Ministry of higher Education

And scientific research

Al-Qadisiyah University
College of computer Science

and an information technology .

Steganography Technique for RGB image

Project produced to the college of sciences as part of the requirement to get bachelor of sciences of computer.

Set By

Huda Hamza kadhim Russel Aill Talb

Farah Ali Mohammed Marwa Abbas Khudair

Supervisor

Dr.Rana j. Aljanaby

2017-1438

بسم الله الرحمن الرحيم

ربنا انك تعلم ما نخفي وما نعلن وما يخفى على الله من شي

في الأرض ولا في السماء

صدق الله ألعلي العظيم

إبراهيم (٣٨)

الإهداء

إلى من أصلهم ثابت وفرعهم في السماء . . .

إلى من حبهم رضا وبغضهم سخطا وبلاء . . .

إلى المثل الأعلى في الشهادة و الفداء . . .

محمدا ((ص)) واله الطيبين الأتقياء . . .

. . نهدي بحثنا هذا . .

سائلين المولى عزوجل أن يمن علينا بالعلم الوفير . . .

والتوفيق الكثير . . .

والحمد لله رب العالمين

Acknowledgment

First of all, we produce grateful thank to Allah ,and we like to express our respect to our research supervisor Dr."Rana J.AL-janaby". To helping us and supporting us to go on to achieve this work. We would like to say "thanks" to hands which supporting us to transfer us from darkness of ignorance to brightness of knowledge to all teachers in computer department.

Abstract

Steganography is the art and science of secret communicating and storage in away , which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to d detect, intercept and modify messages without being able to violate certain security premises guaranteed by a crypto system . the goal of steganography is to hide messages inside other "harmless" messages in away that does not allow any "enemy" to even detect that there is asecond secret message present.

In this project, new steganography algorithm for RGB image is created . This algorithm can be divided into two stages. The first one is by encrypting the secret message. The second one is that it can select one Channel as indicator channel to indicate the channel that are used to embed secret key. This algorithm in turn can be used to solve the problem of the traditional LSB technique, preventing attacker from secret message extracting by accumulating LSB in stego image.

Chapter One

General Introduction

(1-1)Introduction

Information hiding represents class of processes used to embed data in to various forms of media such as image, audio, video, and text or any unused area in the storage media. The embedded data should be invisible and inaudible to a any human observer. This means that the information is hidden in such manner that it cannot be detected by human senses or deliberately damaged.

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks. *[1]*

*(1-2)*Aim of project

This project aims to hide secret message to RGB image using improved Least significant Bit to prevent attacker from accumulate LSB in pixels of stego image this is due to the proposed embedding technique that depend on indicator and comparing process between secret bit and LSB pixel(cover image)

(1-3) Steganography Definition

Steganography is a two part word of Greek origin."Stegano", or "covered" and "grapy" or "writing", it doesn’t not convey the transformation of information, but rather its hiding aspect.

Steganography is the art and science of hiding the fact that communication is happening. While classical steganographic depend on keeping the encoding system secret, modern steganography is detectable only if secret information's known, e.g.asecret key. Because of their invasive nature steganography systems leave detectable traces with an image's characteristics, e.g. it’s Fourier signature. This allows an eavesdropper to detect images that have been modified, revealing that secret communication is happening although the secrecy of information is not degraded, it’shedden nature is revealy which defeats the whole purpose of steganography.

Steganography is technique to make confidential message imperceptible to human eyes by using some other data like an image. The data that hides the secret message is called "cover", "vessel”,"carrier", "countainer", or "dummy data" of the secret message. It looks innocent, attackers cannot see anything to attack therefore; steganography is more "information imperceptualizing technique". Than an "information hiding technique". Encryption of the embedded data further improves security. This scenario is analogous to putting something in Avery secure safe and then hiding the safe in hard to find place.

The main goals of steganography are: -

- To avoid drawing suspicion to the transmission of hidden (secret) message. if suspicion is raised, then this goal is defeated .
- To hide message inside other "harmless" message in away that doesn't allow any enemy to even detect that here is a second secret message present.
- The goal of steganography is undetectability, not secrecy only. *[3,4]*

(1-4) Project layout

The project consist of five chapters as follows:-

* *Chapter two (steganography system).*

This chapter consists of some illustrations about the applications of illustrations about the applications of information hiding, the comparison between the steganography, and the cryptography and the covering types classifications for steganography.

* *Chapter three (proposed steganography system in image).*

In this chapter the overall work is documented and the designed algorithms is presented.

* *Chapter four (tests & result).*

This chapter shows the tests of the cover image frames using **MSE** **PSNR** fidelity measures. And show the table result of the some samples of images.

Chapter two

Steganography System

(2.1) Some applications of information hiding

There are a number of applications driving interest in the subject of information hiding: -

- Military and intelligence agencies require unobtrusive communication.
- Criminals also place great value on unobtrusive communication. Their preferred technologies include prepaid mobile phone, mobile phone, which have been modified to change their identity frequently and hacked corporate switchboards through which calls can be rerouted.
- Lows enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so as to detect and trace hidden messages.
- Recent attempts by some government to limit online free speech and the civilian use of cryptography have spurred people concerned about liberties to develop techniques for anonymous communications on the net including anonymous remailers and web proxies.
- Schemes for digital election and digital cash make use of anonymous communication techniques.
- Marketers use email forgery techniques to send out huge numbers of unsolicited messages while avoiding responses from angry users. *[2,3]*

(2.2) Steganography and cryptography

Steganography encompasses techniques of transmitting secret data through innocuous such that it's presence cannot be detected. Steganography can be viewed as akin to cryptography. Booth have been used through out recorded history as means add elements of secrecy to communication. Cryptographic techniques "scramble" a message so that if it is interrupted, it can not be understood. Unlike cryptography, steganography doesn't encrypt information, it just hide them. Steganography seeks to make the very presence of the message undetectable and it may be used in conjunction with cryptography by hiding previously encrypt message. More comparison notes are shown in table(2-1).

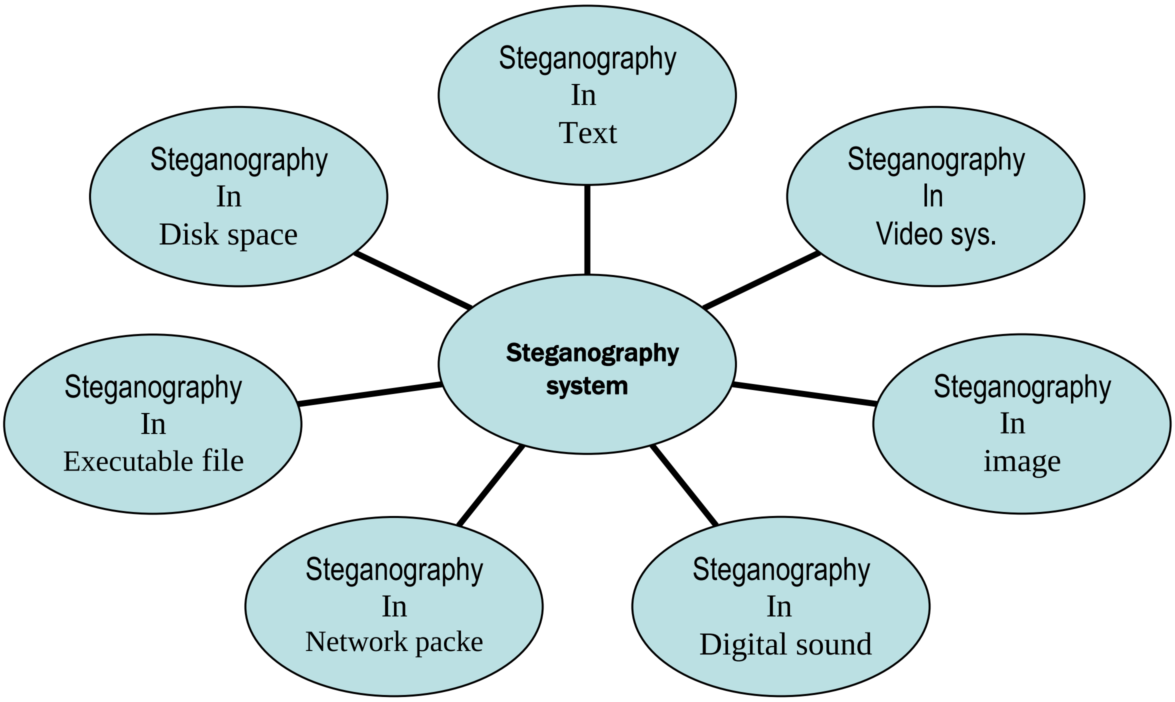
Table (2-1) comparison between steganography and cryptography: -

Cryptography	steganography
Cryptography is the science/art of transforming meaningful information into unintelligible text. **Crypt=secret** **Graphy=writing**	**Steganography is the science is of hiding in formation inside object.** **Stega=hidden.** **Graphy=writing.**
Any person has the ability of detecting and modifying the encrypted message.	**The hidden message is imperceptible to any one.**
The cryptographic system is broken when the attacker can read the secret message (decrypt the ciphered message).	**Breaking asteganography system has two stages:** **1. The attacker can detect the embedded message.** **2. The attacker is able to read the embedded massage.**
Steganography cannot be used to adapt the robustness of cryptographic system.	**Steganography can be used in conjunction with cryptography hiding an encrypted message.**
The goal of secure cryptographic system is to prevent an interceptor from gaining any information about the plain text from the intercepted cipher text.	**The goal of secure steganographic system is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.**

[5]

(2.3) Cover type classifications for steganography [5]

Steganography is the study of methods of concealing data in the noise of another data set in such a manner that the existence of the embedded data is a detectable. Caries of such data can be text, disks and storage devices, network packet, audio, image, video, or any digitally represented code. Figure (2-1) shows different steganography covers.


Steganography In Text
Steganography In Disk space
Steganography In Video sys.
Steganography system
Steganography In Executable file
Steganography In image
Steganography In Network packe
Steganography In Digital sound

As an example the steganography system in image will be described in some detail as follows. *[5]*

(2.3.1) Steganography in image

The computer-based steganography is based on three principles. These are: -

1.The files that contain digitized image can be altered to certain extend without losing their functionality unlike other types of data to be exact in order to function properly.
2. Human Vision System (HVS). It's inability to distinguish minor changes in images colors.
3. The computer –based steganography usually depends on randomness.

There are many occurrences of randomness in computer based information. Steganographic data can be hidden in to this random information. The qualities of steganographic method are judged on whether the addition of the steganographic data changes the randomness.

Image files are good example of random data for the following reasons.
1. The data in image file are represented as asset of pixels that when displayed on a computer system gives an approximation to picture.

2.image files are made up of portions that are visually constant for example. In a scanned picture of person, parts of the person's face may look visually constant, but the pixel values representing these parts are not normally constant.

3. An image file usually contains a random spread of noise.
Thus, image steganography has come quite for with the development of fast powerful graphical computers. *[6,7]*

Chapter Three

Proposed steganography system

(3.1) Introduction

This chapter contains all the stages of the image steganography. Firstly, the proposed covered file is presented next the module of proposed system is introduced in this module uses classical techniques of hiding information in each one the select bit in the original image inverse to get max error and then show the result effected image.

(3.2)- Construct of file images (Bmp)

This type of file is most spread and widely used because this type (Bmp) is typical and supported by windows operating system. Most of the applications that deal with the digital images deal with that type of images.

1-file header: -

Data guide of file heads for such file image has affixed size which is (54) byte this size includes data about this type and the size of the image file and the title of the beginning of image data area with in the file.

2-Image information area (heads): -

This area contains the properties data of image file which exist within the file. The size of this area is fixed (40) byte

(3 .4) Least significant bit

Least significant bit (LSB) insertion is a common , simple approach to embedding information in a cover image . the least significant bit (in other words , the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message when using a 24-bit image , a bit of each of the red green and blue colour components can be usd , since they are each represented by a byte . In other words. One can store 3 bit in each pixel An 800 x 600 pixel image , can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data . For example a grid for 3 pixels of a 24-bit image can be as follows :

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

when the number 200 , which binary representation is 11001000 , is embedded into the least significant bits of this part of the image , the resulting grid is a follows :

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the gri , only the 3 underlined bits needed to be changed according to the embedded massage . On average , only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size . Since there are 256 possible intensities of each primary colour , changing the LSB of a pixel result in small changes in the intensity of the colours . These changes cannot be perceived by the human eye-thus the massage is successfully hidden .

Algorithm

Input:- cover BMP image , secret message

Output:- Stego image

Stepl:- Read BMP image(cover image)

Step2:- Read secret message

Step3:- Encrypt secret message

Step4:- select blue channel as indicator channel

Step5:- compare next bit from encrypted secret message with LSB from channel (R And G)

If encrypted secret bit equal to LSE of Channel R then make LSB of channel B =1 goto step6

Else if encrypted secret bit equal to LSB of Channel G then make LSB of channel B= 0 goto step6

Else if encrypted secret bit not equal to LSB of channel R nor G then set LSB of channel B to 1 and replace LSB of R to secert bit

Step6:- repeat steps 6 until Bmp image is completed .

Chapter four

Tests & results

Conclusion & Suggestion

Introduction

This chapter includes aset of results for all implement techniques of image steganography, all tests are summarized in table (4.1) that show the differences among the classical steganography techniques, and show the testing results of the image steganography techniques.

(4.2) Embedding Evaluation and fidelity Criteria.

The MSE and PSNR fidelity measures are used in this chapter to test the implemented steganography techniques of the proposed system.

4.2.1-Mean Square Error (MSE)

Mean square error computes the signal difference between distorted image and original one according to the following formula:

$$MSE=1/w*h \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} (I_{xy}-I'_{xy})\wedge^{2} \qquad .... 4.1$$

Where w, h is the width and height of image, I_{xy}, I''_{xy} represent the pixel with row number x and column number y in the original image and the distorted image respectivly.recall that minimum MSE is better candidate. *[6]*

4.2.2-Peak signal to noise ratio (PSNR).

Peak signal to noise ratio is another difference distortion metrics that is adopted to obtain the visual quality of the preprocessed image or the stego-image. PSNR is computed using the following formula:

$$PSNR=10 \log (l-1)\wedge^{2}/MSE \qquad .... 4.2$$

Where l is the gray levels (e.g., for 8 bit per pixel l=256) *[6]*

Image Name	*Image size in MB*	*Message Length*	*MSE*	*PSNR*
Image1	*1.21*	*32*	*1.8527e-04*	*196.7621*
Image2	*1.21*	*24*	*1.6509e-04*	*197.9152*
Image3	*1.28*	*30*	*9.5982e-05*	*203.3388*

The table of MSE and PSNR

4.3-Conclusion

It improve the traditional Least Significant bit approach for the following reasons , first one , because of using the indicator LSB to indicate which channel are used to store one bit of secret message solve the problem of sequential embedding in LSB . Second , in each pixel only two bits at most instead of three will be used so the similarity between original and stego image will be increased .

4.4-Recommended Future Work.

1- Developing the system to hide real data in image.

2- Developing the system to contain key word for unauthorized setup.

3- Developing image steganography using enhanced methods (error recovery techniques).

References

[1]. Fabian a.p.petitcolas, ross j. Anderson and Markus g. Kuhn ,"information hiding :A survey", proceedings of the IEEE, special issue on protection of multimedia content, July 1999.

[2]. Stefan K, Fabian A.P.Petitcolas,"information hiding techniques for Steganography and digital watermarking", Artech house press ,2000.

[3]. Abdullah M. A Jafar, "Audio hiding in Audio file by using low-bit encoding", M.SC. Thesis, informatics institutes for postgraduate studies, Iraqi commission for computers and informatics, 2003.

[4]. Alain C. Brainos,"A study of steganography and the Art of hiding information", East Carolina university, 2004.

[5]. Neil F.johanson, Zorn Doric, and sushil. J.,"information hiding steganography and watermarking-attacks and countermeasures", Georgemason university, 2001.

[6]. Zaid k. Ibrahim," image based steganography system", m.sc.thesis, college of science, al – Nahrain University, 2002.

[7]. Mehdi K, Husrev T. Sencar, and Nasir M.,"Image steganography concepts and practice", Polytechnic University, Brooklyn, ny 11201, USA, April 22 , 2004.
Mehdi, taha, memon@isis.poly.edu.

content