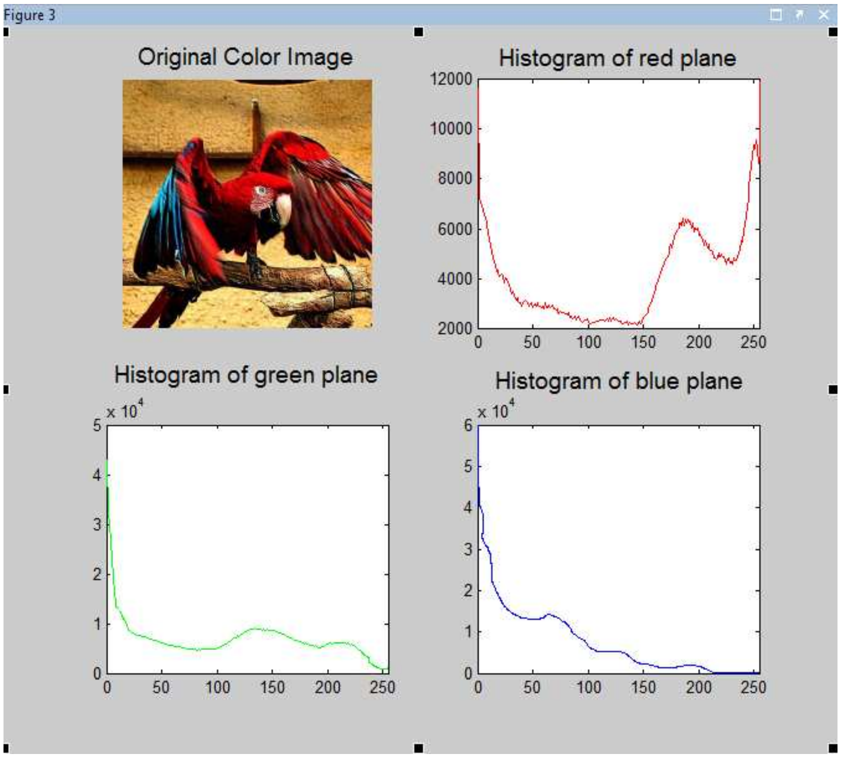


Figure (0-49) Histogram of Stego-Animal1.bmp

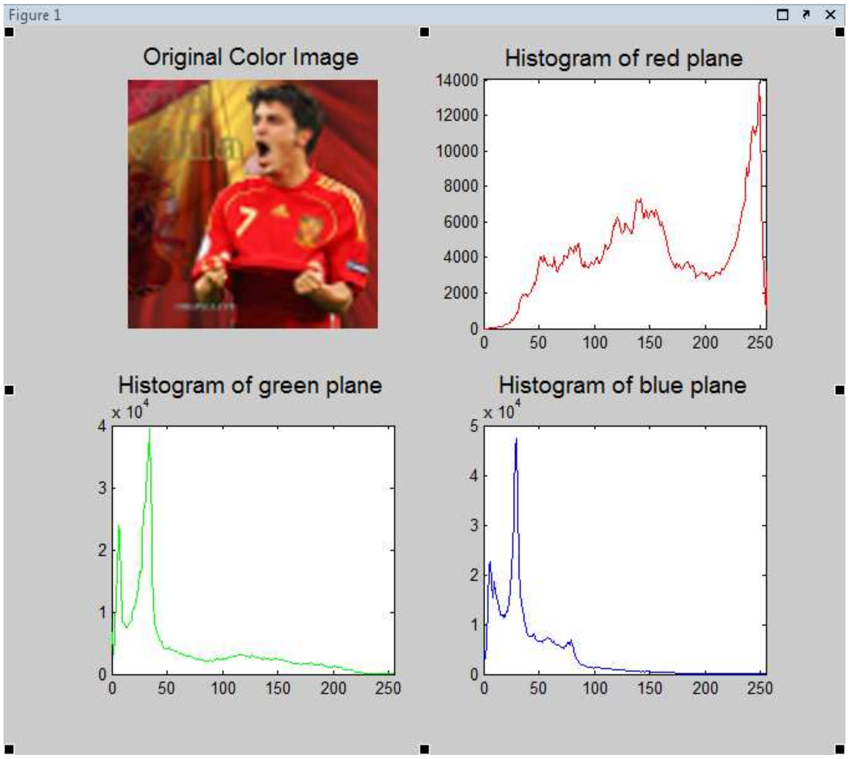


Figure (0-50) Histogram of Original Football1.bmp

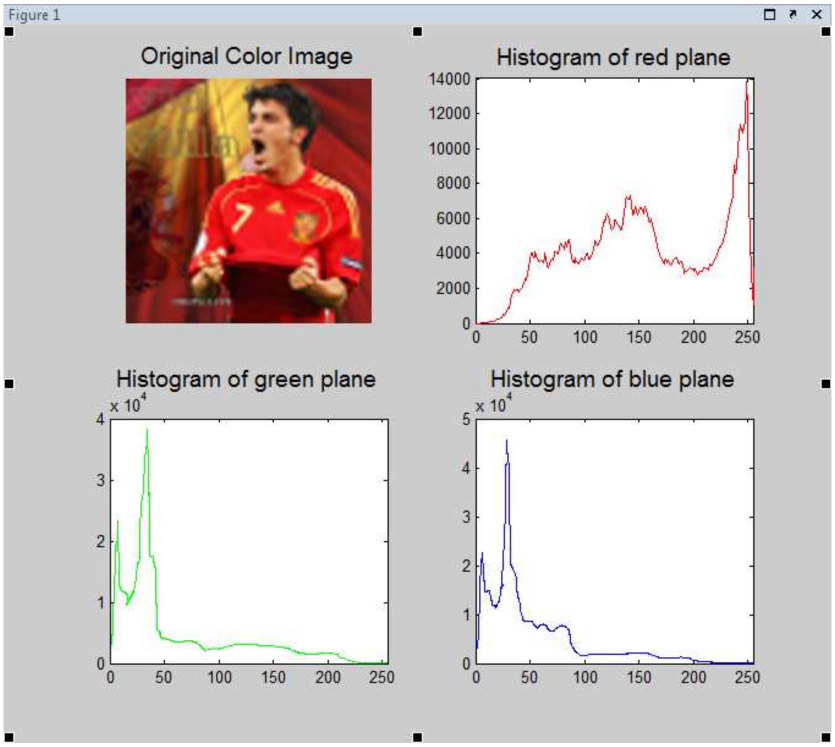


Figure (0-51) Histogram of Stego-Football1.bmp

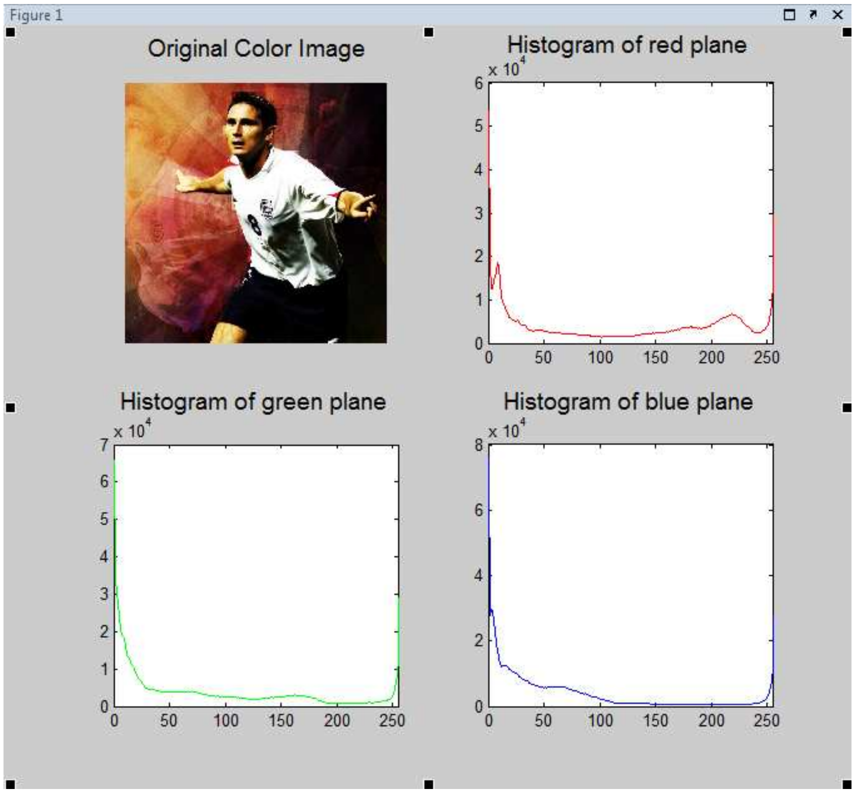


Figure (0-52) Histogram of Original Football2.bmp

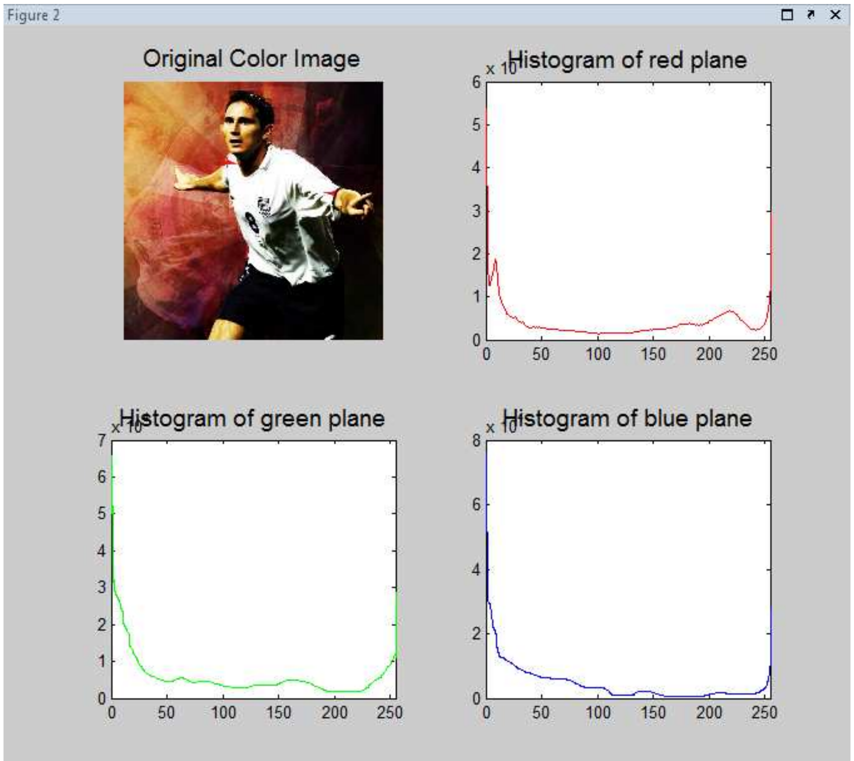


Figure (0-53) Histogram of Stego-Football2.bmp

After studying the above tables', figures and performing calculation based on PSNR value, average hiding capacity and after viewing the above three figures we can conclude that the average hiding capacity of the proposed technique shows more satisfied experimental out comes, retains good visual clarity of stego images, In the histogram analysis the histogram of red channel is unchanged because we have used the red channel as an indicator for bit embedding whereas significant changes in green and blue channel can be easily noticeable.

6.4. Robustness

All algorithms that operate to hide data inside the cover directly spatial domain is considered irresistible to vandalism operation like image processing operation pressure, rotation, cut …etc , when the image is used as a cover for data since that data were hidden within the image points, thus any image processing operation will result in changing of the points location or increasing or decreasing its load. This affects the hidden secret message within the image.

Chapter Seven

Chapter Seven

Conclusions

7.1. Overview

After studying known methods, we chose the method of the data embedding inside the cover directly which is distinguished by increasing of the data load but, it is irresistible for the vandalism operations.

7.2. Analystic Results

The new algorithm as suggested in comparison with Gutub pixel indicator and Ghosal's new pair wise bit algorithms which they have a relationship with the proposed algorithm. The comparison has been carried out throughout the following criteria: image quality test PSNR, Data load which can be embedded inside the image bayload, security test histogram along with testing the vandalism's resistance.

Concerning, The test of the quality of the image through PSNR image quality, the proposed algorithm shows more satisfied experimental out comes.

Figure (7-1) show image quality by comparing between the original images after embedding of the secret data inside it by using PSNR on the following images (Animal 1, Animal 2, Football 1 and Football 2).

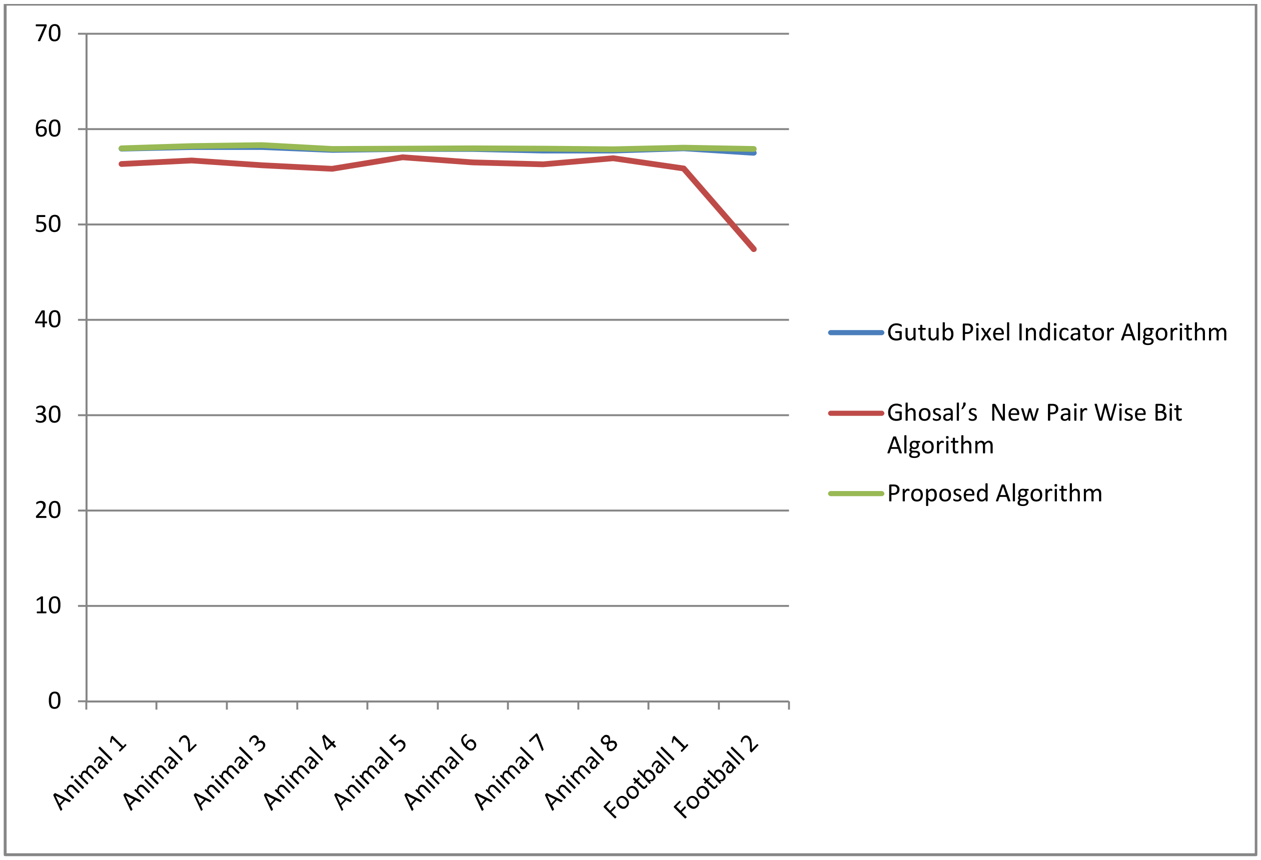


Figure (0-54) Shows the PSNR test on the following images :

(Animal 1, Animal 2, Animal 3, Animal 4, Animal 5, Animal 6, Animal 7, Animal 8, Football 1 and Football 2).

The data load that will be embedded by using the proposed algorithm is bigger than the data that will be embedded by using Gutub pixel indicator algorithm and the reason for that the proposed algorithm can be embedded from one bit to three bits in each point while Gutub pixel indicator algorithm is embedded only one bit where there is a convergence regarding the data load by using both the proposed algorithm and the Ghosal's new pair wise bit algorithm due to the reason that both of them can embedded data reach to three bits in each point as maximum and one binary as minimum.

Figure (7-2) show the payload inside the following images (Animal 1, Animal 2, Animal 3, Animal 4, Animal 5, Animal 6, Animal 7, Animal 8, Football 1 and Football 2).

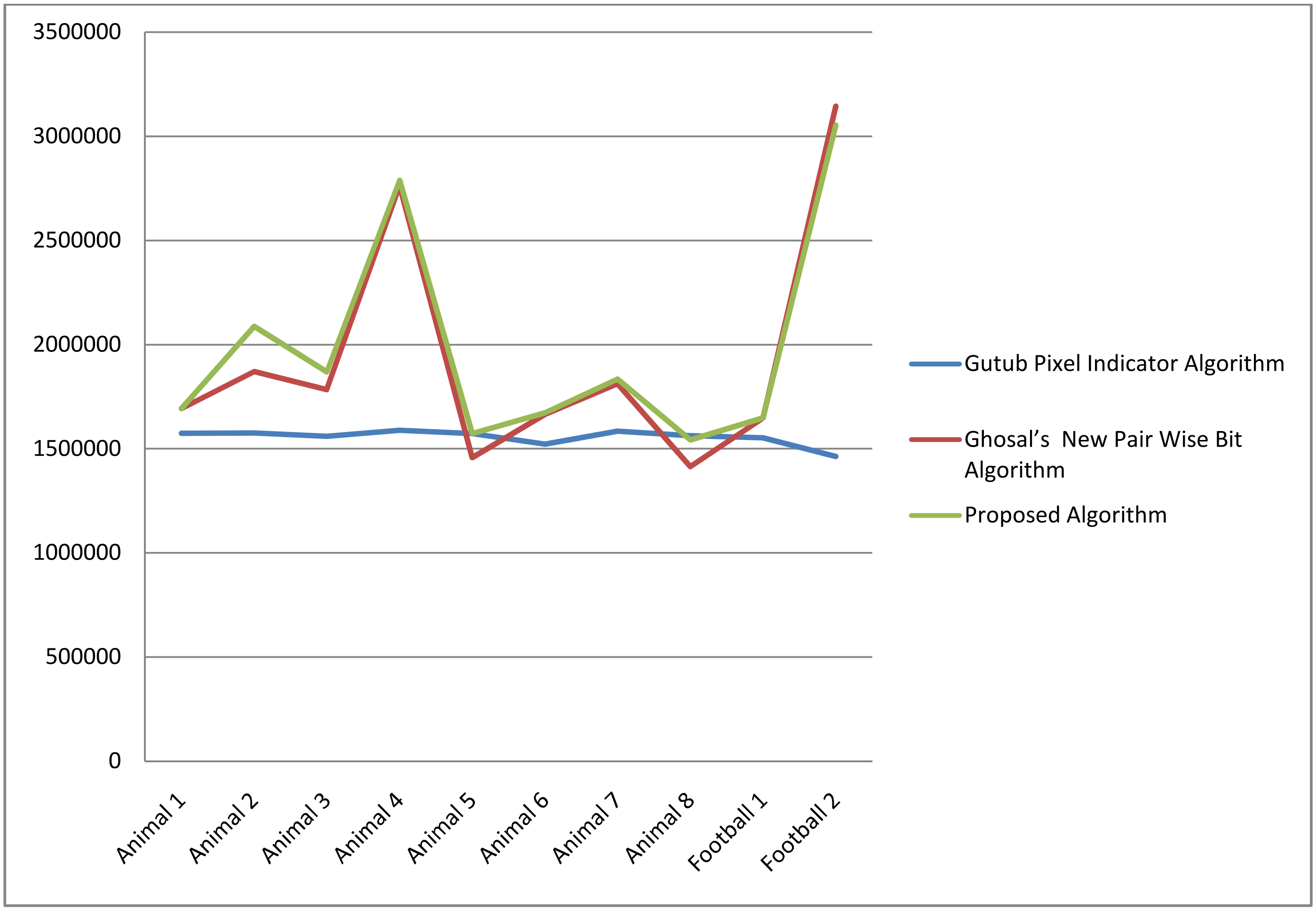


Figure (0-55) shows the payload inside the following images :

(Animal 1, Animal 2, Animal 3, Animal 4, Animal 5, Animal 6, Animal 7, Animal 8, Football 1 and Football 2).

All of algorithms which depends in hiding the data inside the cover directly is considered resistible to vandalism operations when the image is used as a cover for data because the data in this case are hidden within the image points, therefore, any processing on this image will lead to the relocation of points or raise or lower their value which affects the hidden secret message within the image.

7.3. Future Works

This study is considered the basic phase for several future researches and the following operations can be carried out to improve the performance of this algorithm:

1. Proposed algorithm is used to hide the data by using 24-bit bmp colored images; therefore, this study can be expanded on the 32-bit bmp colored images.
2. Developing this algorithm where it can save the secret message even after execution of some modification operations on the image such as pressure, rotation … and so on.
3. Possibility to hide other types of data, such as an image inside another one looks very attractive for studying.
4. Linking between the encryption process and steganography for a higher degree of protection to the data so that the text is encrypted before hiding to increase the security of this algorithm.
5. Using the general key concept in encryption process in shorthand art algorithms where the data can be embedded inside the general key and extract it with the private key.

References

AL-Oqqily, I. (2003). *A Robust Discrete Cosine Transformation-Based Watermarking Algorithm For Digital Images*, (Unpublished Master Thesis), The University Of Jordan, Amman, Jordan.

Anand J.V. & Dharaneetharan G. D. (2011) *New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance Data Security , Proceedings of the 2011 International Conference on Communication, Computing & Security*, 474-476.

Cachin, C. (1998) An Information-Theoretic Model for Steganography, Information Hiding, *Proceeding of Second International Workshop*, Volume. 1525 of lecture Notes in Computer Science, Springer, 306-318.

Cachin, C. (2005) Digital Steganography, *Encyclopedia of Cryptography and Security*, 2005.

Chapman, J. S. (2002). *Matlab Programming for engineers*, (2nd ed), Cole: Thomson Books.

Etting J. Mark. (1998) Steganalysis and Game Equilibria, Information Hiding, *Proceeding of Second International Workshop*, Vol. 1525 of lecture Notes in Computer Science, Springer,319-328.

Fabien, A., Ross,J. & Markus, G. (1999) Information Hiding- ASurvey, *Proceeding of the IEEE, special issue on protection of multimedia content*, 87 (7), 1062-1078.

Ghosal, S. K (2011) A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique, *Greater Kolkata College of Engineering & Management*, Kolkata, India.

Gutub, A. A. (2010) Pixel indicator technique for RGB image Steganography, *Journal of emerging technologies in web intelligence*, 2 (1), 56-64.

Gutub, A.A., Ankeer, M., Abu-Ghalioun, M., Shaheen, A., & Alvi, A. (2008). Pixel indicator high capacity technique for RGB image based steganography , *WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E. 18 – 20

Johnson, N., Jajodia, S. (1998) Exploring Steganography: seeing the inseen, *IEEE Computer*, 58 (8), 26-34.

Johnson, N.F., Duric, Z., Jujodia, S. (2001). *Information hiding: steganography and watermarking attacks and countermeasures*, (1st ed), Boston: kluwer Academic.

Kahn, D. (1983). *The Code breakers: The Story of Secret Writing*, New York: Macmillan.

Katzenbeisser, S., Petitcolas, F. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*, Boston: Artech House.

Khader, M. (2004). *Hiding Text In Digital Images Using Steganography Techniques*, (Unpublished Master Thesis), The University Of Jordan, Amman, Jordan.

Kutter, M. & Petitcolas, F. (1999) A Fair benchmark for image Watermarking Systems, *proceeding of Electronic Imaging Journal* , Vol. 3657, 226-239.

Marvel, L.M., Boncelet, J. & Retter, C. T. (1999) Spread Spectrum Image Steganography, *IEEE Trans. On Image Processing*, 8 (8), 1075-1083.

Na-1, W. (2004). *"A study on data hiding for gray-level and binary images* ", viewed by 14 oct 2012, Retrieved from http://ethesys.lib.cyut.edu.tw/ETD-db/ETD-search/getfile?URN=etd-0707104-144705&filename=etd-0707104-144705.pdf.

Rabah, K. (2004) steganography-The Art of Hiding Data, *Information Technology Journal*, 3 (3), 245-269.

Simmons, G. (1983) The prisoners problem and the subliminal channel, *CRYPTO*, 51-67.

Zollner, J. F., Klimant, H., Tzmann, H. P., Piotraschke A., West, R., Wicke, A. & Wolf, G. (1998) Modeling the security of steganographic systems, *Second international Information Hiding Workshop*, 46 (8), 345-355.