Information Hiding using 8 Bit Image

Luaay .A. shihab

Abstract: ***Steganography is the process of hiding a secret message within alarger one in such a way that someone cannot know the presence or contents of the hidden message. The purpose of Steganography is to maintain secretcommunication between two parties. This paper will show how steganography used in a modern context while providing a practical understanding of what steganography is and how to accomplish it. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead. Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. In this paper cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermark . In this research colored images are used to hideArabic and English texts. The images with BMP extension are used for such hiding operation. The reason behind using BMP type is offering because of it's moreaccuracy in showing the image without any of compressed data and it is considered tobe the most used format in hiding operation, in addition it can handle most importantcolor levels such as (8 bits). The steganography method applied in this work is executed by Delphi language.***

Keyword : steganography, encryption, decryption , information hiding,image.

I. INTRODUCTION

Steganography, coming from the Greek words stegos, meaning roof or covered andgraphiawhich means writing[2], is the art and science of hiding the fact that communicationthe first color image was in 1861 at the hands of the physicist James Maxwell with the help of photographer Thomas Sutton and was considered just an experiment for color imageis taking place. Using steganography, you can embed a secret message inside apiece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related[1]. Cryptography scrambles messageso they cannot be understood. Steganography on the other hand, will hide themessage so there is no knowledge of the existence of the message in the first place. Insome situations, sending an encrypted message will arouse suspicion while an "invisible"message will not do so.

Both sciences can be combined to produce better protection ofthe message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques. Therefore, the principle defined once by Kerckhoffs for cryptography, also stands forsteganography: the quality of a cryptographic system should only depend on a smallpart of information, namely thesecret key.

The same is valid for good steganographicsystems: knowledge of the system that is used, should not give any information about theexistence of hidden messages. Finding a message should only be possible with knowledgeof the key that is required to uncover it. Color images Color Image[5], are digital images that support color by allocating three boxes per pixel to determine the severity of the three colors core (red, green, and blue) and each box contains 8 bite for writing them, for example the intensity green may be 100000 i.e. there are 24 house per pixel ,but some images may be only 8 house and contains 256 color only .

II. STEGANOGRAPHY CONCEPTS

Although steganography is an ancient subject, the modern formulation of it is often given in terms of theprisoner's problem proposed by Simmons where two inmates wish to communicate in secret to hatch an escape plan[14]. All of their communication passes through a warden who will throw them in solitary confinementshould she suspect any covert communication[12]Almost all digital file formats can be used for steganographyfig(1), but the formats that are more suitable are thosewith a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy fargreater than necessary for the object's use and display.Steganography is the art and science of writing hidden messages in such a waythat no one apart from the intendedrecipient knows of the existence of themessage. Unlike cryptography, where the existence of the message is clear, but the [6]Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contentsof a message secret, steganography focuses on keeping the existence of a message secret[14]meaning is obscured, the steganographic technique strives to hide the very presenceof the message itself from an observer. Steganography simply takes one piece ofinformation and hides it within another Theredundant bits of an object are those bits that can be altered without the alterationbeing detected easily. Image and audio files especially compatible with thisrequirement, while research has also uncovered other file formats that can be usedfor information hiding If applied to images, that degradation, at times, may be visible tothe human eye [1] and point to signatures of the steganographic methods and tools used.

Manuscript received May, 2013.
Luaay . A . Shihab Nursing of college basrahuniversity, Basrah, Iraq

These signatures mayactually broadcast the existence of the embedded message, thus defeating steganography[12].

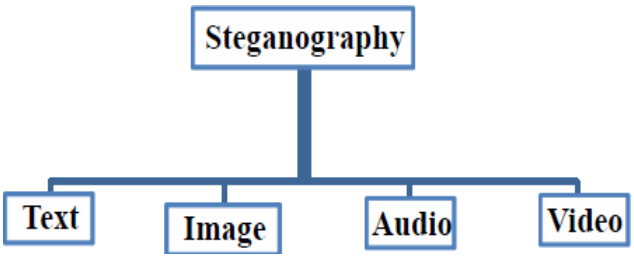


Figure (1) Steganography in multimedia file

III. WATERMARKING FOR IMAGE AUTHENTICATION

In authentication applications, the objective is to detect modifications of the data. This can be achieved with socalled"fragile watermarks" that have a low robustness to certain modifications like compression, but are impairedby other modifications [2]. Furthermore, the robustness requirements may change depending on the data typeand application. Nevertheless, among all possible watermarking applications, authentication watermarks require thelowest level of robustness by definition. It should be noted that new approaches have emerged in which dataattributes, such as block average or edge characteristics, are embedded and check if the received image still has thesame attributes.[5] It is clear that such schemes may require a higher robustness if identification of the modified area of interest.

IV. LEAST SIGNIFICANT BIT SUBSTITUTION:

Bitplane tools encompass methods that apply LSB insertion and noise manipulation. These approaches are commonin steganography and are relatively easy to apply in image and audio . A surprising amount of information canbe hidden with little, if any[13], The image formats typically used in suchsteganography methods are lossless and the data can be directly manipulated and recovered. Some of theseprograms apply compression and encryption in addition to steganography services. These services provide bettersecurity of the hidden data. Even so, the bitplane methods are rather brittle and vulnerable to corruption due tosmall changes to the carrier.The embedding process consists of choosing a subset {j1, . . . , jl(m)} of cover- elements and performing thesubstitution operation cji mi on them, which exchanges the LSB of cjiby mi (mi can either be 1 or 0). One couldalso imagine a substitution operation which changes more than one bit of the cover, for instance by storing twomessage bits in the two least significant bits of one cover-element. In the extraction process, the LSB of the[4]

selected cover-elements are extracted and lined up to reconstruct the secret message. One problem remains to be solved: in which way should the cjibe chosen?In order to be able to decode the secret message, the receiver must have access to the sequence of element indicesused in the embedding process, In the simplestIn its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels are not often used on the Internet and might arouse suspicion [3]. For this reason, LSB steganography has also been developed for use with other image file formats.

V. HIDE DATA WITH IN IMAGES

For the purpose of understanding how to complete the process of concealment within images must understand how the representation of the image within the calculator First[9], is a matrix of values representing the intensity of illumination at that point and is represented every point b (byte) and one 1-byte (8-bit) These values represent an introduction to the color table palette in the prefix File Header, the number of

levels DIFFERENT COLOR that can be represented in eight cells is 256 bilateral level chromatically any color just grandmothers table contains 256 colors.the images vary in terms of the number of colors that they contain and in terms of size other than the number of cells (Bit) [13], the most important of these speci

VI. PHOTOS BILATERAL

At the beginning of the emergence of computers were pictures represent cell one Each unit mock it be worth the (1,0) any black or white and stored image two-dimensional ciphers or units, so called these images (b pictures black and white) or monochrome .After pictures black and white, appeared images grayscale an image monochrome, to[10], but is made up of shades of gradients of gray gives information about the intensity of lighting only, without color, and the number (Bits) used to represent each point showing the number of levels of light intensity[14], and common image is that used (8-Bit) which can display 256 gradual chromatically These photographs although it is colorful but still so far used in many applications .

VII. TYPES OF WRITINGSECRET

There are three types of secret writing and applied in the concealment systems, namely[2]: 1-Pure Steganography Concealment pure 2-Secret Key Steganography Concealment secret key 3-Public Key Steganography Concealment public key Pure Steganography Called on the concealment system that does not require an advance exchange of confidential information (fig 2) that Hide system pure and concealment process described as follows:

E: C * M ⟶C

Covers are a potential coverage: C Is a likelihood of the message: M

The return process is described by the following formula D: C ⟶M

Secret Key Steganography 2-3 concealment secret key(K) hides the secret message using a secret key (Cover)

Here the sender chooses cover taking the secret key used to hide the message known to the recipient,[13] it can reverse the treatment and retrieve the secret message and anyone else who does not know the secret key cannot retrieve information and described the process this way concealment following.
EK: C * M * K **?**C
The retrieval of information as follows:
DK: C * K **?**M

Public Key Steganography 3.3 concealment public key This method requires the use of two keys, one private and one public key stored in the base year general data is used in the process of concealment, while the private key (secret) is used to retrieve the message confidentiality in using public key encryption is not necessary that two people share a secret key to form a secret channel Connection , but they only know the public key to the other, as well as in concealment[10]

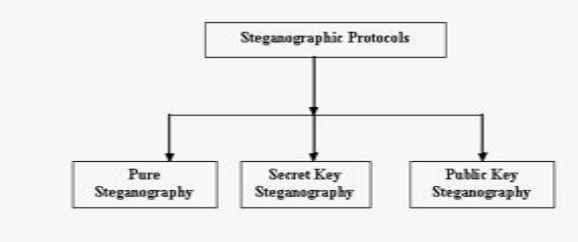


Figure (2): Staganographic

VIII. 8BIT COLOR IMAGES

When there are restrictions on the storage capacity or restrictions on Display devices, many of the systems used24-Bits 8 – to represent the colors (256 colors) do not have to bitslookup table (LUT) 8 – the concept of concordance table Bits image files used colorful actress to store color images[7] In fact, are not taken to store the colors in these images, but a group of bits refers to a table containing valuable

3 – which represents the color of the pixel. The 1 refers to the orange color and the number 2 to the color bytes Green, and so on. It is necessary to choose the values that represent a better image, if the image is represent the spectacle of sunset it is best to red color is represented with great accuracy compared paintedGreen.8 -. We note that it is difficult to see the difference between bits on the color image 24 and image in8 Bits based on the directory storage bits The idea used in the images represented on encoding of the value of the pixel. For example, if the value of 25 pixels, this means going to the line8 – is usually stored in the concordance table in the header of the file to indicate bits in the image files actress. R, G, B 8 – bits colors on the concordance between the values represented on. Palette color LUT table named table .

9- Theoretical consideration

```
Timer1.Enabled := False.

Button1.Enabled := False;

If TSH1.TabVisible Then

Begin

If RB1.Checked Then
Begin
CS1.Socket.SendText('Correct!' + Name. Caption + '!' +
Memo1.Text + '!' + RB1.Caption + '!' +
Edit1.Text + '!' + Edit2.Text + '!' +
Group. Caption + '!'); RB2.Enabled
:= False; RB3.Enabled := False;
RB4.Enabled := False;
Exit;

End;

If RB2.Checked Then
Begin
CS1.Socket.SendText('Correct!' + Name. Caption + '!' +
Memo1.Text + '!' + RB2.Caption + '!' +
Edit1.Text + '!' + Edit2.Text + '!' +
Group. Caption + '!');
RB1.Enabled := False;
RB3.Enabled := False;
RB4.Enabled := False;
Exit;
End;[8-11]
```

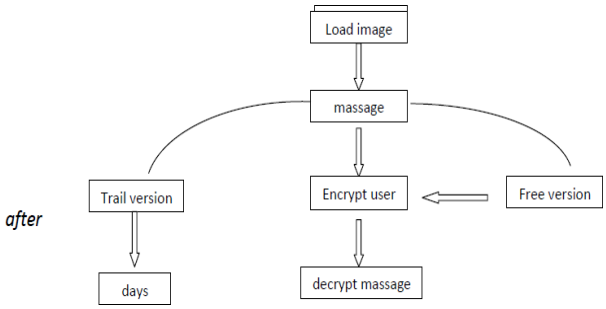
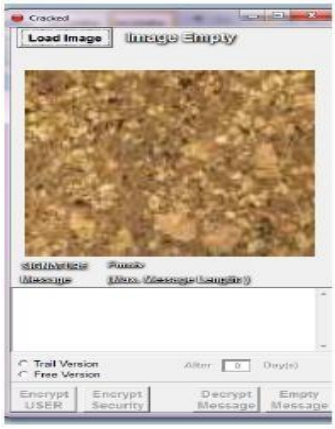


Figure (3) flowchart to hide text in the image and retrieval

Fig(4) original picture of the 8 bit (1234)



Fig(5) image after masking text length

Fig(6) original picture of the 8 bit (1693)

Fig. (7)Image after masking text lengt(

working mechanism at first begin download image and then choose the size of the text to be sent within the image and the image of the 8-bit bmp has the text reaches the number of characters to more than 1200 characters and by the possibility of image and after the agreement between the sender and receiver determines the day and month and year with the code (username and password) in order to Checking out the recipient must enter the name and password so that he can open the images and see the text has been the experience of more than 75 pictures with text in the lab and has been successfully attach some of the designs above 4-5-6-7

IX. CONCLUSIONS

This paper used the 8 bit image andsteganography techniques to hide secret message of (50) different in to cover image and hiding in image files implementations of those techniques have been performed. Gives perfect recons traction of the secret messages.

REFERENCES

1. Analysis and Implementation of Distinct Steganographic Methods Kavaklıdere, Ankara/TURKEY 2002.
2. information hiding using steganography/muhalim Mohamed amin/university teknologimalaysia 2003.
3. an overview of image steganography/ t .morkel, j.h.p.eloft/university of Pretoria
4. Chi-Kwong Chan and L. M. Chen, “hiding data in images by simple LSB substitution”, Pattern Recognition , 37 (2004), 469-474.
5. LINGUISTIC STEGANOGRAPHY: SURVEY, ANALYSIS, AND ROBUSTNESSCONCERNS FOR HIDING INFORMATION IN
6. TEXT by Krista Bennett 2004
7. Text Hiding Using Artificial Neural NetworksHaiderTarishHaider Engineering College, University of Al-Mustansiriyah /Baghdad , 2012.
8. AlkhraisatHabes, "Information Hiding in BMP image Implementation, Analysis and Evaluation",2006 .
9. Delphi language guide October 2004 scotts valley ,California.
10. Information hiding techniques A tutorial reviewSabuMthampi (Assistant professor , LBS college of engineering Kasarng of – Kerala – India 2004) .
11. Steganography Implementation on (BMe) colored image type Shaed Abdul rahmanHisson , Ilaf Osama AbdElmajid university of Mosul 2008 .
12. building user interfaces with Delphi 2009 , Corporate Headquarters / San Francisco California , 4111 EMEA / SL6 1SF , United kingdom Asia – Pacific Headquarters Melbourne VIC 3000 / Australia .
13. Digital Image Steganography Pradeep Kumar Saraswat RK Gupta VSRD international Journal of computer science India 2012 .
14. Informationhiding techniques forSteganography and digital water marking / Stefan Kat ZenbeisserFnbienA.P.Petitcolas 2000 .
15. AN OVERVIEW OF IMAGE STEGANOGRAPHY