



Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method

إخفاء النصوص في صور من نوع **RGBA** باستخدام قناة ألفا و طريقة المؤشر

By
Ghaith Salem Sarayreh
(400910328)

Supervisor
Dr. Mudhafar Al-Jarrah

A thesis Submitted in partial Fulfillment
of the requirements of the Master Degree in Computer Science

Faculty of Information Technology

Middle East University

Amman – Jordan
Jan, 2014

Authorization Statement

I, Ghaith Salem Alsarayreh, authorize Middle East University to supply hard and electronic copies of my thesis to libraries, establishments, bodies, and institutions concerned with research and scientific studies upon request, according to university regulations.

Name: Ghaith Salem Alsarayreh

Date: 27-1-2014

Signature:

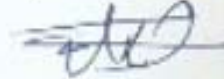


إقرار تفويض

أنا غيث سالم الصرايرة أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي
للمكتبات أو المؤسسات أو الهيئات المعنية بالأبحاث و الدراسات العلمية أو الأفراد عند
طلبها.

الاسم: غيث سالم الصرايرة

التاريخ: ١٠/١٠/٢٠١٧

التوقيع: 

COMMITTEE DECISION

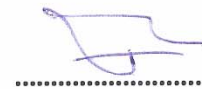
This is certifying that the thesis entitled "Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method" Was successfully defended and approved on January 27th 2014.

Examination Committee Members

Signature

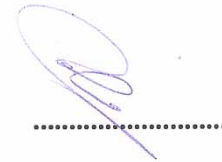
Dr. Ahmad k. Ahmad **Chairman**

Department of Computer Information System
(Middle East University)



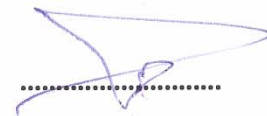
Dr. Mudhafar Al -jarrah **Member & supervisor**

Department of Computer Information System
(Middle East University)



Dr. Jihad Alsadi **Member**

Department of Computer Information System
(Arab Open University)



DEDICATION

I dedicate this thesis to my parents, who first planted the seeds of knowledge and wisdom in me. From my birth and throughout the development of my life, they have encouraged me with love and care to seek out knowledge and excellence. They challenged me to pursue my dreams, which led me to the completion of this endeavor.

ACKNOWLEDGEMENTS

At first I would like to acknowledge my supervisor Dr. Modhafar Al-jarrah who offered me guidance and assistance throughout my study. I wish to thank all my friends and family, who helped me by contributing in many ways.

Abstract

Steganography is the art and science of protecting confidential information through concealing its existence. It is an ancient art of hiding secret messages in forms or media that cannot be observed by an adversary. The field of Steganography has been revived lately to become an important tool for secure transmission of secret messages.

This thesis investigates the hiding of text messages and documents within the alpha channel of RGBA color images. The proposed model consists of two phases. In the first phase the secret text is stored as bits in the LSB part of the alpha channel. The number of bits stored in each alpha channel of a pixel is variable, in order to make it harder for an attacker to detect. The RGB color channels of a pixel are used as a guide or indicator to select the number of bits to store in the alpha channel of the same pixel. The numbers of hidden bits per pixels are 1, 2, or 3, depending on the indicator value, which gives an average of 3 bpp. This phase is implemented in two algorithms: Embed, to hide a secret text document inside a cover image of RGBA type, and Extract, to recover the hidden text document from the stego image produced during embedding.

The purpose of the second phase is to separate the alpha channel from the RGB channels of the stego image, and to attach the alpha channel to a different image, a semi-stego, with different RGB channels values, in other words to Swap the alpha channel of the two un-related images. The resulting semi-stego RGBA image will show no relationship between the color channels and the alpha channel. The semi-stego image is transmitted to the destination. At the destination, the semi-stego goes through another swap, in which the alpha channel is separated and attached to a copy of the original cover image which the destination will have for this purpose. The final part of this phase is the extraction of the secret message from the re-created stego RGBA image. The swapping operation is implemented in the Swap algorithm.

The experimental work tested the hiding and extraction of text documents of various sizes, up to the maximum hiding capacity. The stego images showed no visual quality degradation even with using the maximum hiding capacity. A comparison is made

of the PSNR metric between the proposed model and that of a model that uses hiding in the RGB channels, using the same color images, and an equal size secret messages. The results showed a similar or improved PSNR value for most of the test pairs of image / text.

The contributions of this work is three fold: (i) hiding in the alpha channel, leaving the color channels un-altered, which gives better un-detectability compared to just RGB, (ii) Using the color channel as an indicator to store in the alpha channel, and (iii) Using the Swap operation to exchange the alpha channel between the original stego image and the semi-stego image.

The proposed algorithms have been implemented in Matlab 2012b. A possible application of the proposed model is in the hiding of confidential documents transmitted over public networks. The thesis ends with conclusions and suggestions for further work.

الملخص

إسلوب الكتابة المخفية (ستيغانوغرافي) هو علم وفن حماية المعلومات السرية من خلال إخفاء وجودها . إنه فن قديم لإخفاء الرسائل السرية في أشكال ووسائط مختلفة بحيث لا يمكن ملاحظتها من جهة معادية . لقد تم إحياء حقل الكتابة المخفية مؤخرا وأصبحت أداة مهمة للتراسل الآمن للرسائل السرية .

تبحث هذه الرسالة في إخفاء الوثائق النصية في قناة ألفا للصور الملونة نوع RGBA. يتكون الموديل المقترح من مرحلتين . في المرحلة الأولى يتم تخزين النص السري بصيغة بت في الجزء الأقل أهمية (LSB) من قناة ألفا . عدد البتات المخزونة في قناة ألفا التابعة لبكسل (Pixel) يكون متغيرا ، وذلك لجعل الكشف أصعب على المهاجم . يتم استخدام قيم الألوان الثلاثة كدليل لاحتمال عدد البتات للخرن في قناة ألفا . عدد البتات المخفية في قناة الفا يكون إما 2 أو 3 أو 4 ، اي بمعدل 3 بت للبكسل ، والذي يتم تحديده اعتمادا على قيمة دليل الألوان. تم تطبيق هذا الجزء في خوارزميتين: خوارزمية ضمن (Embed) لإخفاء الرسالة السرية في ملف غطاء نوع RBGA ، وخوارزمية إستخرج (Extract) لاستخراج الوثيقة السرية .

الغرض من المرحلة الثانية هو لفصل قناة ألفا عن قنوات الألوان في الصورة المعدلة (stego) ولربط قناة ألفا لصورة مختلفة ، صورة تمويه ، والتي يكون لها قيم لونية مختلفة ، بمعنى آخر تبادل قناتي ألفا للصورتين . صورة التمويه (semi-stego) الناتجة عن التبادل لن يكون فيها أي علاقة بين قنوات الألوان وقناة ألفا . يتم إرسال صورة التمويه الى الجهة المستلمة حيث يتم هناك إعادة تبادل قناة ألفا ، ويكون بين صورة التمويه ونسخة عن الصورة الاصلية التي تكون متوفرة لدى المتلقي . الجزء الاخير من هذه المرحلة يكون بإستخراج الرسالة السرية من الصورة المعدلة الناتجة عن التبادل . يتم تنفيذ عملية التبادل في خوارزمية إستبدال (Swap) .

العمل التجريبي تضمن الإخفاء والإستخراج لوثائق نصية متعددة بأحجام مختلفة منها الحد الاعلى لسعة الخزن . الصور المعدلة لم يظهر عليها تغيير خلال التقييم بالنظر وعند الخزن بالحد الأقصى .تم إجراء مقارنة لمعيار التشويش بين النموذج المقترح ونموذج يستخدم الخزن في قنوات الألوان ، وبإستخدام نفس للصور الملونة ووثائق نصية متساوية . بينت النتائج قيم متساوية او أفضل في معيار التشويش للموديل المقترح ، في حالات عدة حالات من الصور والوثائق النصية.

مساهمات هذا البحث يمكن إيجازها فيما يلي: (أ) إخفاء البيانات في قناة ألفا بدون تغيير في قنوات الألوان والذي يؤدي الى احتمالية كشف أقل ، (ب) إستخدام قنوات الألوان كمؤشر ، و (ج) استخدام عملية التبادل لتبديل قناة الفا بين الصورة المعدلة والصورة التمويهية .

نفذت الخوارزميات في نظام Matlab 2012b .

من التطبيقات الممكنة للموديل المقترح إخفاء الوثائق السرية التي يتم إرسالها على الشبكات العامة . تنتهي الرسالة بتقديم الاستنتاجات والاعمال المستقبلية .

Content

Cover Page	I
Authorization Statement	II
إقرار تفويض	III
Examination Committee Decision	IV
DEDICATION	V
ACKNOWLEDGEMENTS	VI
Abstract	VII
الملخص	IX
Content.....	X
List of Tables	XIII
List of Figures	XIV
List of Abbreviations	XV
Chapter (1) : Introduction	1
1.1 Introduction.....	1
1.2 Problem Definition.....	5
1.3 Objectives	5
1.4 Problem Significance and Motivation.....	5
1.5 limitations	5
1.6 Methodology	6
1.7 Thesis Layout.....	6
Chapter (2) : Termenology and Basic concepts of stegonagrphy	7
2.1 stegonagrphy	7
2.2 stegonagrphy categories according carrier type	7
2.2.1 text stegonagrphy	8
2.2.2 image stegonagrphy	8
2.2.3 audio stegonagrphy	9
2.2.4 video stegonagrphy	9
2.2.5 Protocol stegonagrphy	10
2.3 stegonagrphy process.....	10
2.4 uses of stegonagrphy	10
2.5 stegonagrphy algorithms	11
2.6 security servieces offered by stegonagrphy	11
2.7 stegonagrphy problems	12
2.8 stegonagrphy types	12
2.8.1 pure stegonagrphy.....	12
2.8.2 secret key stegonagrphy.....	13
2.8.3 public key stegonagrphy	13
2.9 stegonagrpic technique	14
2.9.1 Least Significant Bit (LSB)	14
2.9.2 Masking and Filtering	14
2.9.3 Transform Technique	15

Chapter (3) : Literature survey.....	16
3.1 Introduction	16
3.2 Information Hiding	16
3.3 Information Hiding Technique	17
3.3.1 Injection	17
3.3.2 Substitution	17
3.3.3 Generation	17
3.4 Cover Image Formats	18
3.5 RGBA Color Image	19
3.6 Alpha Channel	20
3.7 Related Work	21
3.7.1 RGB image based stegonagrphy	21
3.7.2 Spitial Domain Based On RGB Image	21
3.7.3 Using The Two Least Significiant Bits As Indicator	22
3.7.4 Caculating The Number Of Ones And Zeros In Red Channel	22
3.7.5 Hiding Data Directly in a Special Domain	23
Chapter (4) : Steganography Evaluation Criteria.....	24
4.1 Steganography Evaluation Criteria	24
4.1.1 Capacity	24
4.1.2 Robustness	24
4.1.3 Undetectable	25
4.1.4 Invisibility	25
4.1.5 Security	25
4.2 Steganalysis Attacks	25
4.3 Attacks to Steganographic Systems	26
4.4 Full-reference Metrics (FR)	28
4.1.4 Peak Signal to Noise Ratio (PSNR).....	28
4.1.5 Mean Square Error (MSE).....	28
Chapter (5) : The proposed alpha based steganography method	30
5.1 The proposed algorithm	30
5.1.1 Embedding process	30
5.1.2 Extracting process	34
Chapter (6) : Experimental work and Discussion of results	37
6.1 Implementation	37
6.2 Image selection	37
6.3 Embedding processes.....	37
6.4 Extracting processes.....	39
6.5 Discussion of results	41
6.6 Example for sending and receiving a message	46
Chapter (7) : Conclusion and Future Work	53
7.1 Conclusion	53

7.2	Future Work.....	53
	References.....	55

List of Tables

Table 3.1: Alpha value representation	20
Table 3.2: The indicator relation with the hidden data and the other two channels	22
Table 6.1: Proposed algorithm Vs Ghosal Algorithm	41
Table 6.2: Evaluation criteria for four images.....	42

List of Figures

Figure	page
Figure 1.1: Cryptography Processes	4
Figure 2.1: Steganography Categories According Carrier Types	8
Figure 2.2: The Steganography Process.....	10
Figure 3.1: RGBA Image channels.....	19
Figure 5.1: Embedding Process	31
Figure 5.2: Proposed Embedding Model	33
Figure 5.3: Extracting Process	34
Figure 5.4: Proposed Extracting Model	36
Figure 6.1: load cover image.....	38
Figure 6.2: choosing text file.....	38
Figure 6.3: saving stego image.....	39
Figure 6.4: choosing stego image.....	40
Figure 6.5: Extracted information.....	40
Figure 6.6: Cover and Stego Image of Baboon	42
Figure 6.7: Cover and Stego Image of Flower	43
Figure 6.8: Cover and Stego Image of Horse	43
Figure 6.9: Cover and Stego Image of Lenna	44
Figure 6.10: Histogram analysis Baboon Image.....	44
Figure 6.11: Histogram analysis Flower Image.....	45
Figure 6.12: Histogram analysis Horse Image.....	45
Figure 6.13: Histogram analysis Lenna Image.....	46
Figure 6.14: Cover image.....	46
Figure 6.15: Semi-Stego Image.....	46
Figure 6.16: Load secret message	47
Figure 6.17: Load secret message	47
Figure 6.18: Save stego image.....	48
Figure 6.19: Load stego image	48
Figure 6.20: Choose Semi-Stego image.....	49
Figure 6.21: Save semi-stego image with alpha.....	49

Figure 6.22: Load semi-stego image with alpha.....	50
Figure 6.23: Load cover image.....	50
Figure 6.24: Save stego image with alpha.....	51
Figure 6.25: Load stego image with alpha.....	51
Figure 6.26: Save message	52

List of Abbreviations

PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
FR	Full-reference Metrics
TIFF	Tagged Image File Format
BMP	Microsoft Windows Bitmap
PNG	Portable Network Graphic
LSB	Least significant bit insertion
DCT	Discrete Cosine Transform

Chapter One

Introduction

1.1 Introduction

Data transmission security has become an extremely important field of research, due to the rapid rise in cybercrime, information theft, industrial espionage and attacks on private individuals' data. Even business documents that are not sent over the internet can be at a risk, by insiders attack. One important defense against such attacks is a technique to hide the existence of private documents from un-authorized individuals Steganography is to hide secret information in carriers (media) such as images, audio files, text files, videos and data transmission channels (Johnson, et al., 2001),(Curran & Bailey, 2003).

Steganography literally means covered writing which derived from two Greek words "*steganos*", meaning "covered," and "*graphein*", meaning "to write. Steganography is hiding information through a secret channel so that it will not be detected, so that only the intended recipient or the sender realizes that there is a hidden message (Cachin, 2004).

The objective of Steganography is sending a message through network to an intended receiver and preventing anyone else to know if the message is being sent (Johnson, et al., 2001).

Steganography is the art and science of encoding a secret message into an existing communication channel or into a payload (data unit) in such a way that only the sender and intended receiver are aware of its existence. (Petitcolas, et al., 1999).The main

objective of Steganography is to communicate safely and to avoid drawing suspicion to transmission of a hidden data (Johnson & Jajodia, 1998).

Steganography is the process that takes a piece of information and hides it within other information. Computer files such as images, audio files, and videos contain unused or insignificant areas of data. Steganography takes the information that we want to hide, and replacing them with these areas. Then the communication parties can exchange information without knowing of the third party what really lies inside of them. (Johnson, et al., 2001)

A multitude of methods of steganography have been used throughout history, the first used of steganography back to 440 BC (Uma Devi, 2006). There are many techniques used such as; the physical techniques by using the body and the material objects, digital techniques, network techniques, and digital text technique.

Throughout history, there are many of the stories about the use of steganography in several methods and techniques; the most prominent was the use of physical technical. There is a story about king of Sparta "Demaratus" (from 515 until 491 BC) when he wanted to notify Sparta that "Xerxes" intended to invade Greece. To avoid capture, he scraped the wax off of the tablets and wrote a message on the underlying wood. He then covered the tablets with wax again. The tablets appeared to be blank and unused so they passed inspection by sentries without question. In another story the used method was to shave the head of a messenger and tattoo a message or image on the messengers head. After allowing his hair to grow, the message would be undetected until the head was shaved again. (Petitcolas, et al., 1999)

Modern steganography entered the world in 1985 (Gaggar, et al., 2013) with the advent of the personal computers being applied to classical steganography problems, the following are an example of these techniques:

1. Hiding information within the lowest bits of images or sound files.
2. Hiding information within encrypted data or within random data.
3. Including data in ignored sections of a file such as hiding information in tampered executable files.
4. Embedding Pictures in a video file.
5. Modifying the echo of a sound file (Echo Steganography).
6. Making text the same color as the background in word processor documents, e-mails, and forum posts.

Network steganography is a general term of all information hiding techniques that may be used to exchange information in telecommunication networks. "Krzysztof Szczypiorski" was introduced this term in 2003 (Krzysztof, 2003).

Network steganography use the communication protocols control elements and their basic intrinsic functionality, unlike the typical steganography methods which use digital media such as images, audio and video files as a cover for hidden data (Craig, 1997).

Typical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the PDU (Protocol Data Unit). (Murdoch & Lewis, 2005)

Akbas (2010) said that "Unicode steganography uses lookalike characters of the usual ASCII set to look normal, while really carrying extra bits of information. If the text

is displayed correctly, there should be no visual difference from ordinary text. Some systems, however, may display the fonts differently, and the extra information would be easily spotted".

At the present time because of the massive amounts of sensitive and important data that is stored on computers and transmitted by the Internet, there is an urgent need to ensure security and safety of this information. Steganography and cryptography are methods to ensure security and safety of information.

Encryption is a science concerned with converting information into a form that is incomprehensible to the reader; this information may be stored in the storage media or transported via communication networks (Kumar, 2003). The difference between Steganography and cryptography is that Steganography hides the existence of a message, while cryptography is makes a message unintelligible even when the message is discovered by unauthorized partys. (Conrad, 2007) Figure 1.1 shows the encryption and decryption in cryptography.



Figure 1.1: Cryptography Processes

In cryptography different operations may be used depending on the purpose of cryptography, such as key generation, secrecy or privacy, message authentication, cryptography, and no repudiation; No repudiation is a way to ensure that a message has been sent and received by the parties of communication, which mean that the sender of a message cannot later deny send the message and that the recipient cannot deny receive the message. (Barker & Barker, 2008)

This thesis proposes a new steganographic method using the RGBA format for cover images, in which the alpha channel used as a storage location of text bits, while the RGB channels will be used purely as an indicator of the number of bits from the alpha channel to be flipped. In other words, the color channel will remain intact.

1.2 Problem Definition

The problem tackled in this thesis addresses the hiding of secret text documents in RGBA images, with the aim of reducing image distortion and improving un-detestability. The research idea focuses on the use of the indicator method (Gutub, et al., 2008) combined with the use of the alpha channel for storage of the text to be hidden.

1.3 Objectives

The aim of this work is to improve information hiding of text documents in digital images, using the indicator method and the alpha channel in RGBA images, taking into consideration relevant Steganography evaluation criteria.

1.4 Problem Significance and Motivation

The Steganography field at is one of the interesting areas of research in security, it is very important these days because of the need to secure data transmitted over networks. Steganography is in many cases becoming a substitute to cryptography because regardless of the complexity, any cryptography algorithm can be broken once it becomes evident that there is some encryption of data, while Steganography does not invite attacks because ideally there is no can be seen.

1.5 Limitation

Limitations in this research are:

- 1- The limited availability of benchmark RGBA images.

- 2- The extra storage needed for the alpha channel.

1.6 Methodology

1. Studying of techniques and models in LSB based Steganography with reference to the concepts of an indicator or selector, as a guide for selection of storage locations for message bits.
2. Designing Steganography procedures to store message bits in alpha channel using the RGBA channels as indicator.
3. Implement the proposed procedures as modules in Matlab.
4. Analyze standard images using the implemented Matlab modules.
5. Evaluating results of both methods.
6. Discuss results and give conclusions and the recommendation for future work.

1.7 Thesis Layout

The thesis consists of seven chapters: the current one is the introduction to the general view of steganography and, presents problem definition, objectives, motivation, significance and solution approach of the problem and the goal of the thesis. Chapter two presents the terminology and basic concept of steganography. Chapter three is an overview of the literature survey and the related works. Chapter four views the steganography evaluation criteria. Chapter five presents the proposed alpha channel based steganography method and the structure of the model which consist of two stages: the embedding process, and extracting process. Chapter six presents the experimental work and discussion of results. Chapter seven presents the conclusion, and future Works.

Chapter Two

Terminology and Basic Concepts of Steganography

2.1 Steganography

Steganography linguistically means secret writing since the word “Steganography” is originally made up of two Greek words steganos (secret) and graphy (writing). Practically, it means the art and science of hiding or camouflaging secret data in an innocent looking dummy container in such a way that the existence of the embedded data is imperceptible and undetectable (Bailey, et al., 2004).

Steganography is the process of hiding secret data within public information. Secret data can be a plaintext or cipher text, or any kind of data that can be hidden in digital media. Since all kinds of secret data must be translated into binary, we always hide binary data whatever this secret data or file is.

Steganography considered as a multidisciplinary field since it combines digital signal and data compression methods, information theory, signal coding theory, digital communication theory, digital signal processing, cryptography and the theory of human visual perception, all employed to satisfy the needs of information security (Cole, 2003)

2.2 Steganography Categories According Carrier Types

The carrier is the signal, stream, or data file into which the hidden data is hidden by making modifications. Such as image files, documents, video files, audio files, and protocol as shown in figure 2.1. The carrier should look and work the same as the original unmodified carrier, and should appear normal to anyone inspecting it. File formats with a

high degree of redundancy is preferable since redundant bits can be replaced with secret information without the embedded information being perceivable.

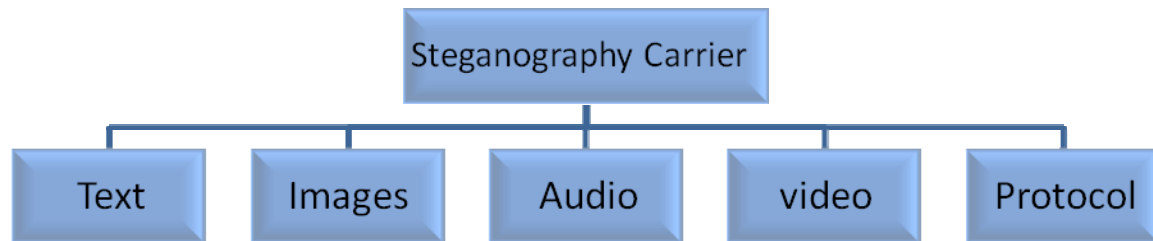


Figure 2.1: Steganography Categories According Carrier Types

2.2.1 Text Steganography.

Steganography can be used in text documents by adding white spaces in the end of lines of a document. This type of Steganography is effective because the white space occurs naturally and it's not visible to the human eye at all in most of text document editors. When using this Steganography technique there is no way to suspected if there is any hidden data (Morkel, et al., 2005).

2.2.2 Image Steganography.

Usually the Least Significant Byte (LSB) is used when hiding information inside images. Image file simply is a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside of is images have a high quality, resolution and their size such as 24 Bit BMP (Bitmap) image which is the largest type of file. So this type is easier to hide and mask information inside it. It is important to remember that the hidden information will be lost if the stego-file then converted to another image format (Morkel, et al., 2005).

2.2.3 Audio Steganography.

There are many techniques used in audio steganography when we need to hide information inside audio file; the technique usually used in hiding information inside Audio files is low bit encoding which is similar to LSB in image files. Using the low bit encoding is a risky method because it is usually noticeable to the human ear. Another method used to hide information inside of an audio file is Spread Spectrum, this method works by adding random noises to the signal, the information spread across the frequency spectrum of the audio file. Another method of hiding information inside an audio file is Echo data hiding. This method hides information by simply adding extra sound to an echo inside an audio file, this method better than other methods of hiding information audio files because it can actually improve the sound of the audio inside an audio file (Morkel, et al., 2005).

2.2.4 Video Steganography.

Usually when hide information inside the video the DCT (Discrete Cosine Transform) method used. DCT works by make inconsiderable changing on each of the images in the video, so it's not noticeable by the human eye. The DTC change the values in certain parts in the picture, where the number of rounds the greatest integer, for example, if the value is 4.578 become 5. Steganography in Videos is similar to that of Steganography in Images, a part of information is hidden in each frame of video, while a small amount of information is hidden inside of video, the hidden information not noticeable, as known whenever the information that is hidden increased, the change will be become more noticeable (Morkel, et al., 2005).

2.2.5 Protocol Steganography

The term protocol Steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where Steganography can be used (Chang & Tseng, 2004)

2.3 Steganography Process

Steganography process as shown in figure 2.2 has the following components:

1. **Secret message:** The data to be hidden which can be in the format of text, audio, video, or image.
2. **Cover –Media :** It refers to the object used as the carrier to embed the secret message inside it.
3. **Embedding Algorithm:** Known as hiding message procedure.
4. **Extracting Algorithm:** Known as unhide/uncover the message procedure.
5. **Stego-media (image):** Refers to the generated object, which is carrying a hidden message.



Figure 2.2: The Steganography Process

2.4 Uses of Steganography

Steganography is used by the two sides of society, good people and bad people. It is known that criminals use several kinds of steganography to smuggle documents and instructions to their partners, hoping to avoid the law. Dealing with this unlawful use

of steganography is the research core of Steganalysis. The good people Steganalysis to protect secrets and confidential documents for example it is used by government departments, banks, commercial entities as well as individuals who want to protect their data.

2.5 Steganography algorithms

1. Spatial domain

In this algorithm the image format is represented as a rectangular grid of pixels. The human visual system (eye), does not perceive an image as a grid. (Fridrich, 2010)

2. Transform domain.

This algorithm focuses on representing images that are easy to compress. Such techniques are normally lossy and thus form an approximation of the original image with some loss of detail. (Fridrich, 2010)

2.6 Security services offered by Steganography

Steganography ensures the privacy of sensitive information by hiding information in other information, thus confidentiality is offered. Identification and authentication can only be offered if a steganographic key is used, since knowledge of the key can identify a person to be who he says he is. However, the manner in which the information is hidden and the techniques used could also serve as proof of identity. The technique used to embed the information thus becomes the shared secret, and when correctly embedded and extracted provides a means of identification and authentication by Steganography.

2.7 Steganography problems

Steganography can be misused by keeping secrets that could be harmful to innocent people. The biggest concern in the field of steganography is the rapid advancement of research in Steganalysis, the counter-technology of Steganography (Wang & Wang, 2004).

Due to the increase importance of copyright protection, the watermarking technique has many researchers attention. The computer specialists and security researchers have recognized that the Illegal use of steganography might become a threat to the security of the worldwide information infrastructure. Steganography could allow terrorists to communicate in secret without law enforcement having knowledge of this communication. Because of this threat, researchers have been succeeding to find flaws in existing steganography systems. These flaws are exploited for the detection of hidden information, and also include the extraction and destruction of the hidden data. (Kovacich & Jones, 2002)

2.8 Steganography Types

2.8.1 Pure Steganography

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all. (Ashok, 2010)

2.8.2 Secret Key Steganography

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message (Hamid et al., 2010).

2.8.3 Public Key Steganography

Public Key Steganography takes the concepts from Public Key Cryptography as explained below. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message (Hamid et al., 2010).

2.9 Steganographic Techniques

Over the past few years, numerous Steganography techniques that embed hidden messages in multimedia objects have been proposed (Johnson & Jajodi, 1998). There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include:

2.9.1 Least significant bit insertion (LSB)

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. (Muhaimin, et al., 2003)

The data or hide a secret message in the least significant bits cannot be feeling up by humans, so making it a perfect place to hide the data, without any change in the cover object, In this method is replaced the least significant bits of some or all of the bytes inside an image with a bits of the secret message (Katzenbeisser & Petitcolas, 2000).

2.9.2 Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level. (Robert, 2004)

2.9.3 Transform techniques

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants. (Muhaim, et al., 2003)

Chapter Three

Literature Survey

3.1 Introduction

With the tremendous development in technology in recent years proposed several methods of hiding data or information within the image So as to increase protection and data encryption and work on this data does not detect and protect it from penetration or accessed These methods were used to hide data in each pixel in the image, which contains the color scheme is known (RGB), according to every principle of each algorithm used in the distribution of the data or hide the data.

3.2 Information Hiding

Information hiding science considers a wide research area, which involves many applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography: (Isbell, 2002).

1. Watermarking applications usually applied for copyright protection. In this application the message contains information such as owner identification and a digital time stamp.
2. Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user.
3. Steganography hides the secret message within another data set, which means Conceal the existence of the message.

3.3 Information Hiding Techniques

There are three different approaches that can be used to hide information in a cover object: injection, substitution and generation. (Rajanikanth, 2009)

3.3.1 Injection

In injection technique the information can be hidden in a section of a file which will be ignored by the processing application. For example, we can add additional bytes in an executable file; those bytes don't affect the process. The end-user may not realize that the file contains additional hidden information. However, using an insertion technique changes file size according to the amount of hidden information, if the file size increased too much may arouse suspicion. (Mastronardi & Castellano, 2003)

3.3.2 Substitution

Substitution technique is used to replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion. The main advantage of this technique is that the cover file size does not change after the execution of the algorithm. On the other hand, this approach has at least two drawbacks. First, the resulting stego object may be adversely affected by quality degradation—and that may arouse suspicion. Second, substitution limits the amount of data that you can hide to the number of insignificant bits in the file (Fridrich, 2010).

3.3.3 Generation

Unlike injection and substitution, generation techniques do not require an existing cover file. This technique generates a cover file for the sole purpose of hiding the

message. The main flaw of the insertion and substitution techniques is that people can compare the stego object with any pre-existing copy of the cover object (which is supposed to be the same object) and discover differences between the two. We will not have that problem when using a generation approach, because the result is an original file, and is therefore immune to comparison tests. (Shirali-Shahreza & Shirali-Shahreza, 2008)

3.4 Cover Image Formats

There are various format types of image files that can be used for cover images, the main types that are of interest in this research are the following:

1. TIFF (Tagged Image File Format)

In 1986 by an industry committee chaired by the Aldus Corporation the TIFF format was created. The TIFF handles monochrome; gray scale, 8-and 24-bit color, TIFF files can be saved in a variety of color formats and in various forms of compression. Most graphics programs that use TIFF do not compression consequently file sizes are quite big.

2. BMP (Microsoft Windows Bitmap).

It was developed by Microsoft Corporation, BMP stands for bitmap or bump file, It may contain images with 1, 4, 8, or 24 bits per pixel, and is stored by scan line, bottom to top (which causes much aggravation, as almost all graphics formats store data from the top to bottom).

3. PNG (Portable Network Graphic)

PNG stands for Portable Network Graphics, was created as a more powerful alternative to the GIF file format, The PNG format supports an alpha channel, or the

"RGBA" color space. The alpha channel is added to the three standard color channels (red, green, and blue, or RGB) the PNG is saved with 256 colors maximum but it saves the color information more efficiently. It also supports an 8 bit transparency.

3.5 RGBA Color image

The most used image format contains three channels Red, Green, and Blue. Each color (channel) stored in one byte with value from 0... to 255. In 32-bit representation of graphic images, there are four channels of 8 bits as shown in figure 3.1, three color channels Red, Green, and Blue (RGB), and the fourth channel called the alpha channel. The alpha channel specifies how the pixel's colors should be merging with another pixel when the two overlaid and control the transparency or opacity of an image.

RGBA extends the RGB color model with the alpha value. Alpha channel was invented by "Catmull" and "Smithin" in 1971 (Alvy, 1995). The alpha channel used as an opacity channel; where it value varies from 0 to 255, which 0 means completely transparent while 255 means opaque. Not all RGB images contain an alpha value. If RGB images are used to hide the information, it can lead to suspicion because the default value of the alpha in the RGB images is 255. In RGBA images alpha value is not same in all the pixels of the image. Therefore the proposed technique gives much better results if RGBA images are used.

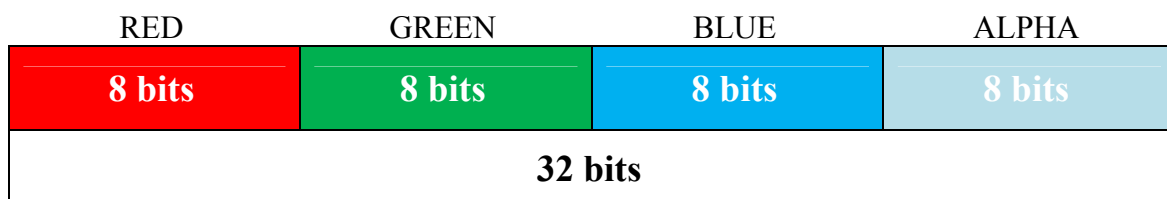


Figure 3.1: RGBA Image channels.

3.6 Alpha channel

ARGB (Alpha, Red, Green, and Blue) consists of Represents true color images in three channels (bytes) in addition to transparency channel taking one byte (Alvy, 1995).

In computer graphics, alpha compositing is the technique of mixing an image with a background to create the appearance of the partial transparency. This process is useful to render images in separate passes and then combine them into a final image.

On each pixel's in image there is portion of data that is reserved for transparency information which controls the transparency and opacity in an image, this value called alpha channel, where 0 represents full transparency to 255 which represents full opacity, the values can be represented as show in Table 3.1, the low value of alpha is full transparency and the high value is full opacity:

Table 3.1: Alpha value representation

Value representation	Full transparency	Full opacity
real value	0.0	1.0
Percentage	0%	100%
Integer	0	255

3.7 Related work

There are many research have been done in the field of handwritten characters recognition. In the following subsections some of researches are most related to this thesis. These researches use different methods and techniques.

3.7.1 RGB image based Steganography.

(Gutub & Mohammad, 2008) proposed a new algorithm for RGB image based Steganography. The algorithm introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. The algorithm offers very high capacity for cover media compared to other existing algorithms.

3.7.2 Spatial domain based on RGB image

The algorithm is invented by (Gutub, 2010) 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 nits of the channel from red, Green and Blue as an indicator for existence of data in the other two channel. The indicator channels are chosen in sequence. With Red being the first in the first pixel 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. As seen in Table 3.2.

Table 3.2: The indicator relation with the hidden data and the other two channels
(Ghosal, 2011).

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

3.7.3 Using the two least significant bits as indicator of one channel.

(Gutub, 2010) has proposed a new improved technique that takes advantage of the 24 bits in each pixel in the RGB images using the two least significant bits of one channel to indicate existence of data in the other two channels. The stego method does not depend on a separate key to take out the key management overhead. Instead, it is using the size of the secret data as selection criteria for the first indicator channel to insert security randomness.

3.7.4 Calculating the number of ones and zeroes in the red channel.

(Ghosal, 2011) proposed a steganographic method works by considering the three channels (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 once 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.

3.7.5 Hiding data directly in a special domain

Seidan (2013) 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 have embedded in the right part are counted in the left part of the channel which chosen for embedding.

The proposed 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. The algorithm has been compared with other known algorithms as (Ghosal, 2011) and (Gutub & Mohammad, 2008), the results proved the power of the new algorithm to hide and extract data.

Chapter Four

Steganography Evaluation Criteria

4.1 Steganography Evaluation Criteria

Steganography styles and techniques can evaluate using various features and factors. Has been developed five factors Steganography evaluation scheme, the “Magic Hexagon Image Steganography Evaluator”, which included the following criteria: Capacity, Perception (Visibility), Robustness, Delectability and Dependency (Lakshari, et al., 2012).

4.1.1 Capacity

The amount of information that is embedded should be as small as possible. Logic suggests that the longer the message, the more the image has to be altered to compensate for this. Obviously, the more a Work is modified, the easier it is for the steganalyst to discover art effects within an image. Therefore, the usual practice for embedding is to make the message as short as possible so that the image is altered as little as possible. (Hamid, et al., 2009)

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system. (Hamid, et al., 2010)

4.1.2 Robustness

Robustness refers to the ability of the embedded data to remain intact if the stego-system undergoes transformation, such as linear and non-linear filtering; addition of random noise; and scaling, rotation, and loose compression (Elnajjar, et al., 2010)

4.1.3 Undetectable

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For example, if a Steganography method uses the noise component of digital images to embed a secret message, it should do so while not making statistical changes to the noise in the carrier. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image. (Hamid, et al., 2010)

4.1.4 Invisibility (Perceptual Transparency)

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover (Hamid, et al., 2010)

4.1.5 Security

The embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key. (Naji, et al., 2009)

4.2 Steganalysis Attacks

Steganalysis is a technique for detection or destruction of the hidden information in the cover media files. The objective of Steganalysis is to discover hidden information and to break the security of its carriers. Steganalysis methods should be used by the Steganographic in order to determine whether a message is secure and accordingly

whether a Steganographic process has been successful (Grover, 1998). There are three types of Steganalysis attacks:

- 1. Visual attacks.** They consist of stripping away the significant parts of a digital content in order to facilitate a human's visual inspection for anomalies (Wayner, 2002).
- 2. Structural attacks.** Sometimes, the format of the digital file changes as hidden information is embedded. Often, these changes lead to an easily detectable pattern in the structure of the file format. For instance, it is not advisable to hide messages in images stored in GIF format. In such a format an image's visual structure exists to some degree in all of an image's bit layers due to the color indexing that represents 224 colors using only 256 values (Westfeld & Pfitzmann, 1999).
- 3. Statistical attacks.** Digital pictures of natural scenes have distinct statistical behavior. With proper statistical analysis, we can determine whether or not an image has been altered, making forgeries mathematically detectable (Mercuri, 2004).

Steganalysis involves two major techniques: visual analysis and statistical analysis. Visual analysis tries to reveal the presence of hidden data through inspection, either with the naked eye (or ear in the case of sound) or with the assistance of a computer. Statistical analysis, on the other hand, attempts to reveal tiny alterations in a carrier objects " statistical characteristics caused by steganographic embedding (Wang & Wang, 2004).

4.3 Attacks to Steganographic Systems

A Steganalysis "attack" represents the technique with which the steganalyst attempts to recover, modify, or remove a stego message. There exist five Steganalysis attacks which are incidentally known message, chosen stego, and chosen message. In the

stego only method the steganalyst only has available the stego medium or the finished stego product. This is by far the most difficult attack approach since there is no starting point from which to start extracting the hidden message. Attacks can be broadly categorized although some attacks will fit into multiple categories (Cummins, et al., 2004) (Brainos, 2000):

1. Basic Attacks

Basic attacks take advantage of limitations in the design of the embedding techniques. Simple spread spectrum techniques, for example, are able to survive amplitude distortion and noise addition but are vulnerable to timing errors. It is possible to alter the length of a piece of audio without changing the pitch and this can also be an effective attack on audio files.

2. Robustness Attacks

Robustness attacks attempt to diminish or remove the presence of a watermark. Although most techniques can survive a variety of transformations, compression, noise addition, etc, they do not cope so easily with combinations of them or with random geometric distortions.

3. Presentation Attacks

Presentation attacks modify the content of the file in order to prevent the detection of the watermark.

4. Interpretation Attacks

Interpretation attacks involve finding a situation in which the assertion of ownership is prevented. Robustness is usually used to refer to the ability of the mark to survive

transformations and not resistance to an algorithmic attack. Therefore the definition of robustness may not be sufficient.

4.4 Full-reference Metrics (FR)

PSNR and MSE are the most common and widely-used full-reference (FR) metrics for objective image quality evaluation. Furthermore, PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods (Wayner, 2002).

4.4.1 Peak Signal to Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) (Curran, et al., 2010) is a standard performance measurement which can evaluate the distortion in an image to determine if the distortion is within the range for natural noise in images or it is the case of a an altered (stego) image. The PNSR is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right)$$

The PSNR measures the similarity between two images (how two images are close to each other), while the MSE measures the difference between these two images. Since the computing of these two metrics is very easy and fast, they are widely-used and very popular (Wang, et al., 2003)

4.4.2 Mean Square Error (MSE)

The MSE is the statistical difference in the pixel values between the original and the reconstructed image. (Stoica, et al., 2003)

The MSE is defined as:

$$MSE = \frac{1}{m n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

Where,

I represents the matrix data of our original image

K represents the matrix data of our degraded image in question.

m represents the numbers of rows of pixels of the images and **i** represents the index of that row.

n represents the number of columns of pixels of the image and **j** represents the index of that column.

Chapter five

The proposed alpha based steganography method

5.1 The proposed algorithm

The suggested research will consider the use of the alpha channel in combination with the Red, Green and Blue color channels for the storage of bits of the secret message.

The RGB channels will be used as an indicator for selection of the number of bits to store in the alpha channel of each pixel. There will be no change so to stored values of RGBA channels, there value remain un-altered.

For more security in the transmission the of the generated stego image, the proposed method uses a novel approach in which the alpha channel of the stego image is swapped with the alpha channel of another, un-related image. The sending party sends a different image with the alpha channel containing the secret message, this image is referred to in this work as "semi-stego". The receiving party cannot view the message or decrypt the image if he does not have the first image that was separated from its alpha channel. The receiving party has to have available a copy of the un-altered original image, in order to carry out a reverse swap, in which the original cover and the alpha containing the secret message are re-merged, after that the process of message extraction can proceed.

5.1.1 Embedding process

Embedding algorithm is the algorithm used to embed information in cover media as shown in figure 5.1, the algorithm described in next section.

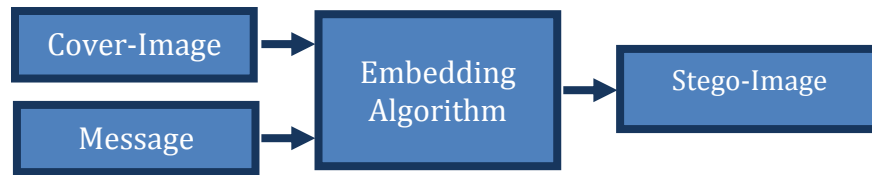


Figure 5.1: embedding process

Embedding Algorithm

Input:

- Cover image file (image formats that support Alpha transparency).
- Secret message file (not necessarily text format).

Output:

- Stego image file, will be converted to PNG) in 32 bit RGBA format.

Processing:

- **Read** Cover file into Stego array
- **Open** Secret file
- **Read** and store secret file as bits into BinaryMessageArray
- Remaining Bits = Size of BinaryMessageArray

Next_bit = 0

While Next_bit < RemainingBits

- Move to next pixel of Stego array
- $RGB_Sum = R + G + B$
- $Indicator = \text{Mod}(RGB_Sum, 3)$

Switch (Indicator)**Case 0:**

- Get 2 bits from BinaryMessageArray and store in Alpha LSB of the current pixel.
- $\text{Next_bit} = \text{Next_bit} + 2$

Case 1:

- Get next 3 bits from BinaryMessageArray and store in Alpha 2 LSB's of the current pixel.
- $\text{Next_bit} = \text{Next_bit} + 3$

Case 2

- Get next 4 bits from BinaryMessageArray and store in Alpha 3 LSB's of the current pixel
- $\text{Next_bit} = \text{Next_bit} + 4$

End Switch**End While**

- **Save** Stego array to Stego file

End of Embed Algorithm

Figure 5.2 shows the processes of embedding message in the Alpha channel using the RGB channels as an indicator. The text documents to be hidden will be in ASCII or UNICODE, and multi-lingual (English – ARABIC).

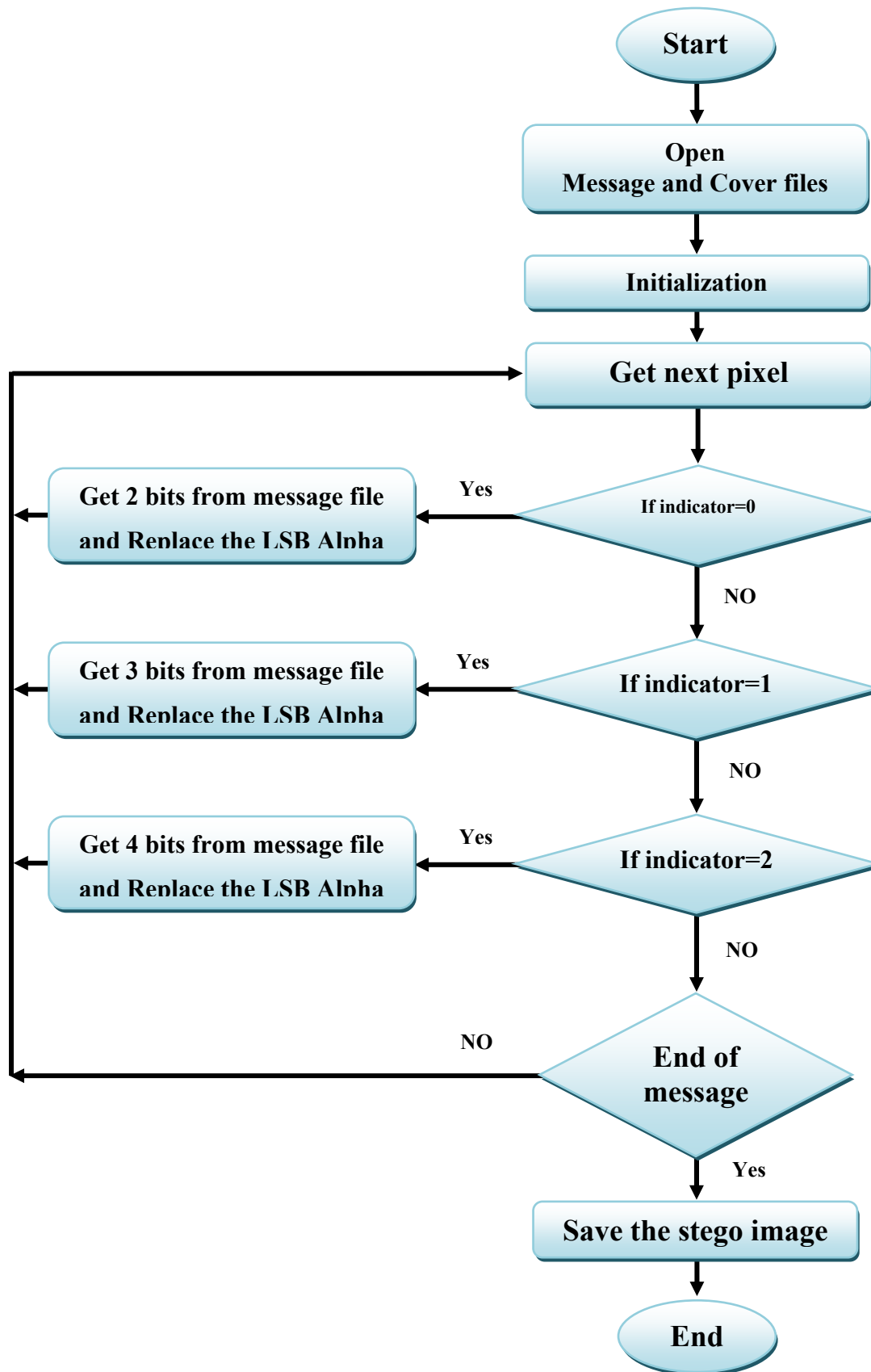


Figure 5.2: proposed Embedding Message Model

5.1.2 Extracting process

Extraction algorithm is the algorithm used to extract the information from the stego media as shown in figure 5.3, the algorithm described in next section.



Figure 5.3: Extracting process

Extracting Algorithm

Input:

- Stego image with Alpha file, in 32 bit RGBA format.

Output:

- Recovered Secret file

Processing:

- **Open** Stego file
- **Get** Stego Size
- **Get** Secretmessage size in bytes(stored in the stego file)

Next_bit = 0

// Initialize array

- Recovered_bits = empty

While Next_bit < SecretBitsCount

 Move to next pixel

 RGB_Sum = R + G + B

 Indicator = Mod (RGB_Sum, 3)

Switch (Indicator)**Case 0:**

- Get 2bits from Alpha LSB and append to Recovered_bits array
- $\text{Next_bit} = \text{Next_bit} + 2$

Case 1:

- Get 3 bits from Alpha LSB and append to Recovered_bits array
- $\text{Next_bit} = \text{Next_bit} + 3$

Case 2:

- Get 4 bits from Alpha LSB and append to Recovered_bits array
- $\text{Next_bit} = \text{Next_bit} + 4$

End Switch**End While**

- **Convert** Recovered bits array to Recovered bytes array
- **Open** Recovered Secret file as text file for output
- **Save** Recovered bytes array to Recovered Secret file

End of Extract Algorithm

Figure 5.4 shows the processes of **extracting** message from stego-image.

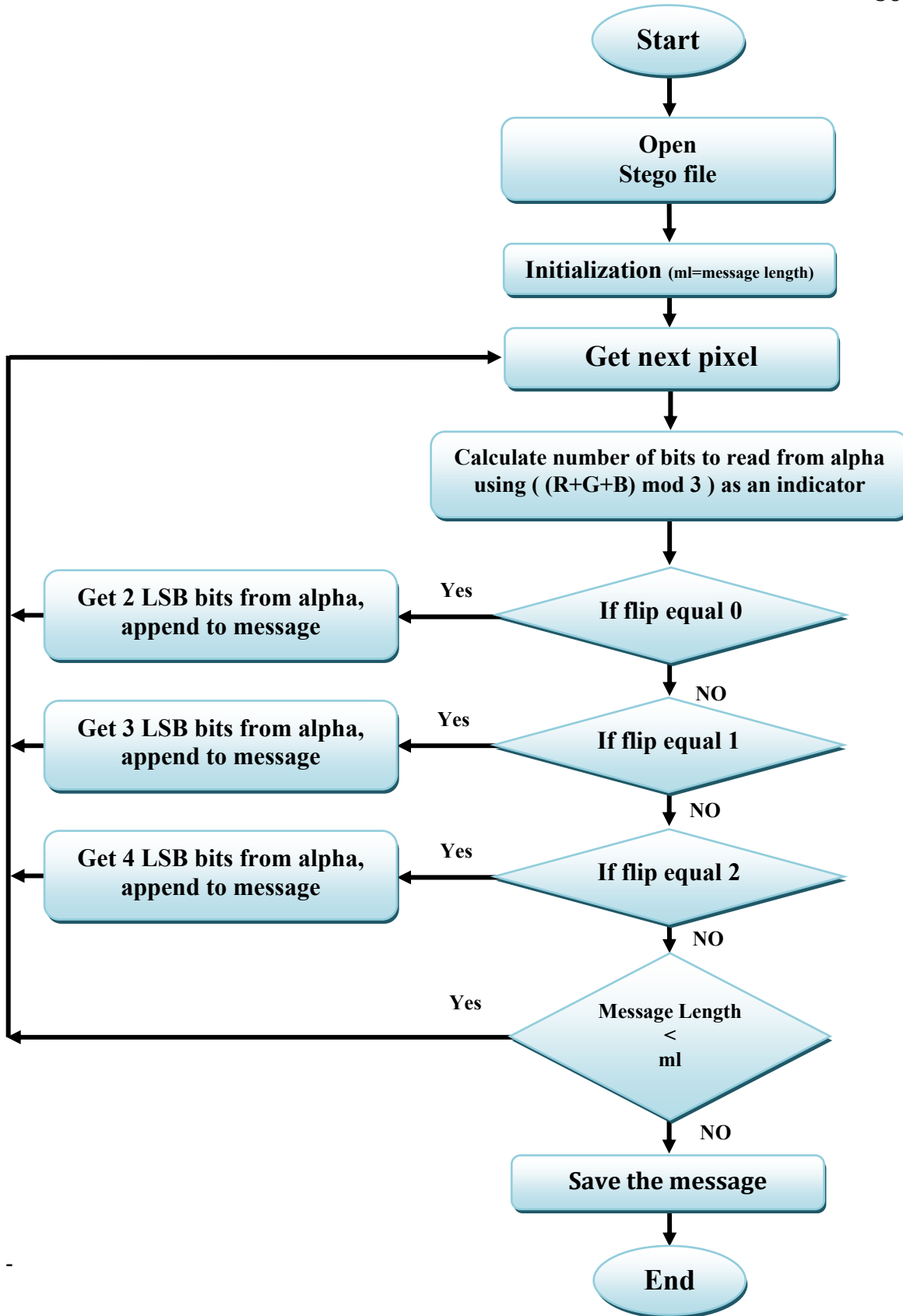


Figure 5.4:proposed Extracting model

Chapter six

Experimental work and Discussion of results

6.1 Implementation

The proposed Steganography algorithm was implemented using MATLAB Version R2013a for RGBA images were taken as input. The proposed algorithm was tested on images that contain alpha channel from various categories such as human, birds, animals... etc, in various sizes.

6.2 Image selection

The image that used as a cover image should be large enough to hide the message in it. A 32-bit image should be used.

6.3 Embedding processes

In embedding processes the inputs are 32-bit cover image, and a secret message (text file). The output is Stego image with hidden data.

6.3.1 Load cover image

In this step the input is a 32 bits image, we need to load cover image from the computer files as shown in figure 6.1.

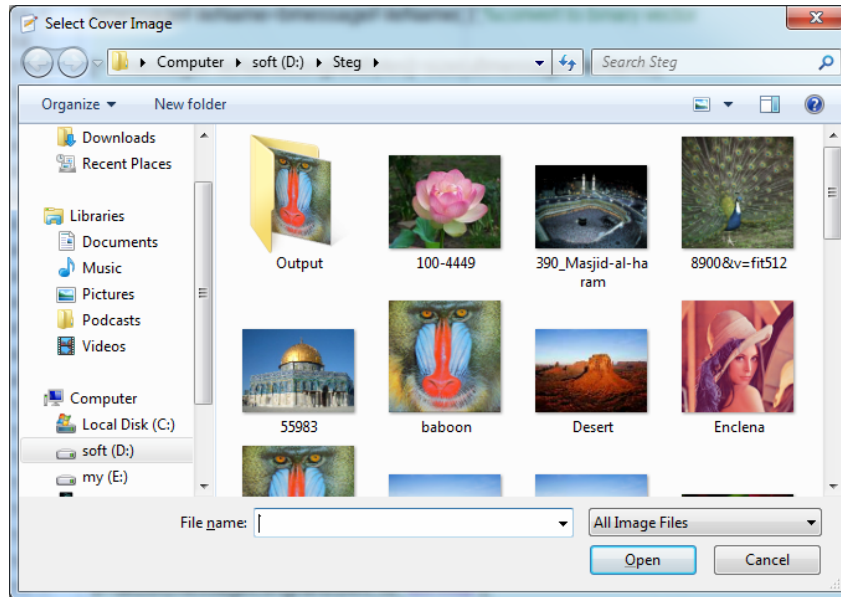


Figure 6.1: load cover image.

6.3.2 Load text message

Figure 6.2 shows the window of choosing the text file that contains information to be embedded in cover image.

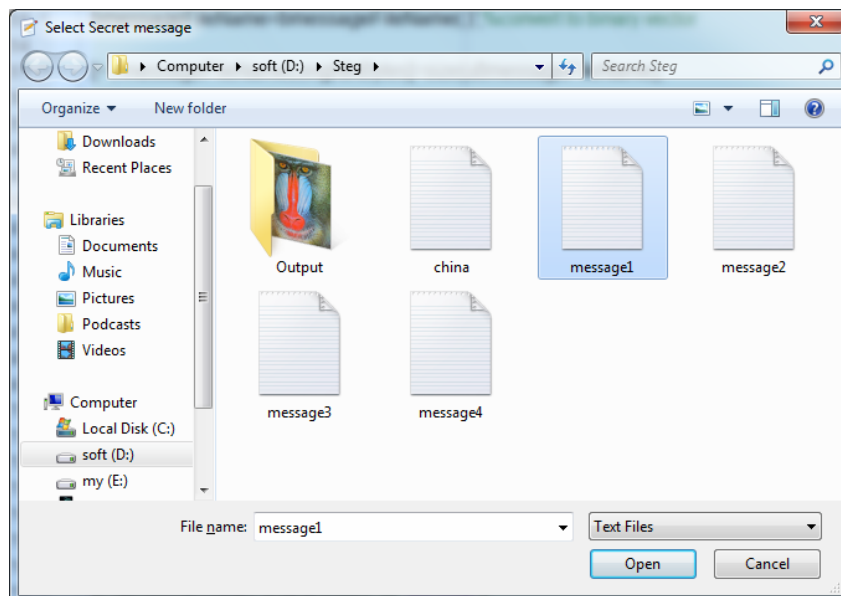


Figure 6.2: choosing text file.

6.3.3 Save stego image

Figure 6.3 shows the window of saving the stego image after embedding the text.

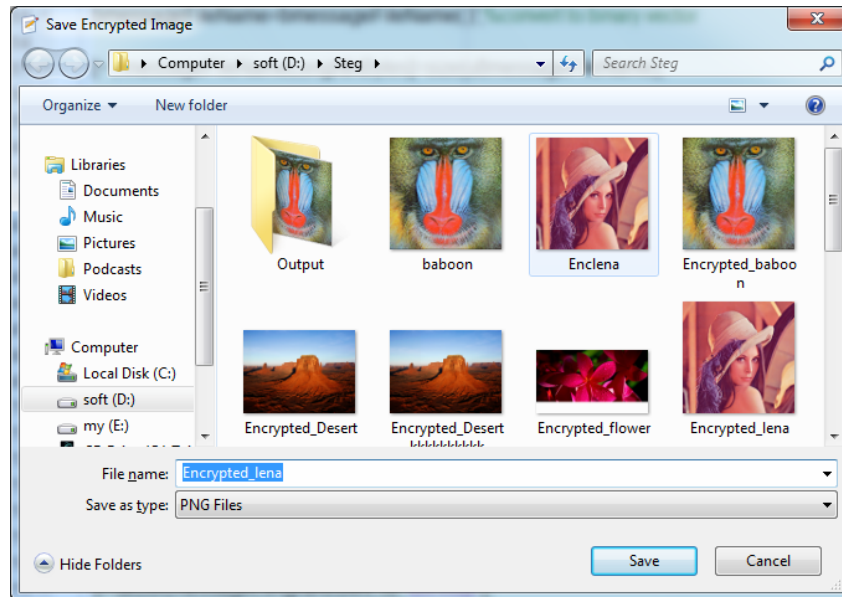


Figure 6.3: saving stego image.

6.4 Extracting processes

In extracting processes the inputs is stego image. The output is text file contain the secret message.

6.4.1 Load stego image

Figure 6.4 shows the window of loading the stego image that contains the secret message.

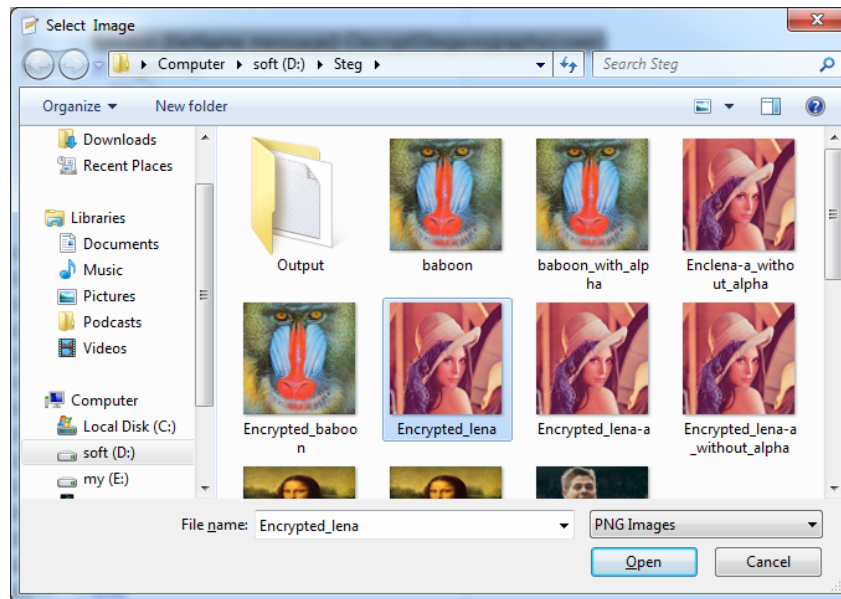
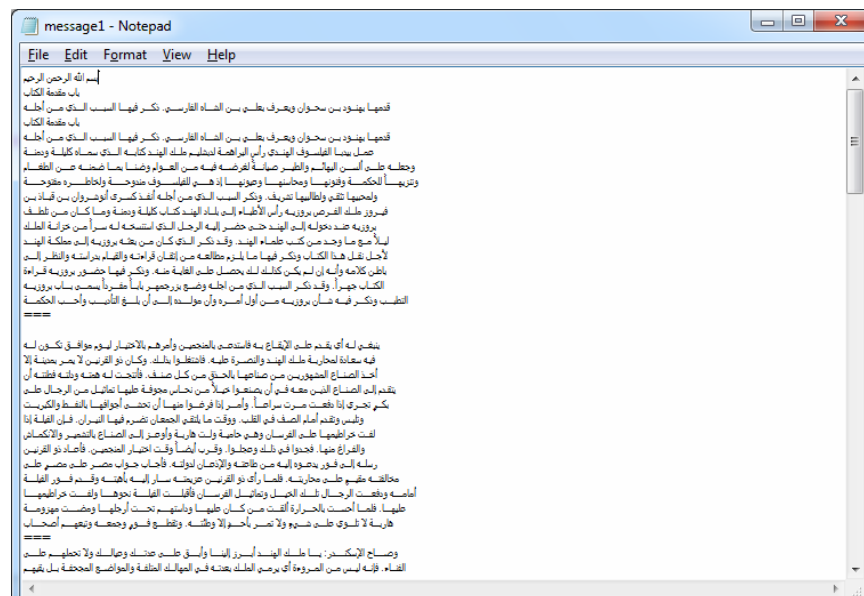


Figure 6.4: choosing stego image.

6.4.2 Save extracted message

Figure 6.5 shows the window of text file after extracting the information, where the text file will be saved in the directory named output.







6.5 Discussion of results

6.5.1 Proposed algorithm Vs Ghosal algorithm (Ghosal, 2011)

The results of proposed algorithm compared with the results of Ghosal algorithm on five cover images as shown in table 6.1.

Table 6.1: Proposed algorithm Vs Ghosal algorithm

Cover image	image Size	Ghosal Algorithm PNSR	Proposed Algorithm PNSR
Cartoon5 	1024*1024	48.06	57.9480
Animal 2 	1024*1024	56.68	57.9169
Animal 10 	1024*1024	56.92	54.6976
Football5 	1024*1024	46.14	54.9168

6.5.2 Proposed algorithm Cover image Vs Stego image

The table 6.2 shows Evaluation criteria for four images, the message was embedded with size 14.8 Kb.

Table 6.2: Evaluation criteria for four images

Image name	Image size	Evaluation criteria	
		PNSR	MSE
Baboon	512 X 512	53.8179	0.2700
Flower	1920 X 1080	61.2563	0.0487
Horse	512 X 512	53.9446	0.2622
Lenna	512 X 512	54.0423	0.2564

Figure 6.6 shows the picture of baboon of size 512 X 512 before and after using the proposed algorithm.

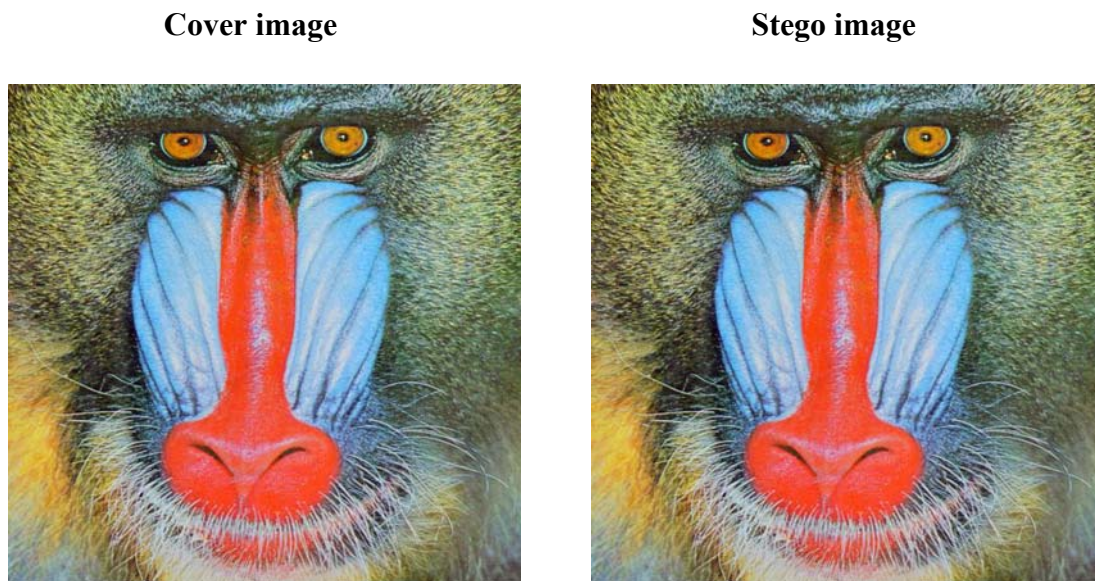


Figure 6.6: cover and stego images of baboon.

Figure 6.7 shows the picture of flower of size 1920 X 1080 before and after using the proposed algorithm.

Cover image



Stego image



Figure 6.7: cover and stego images of flower

Figure 6.8 shows the picture of horse of size 512 X 512 before and after using the proposed algorithm.

Cover image



Stego image



Figure 6.8: cover and stego images of horse

Figure 6.9 shows the picture of lenna of size 512 X 512 before and after using the proposed algorithm.



Figure 6.9: cover and stego images of lenna

6.5.3 Histogram analysis

Figure 6.10 shows that there is no visual affect on the values of RGB channels for the Baboon image.

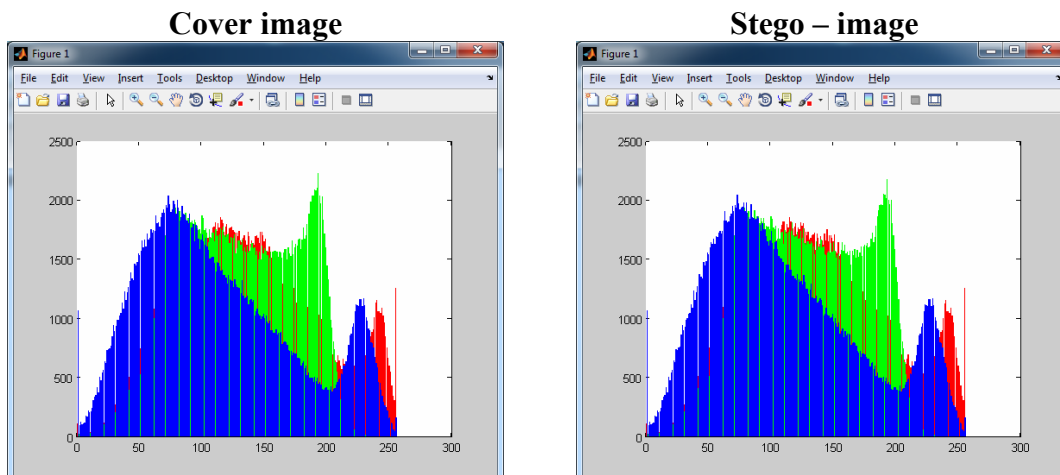
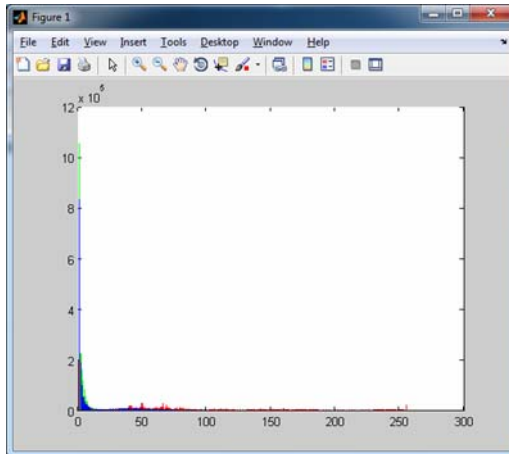


Figure 6.10: Histogram analysis, Baboon image 512 X 512

Figure 6.11 shows that there is no visual affect on the values of RGB channels for the flower image.

Cover image



Stego – image

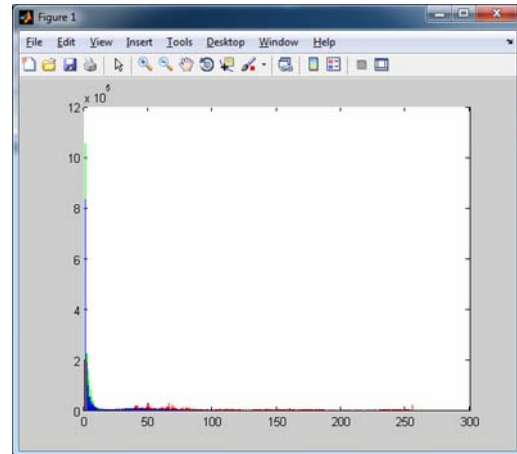
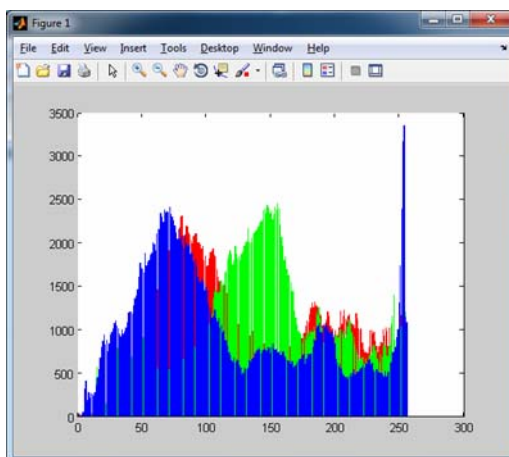


Figure 6.11: Histogram analysis, Flower image 1920 X 1080

Figure 6.12 shows that there is no visual affect on the values of RGB channels for the horse image.

Cover image



Stego – image

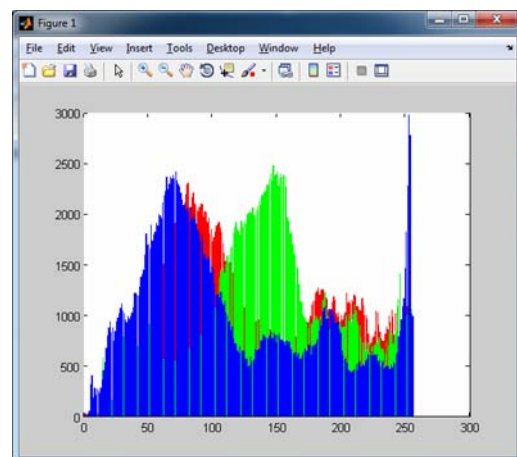


Figure 6.12: Histogram analysis, Horse image 512 X 512

Figure 6.13 shows that there is no visual affect on the values of RGB channels for the lenna image.

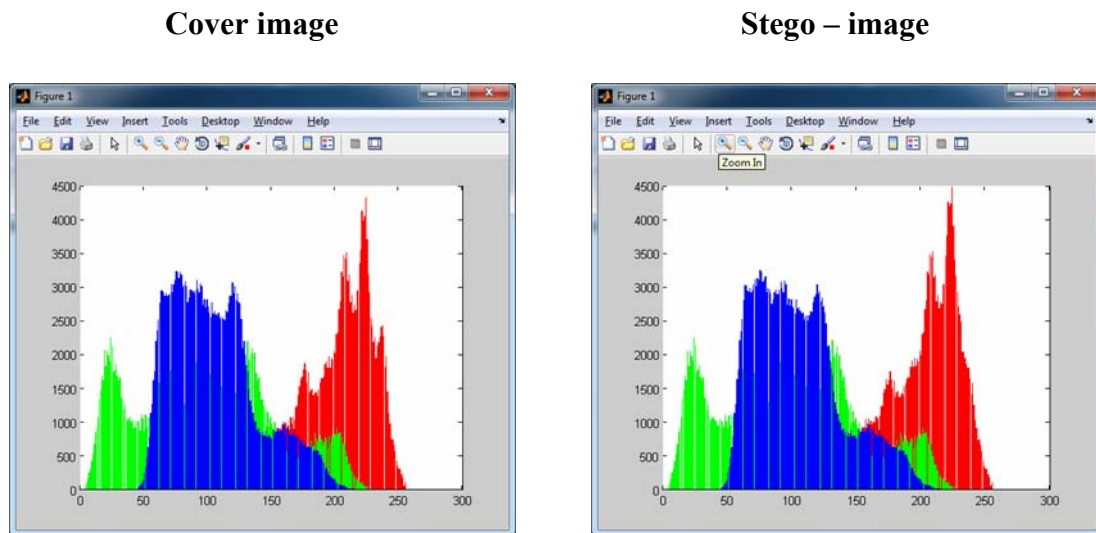


Figure 6.13: Histogram analysis, Lenna image 512 X 512

6.6 Example for sending and receiving a message

The sending party must have a secret message, cover image with alpha, and alternate image without alpha. The receiving party must have a cover image. The cover image and semi-stego image shown in figure 6.14 and figure 6.15.



Figure 6.14: cover image.



Figure 6.15: semi-stego image.

The sending party steps to send a stego image:

Step 1: load a cover image

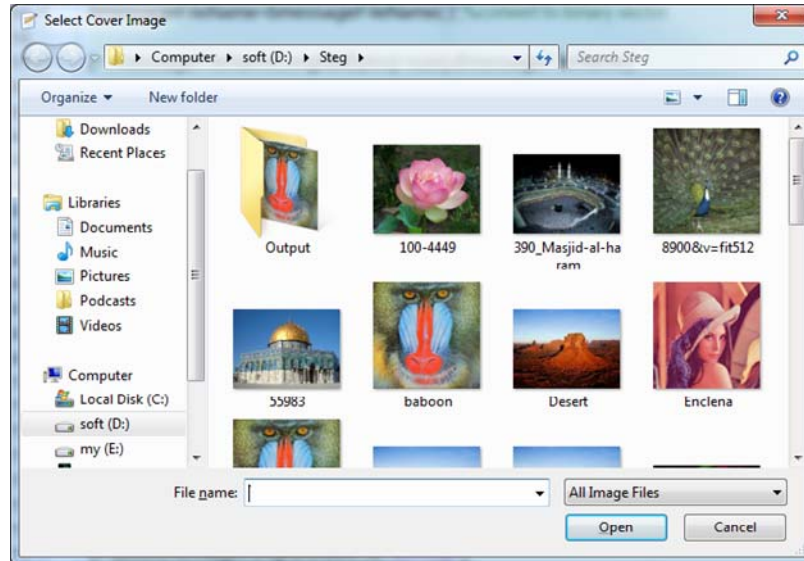


Figure 6.16: load cover image

Step 2: load secret message

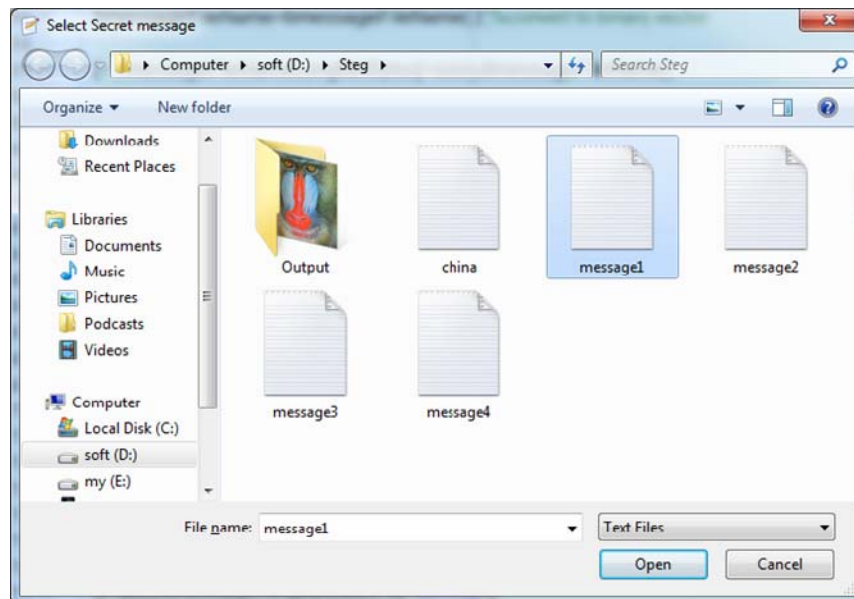


Figure 6.17: load secret message

Step 3: save stego image

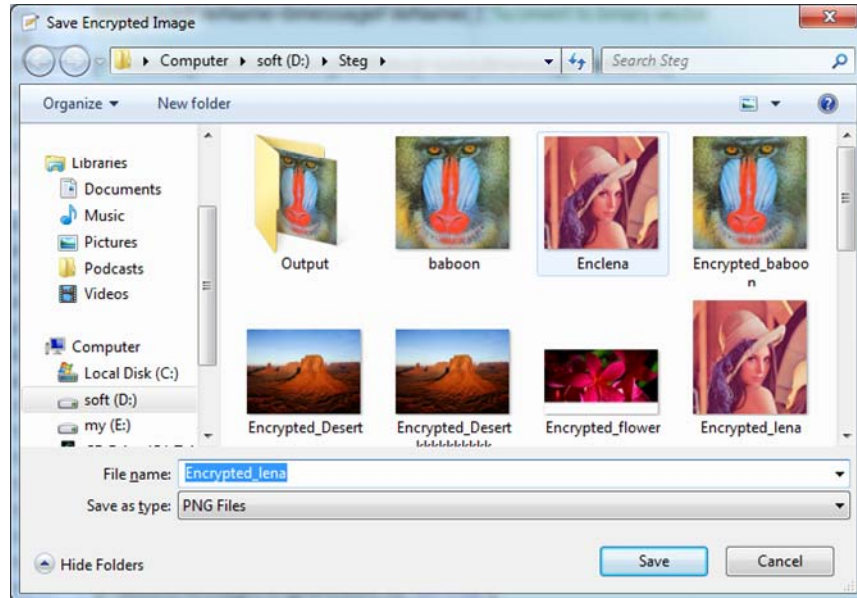


Figure 6.18: save stego image

Step 4: Swapping alpha

Load the stego image

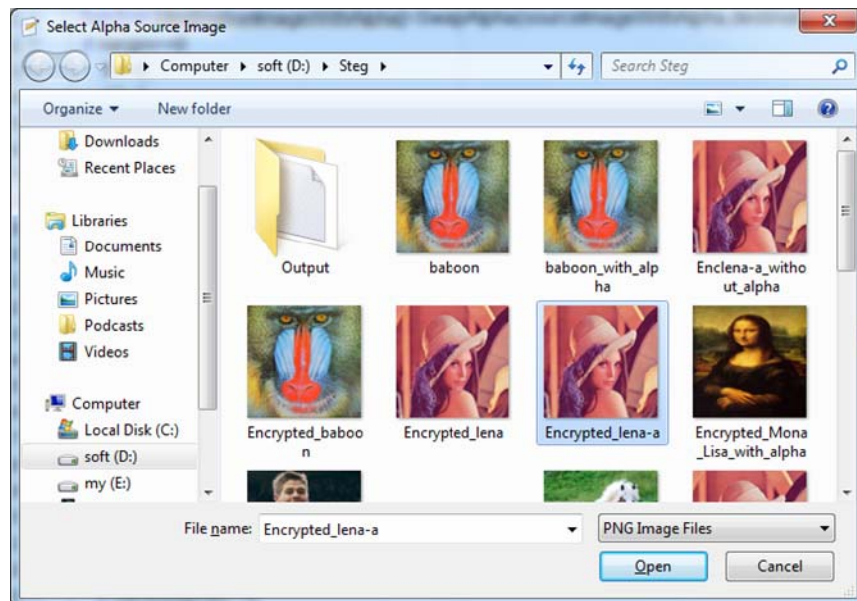


Figure 6.19: load stego image

Choose semi-stego image

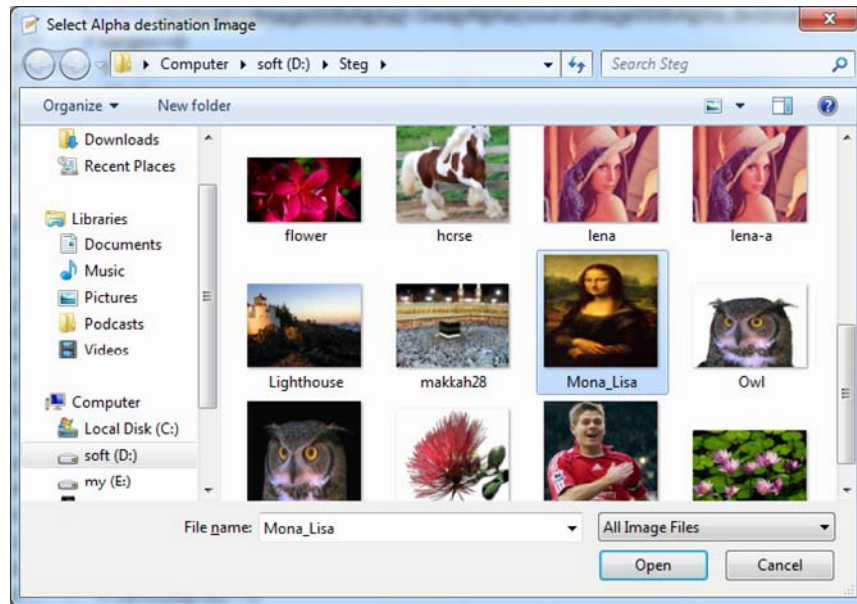


Figure 6.20: load semi-stego image

Save the semi-stego image with alpha

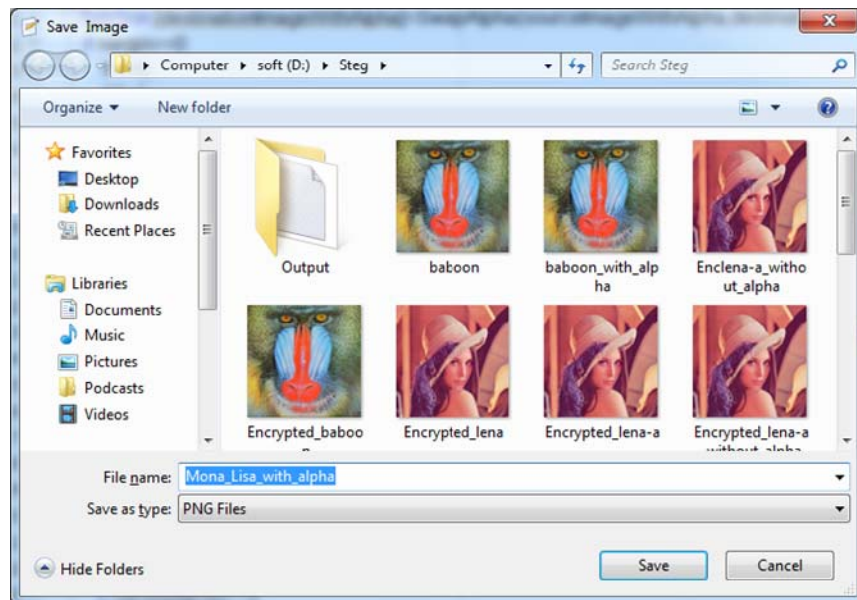


Figure 6.21: save semi-stego image with alpha

The receiving party steps to encrypt a stego image:

Step 1: load semi-stego image

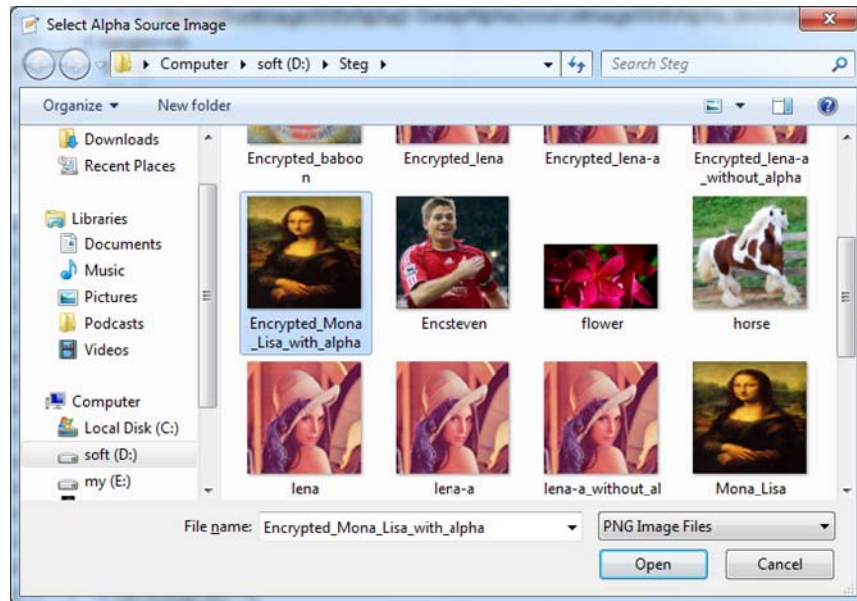


Figure 6.22: load semi-stego image with alpha

Step 2: load cover image

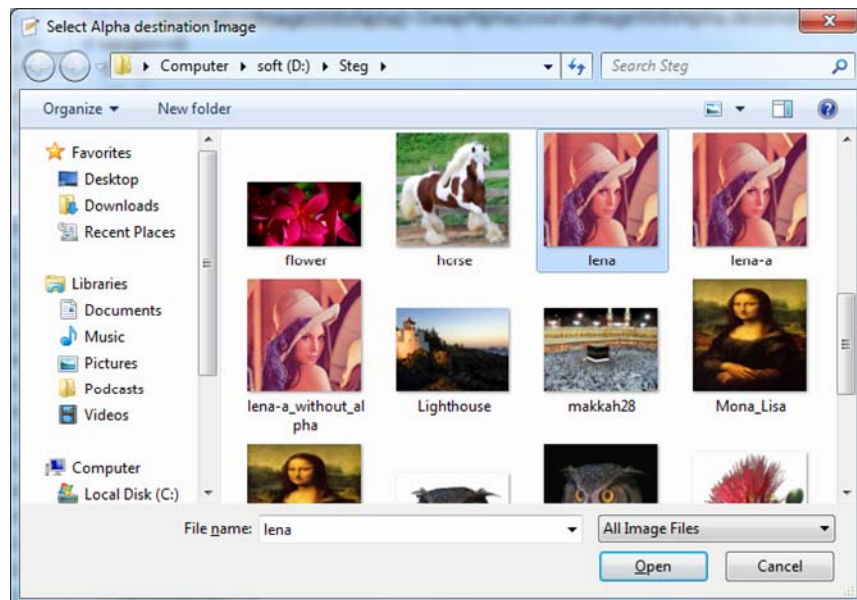


Figure 6.23: load cover image

Step 3: Save the cover image with alpha (stego image)

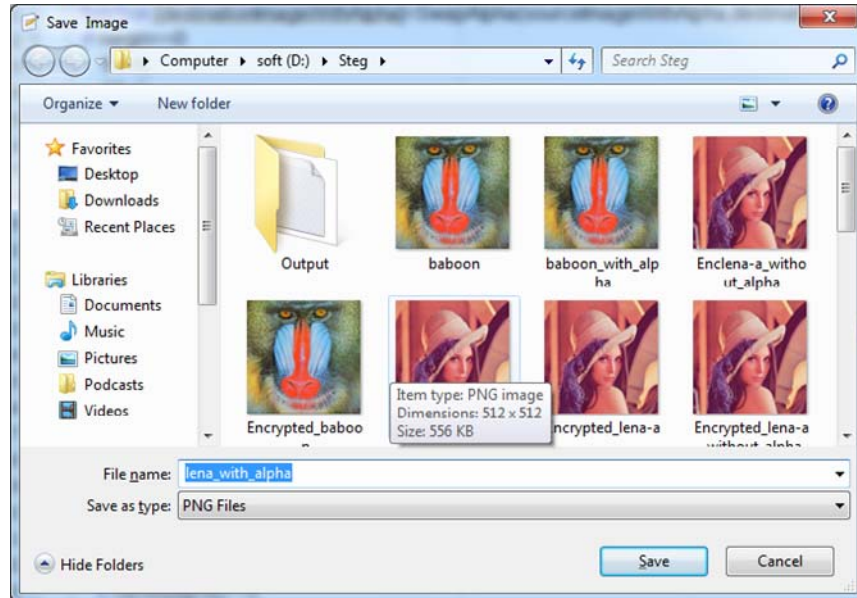


Figure 6.24: save stego image with alpha

Step 4: Then the receiving party decrypts the image

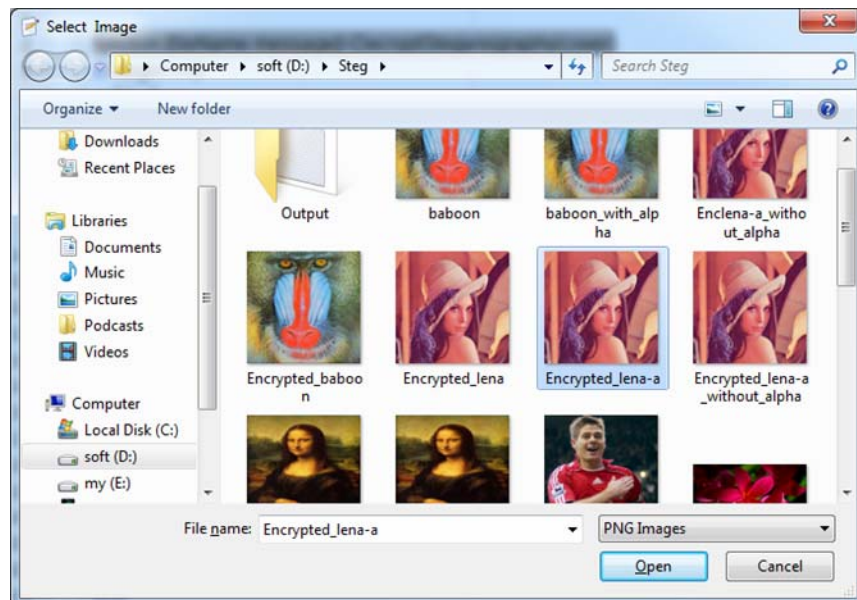


Figure 6.25: load stego image with alpha

Step 5: Save the message

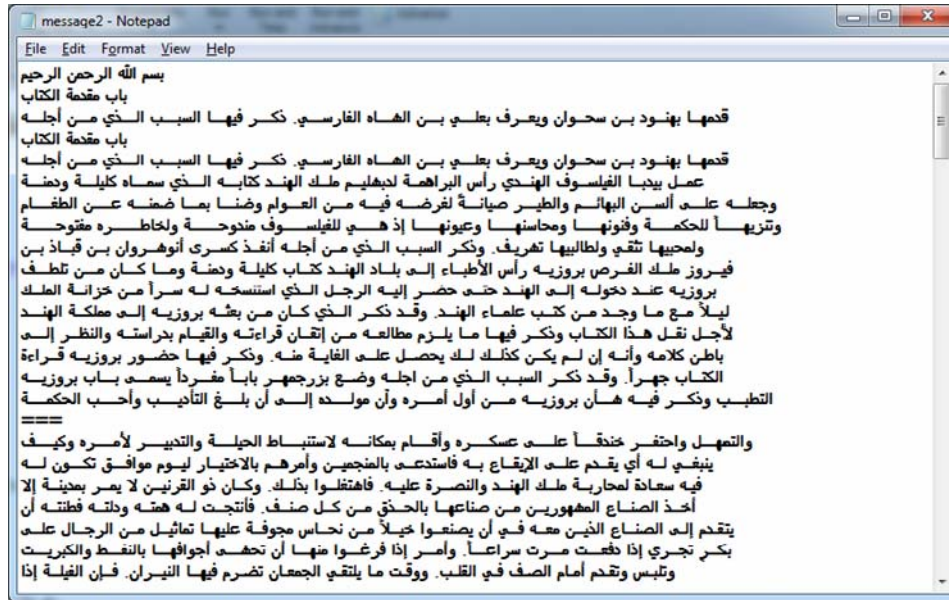


Figure 6.26: save message

Chapter seven

Conclusion and Future Work

7.1 Conclusion

1. The proposed system has demonstrated the practical possibility of hiding data within the alpha channel only of an RGBA image.
2. The hiding capacity in the proposed model is 3 bits per pixel (bpp), which is the same as changing one bit per color channel in an LSB method, but it has the advantage that no change can be detected in the analysis of the RGB channels.
3. The PSNR results for the maximum hiding capacity is considered acceptable as it is well above 30.
4. There is no visual effect on the stego images.
5. The proposed SWAP procedure will improve un-detectability by separating the alpha channel containing the secret text from the indicator RGB channels.

7.2 Future Works

1. Investigating the use of the alpha channel for data embedding in other RGB images such as BMP and TIFF.
2. Investigating the use of equal number of bits per pixel, such as 4 per pixel, stored in random pixels whose location is specified by the color indicator.

3. Splitting data hiding between the RGB channels and the alpha channel, for example 2 bits per channel, to increase hiding capacity.
4. Separating the alpha channel as one byte channel, merging it with a grey one channel image, and sending the composite grey image, then reversing the process at destination.
5. Storing other media in the alpha channel, such as JPG images or short audio messages.

References

- Akbas, A. E. (2010). A New Text Steganography Method By Using Non-Printing Unicode Characters. *Eng. & Tech. Journal*, 28 (1), 72-83.
- Available at:
http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010/researches/Text%20%287%29.pdf.
- Alvy, R. S. (1995). Alpha and the History of Digital Compositing. *Microsoft Tech Memo*, 7, p. 8-15.
- Ashok, J. (2010). Steganography: An Overview. *International Journal of Engineering Science and Technology*, 2 (10), 5985-5992. (Ashok, 2010)
- Bailey, K., Curran, K. & Condell, J. (2004). Evaluation of Pixel-Based Steganography and Stego detection Methods. *The Imaging Science Journal*. 52(3), 131-150.
- Barker E., & Barker W. (2008). Recommendation for Key Management Part 2: Best Practices for Key Management Organization. *NIST Special Publication*.
- Brainos, A. C. (2000). A Study of Steganography and The Art of Hiding Information. Master of Science in Computer Science, East Carolina University.
- Cachin, C. (2004). An information-theoretic model for Steganography. *Information and Computation*, 192(1), 41-56. (Cachin, 2004)
- Chang, C. C., & Tseng, H. W. (2004). A steganographic method for digital images using side match. *Pattern Recognition Letters*, 25(12), 1431-1437.

- Cole, E. (2003). Hiding in Plain Sight: Steganography and the Art of Covert Communication. *Information Technology Journal*. Vol 3, 245-269. (Cole, 2003)
- Conrad, E. (2007). Explanation of the Three Types of Cryptosystems. London University, ISSN 0521-8521. (Conrad, 2007)
- Craig, H. R. (1997). Covert Channels in the TCP/IP Suite. *First Monday Journal*, 2(5).
- Cummins, J., Diskin, P., Lau, S., & Parlett, R. (2004). Steganography and Digital Watermarking. School of Computer Science. The University of Birmingham, p 1-24.
- Curran, K., & Bailey, K. (2003). An Evaluation of Image Based Steganography Methods. *International Journal of Digital Evidence*, 2(2), 1-5. (Curran and Bailey, 2003)
- Curran, K., Cheddad, A., & McKeivitt, P. (2010). Digital image Steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), 727–752.
- Elnajjar, M., Zaidan, A. A., Zaidan, B. B., Elhad, M. M., & Alanazi, H. O. (2010). Optimization Digital Image Watermarking Technique for Patent Protection. *Journal of Computing (JOC) Lille, France*, 2(2), ISSN: 2151-9617, P.P 142-148.
- Fridrich, J. (2010). Steganography in digital media: Principles, algorithms and applications, Cambridge University Press. (Fridrich, 2010)
- Gaggar, A., Manek, K., & Jain, N. (2013). Steganography. *International Journal of Students Research in Technology & Management*, 1(2), 253-259.
- 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.

- Grover, S. (1998). Forensic Copyright Protection. *The Computer Law and Security Report*, 14(2), 121–122.
- Gutub, A. A. & Mohammad, T. P. (2008). RGB Intensity Based Variable-Bits Image Steganography. *Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference*, ISBN: 978-0-7695-3473-2, p. 1322-1327.
- Gutub, A. A. (2010). Pixel Indicator Technique for RGB Image Steganography. *Journal of emerging technologies in web intelligence*, 2(1), 56-64.
- Gutub, A., Ankeer, M., Abu Ghalioun, M., Shaheen, A., & Alvi A. (2008). Pixel indicator high capacity technique for RGB image based Steganography. *WoSPA–5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E. p 18 – 20.
- Hamid, A. J., Zaidan, A. A., & Zaidan, B. B. (2009). Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation. *Journal of Computing (JOC)*, 1(1), ISSN: 2151-9617, P.P 108-113.
- Hamid, A. J., Zaidan, A. A., & Zaidan, B. B. (2010). New Design for Information Hiding with in Steganography Using Distortion Techniques. *IACSIT International Journal of Engineering and Technology (IJET)*, 2 (1), ISSN: 1793-8236, pp. 72-77.
- Isbell, R. A. (2002). Steganography: Hidden Menace or Hidden Saviour. *Steganography White Paper*.
- Johnson, N. F. & Jajodia, S. (1998). Steganalysis of Images Created Using Current Steganography Software. *Proceeding for the Second Information Hiding*

Workshop, Portland Oregon, USA, p. 273-289. (Johnson and Jajodia, 1998)

Johnson, N. F., Duric, Z., & Sushil G. J. (2001). Information Hiding: Steganography and Watermarking - Attacks and Counter- measures. *Advances in Information Security*, Vol (1).

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

Kovacich, G. & Jones, A. (2002). What infosec professional should know about information warfare tactics by terrorists. *Computer & Security*, 21(1), 35-41.

Krzysztof, S. (2003). Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System - HICCUPS. Warsaw University of Technology, Poland Institute of Telecommunications, Warsaw, Poland. Retrieved online from: <http://vanilla47.com/PDFs/Cryptography/Steganography/Steganography%20in%20TCP-IP%20Networks.pdf> (Krzysztof, 2003)

Kumar, M. (2003). Cryptographic Study of Some Digital Signature Schemes. A thesis for degree of philosophy PHD in Mathematics. (Kumar, 2003)

Lakshari, A. H., Abdul-Manaf, A., & Masloin, M. (2012). Magic Hexagon Image Steganography Evaluator. University of Technology Malaysia (UTM), Retrieved online from:

http://www.academia.edu/1014807/Magic_Hexagon_Image_Steganography_Evaluator , on 20th of April 2013 at 9:00 pm.

Mastronardi, G., & Castellano, M. M. (2003). Intelligent Data Acquisition and Advanced Computing Systems. *IEEE*, 11:116 – 119. (Mastronardi, 2003)

- Mercuri, T. R. (2004). The many colors of multimedia security. *Communications of the ACM*, 47(1), 25–29.
- Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image Steganography. In *Information Systems Security Association (ISSA)*, pp. 1-11.
- Muhalim, M. A., Subariah, I., Mazleena, S., & Katmin, R. M. (2003). Information Hiding Using Steganography. Master thesis, Universiti Teknologi, Malaysia. Available at <http://eprints.utm.my/4339/1/71847.pdf>.
- Murdoch, J. S., & Lewis, S. (2005). Embedding Covert Channels into TCP/IP. In *Information Hiding: 7th International Workshop*, Vol 3727 of LNCS, pages 247–261. (Murdoch and Lewis 2005)
- Naji, A. W., Zaidan, A. A., Zaidan, B.B., & Muhamadi, A. S. (2009). New Approach of Hidden Data in the portable Executable File without Change the Size of Carrier File Using Distortion Techniques. *Proceeding of World Academy of Science Engineering and Technology (WASET)*, 56, ISSN: 2070-3724, 493-497.
- Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding: A survey. *Proceedings of IEEE*, 87(7), 1062–1078. (Petitcolas, et al. 1999)
- Rajanikanth, R. K. (2009). A high capacity data-hiding scheme in LSB-based image Steganography. Master Thesis, University of Akron. (Rajanikanth, 2009)
- Robert, K. (2004). Steganography and steganalysis. Internet Publication, available at <http://www.Krenn.nl/univ/cry/steg/article.pdf>
- Seidan, Y. A. (2013). Enhancement of A Steganographic algorithm for Hiding Text Messages in Images. Thesis master, Middle East University Amman, Jordan.
- Shirali-Shahreza, M., & Shirali-Shahreza M. H. (2008). An Improved Version of

- Persian/Arabic Text Steganography Using "La" Word". *Proceedings of the 6th National Conference on Telecommunication Technologies (NCTT)*, Putrajaya, Malaysia, pp. 372-376.
- Stoica, A., Vertan, C. & Fernandez-Maloigne, C. (2003). Objective and subjective color image quality evaluation for JPEG 2000 compressed images. *International Symposium on Signals, Circuits and Systems*, Vol (1), 137-140.
- Uma Devi. G. (2006). Steganography-Survey on File Systems. MS by Research – CSE I I I T Hyderabad, retrieved online from: <http://researchweb.iiit.ac.in/~umadevi/steg.pdf>
- Wang, H. & Wang, S. (2004). Cyber warfare vs. steganalysis. *Communication of the ACM*, 47(10), 76-82.
- Wang, Z., Sheikh, H. R., & Bovik, A. C. (2003). Objective Video Quality Assessment. *The Handbook of Video Databases: Design and Applications*. Boca Raton, Florida: CRC Press, pp. 1041–1078.
- Wayner, P. (2002). *Disappearing cryptography*. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition,. ISBN 1-55860-769-2.
- Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems. *Third International Workshop on Information Hiding*, 61–76.