

Hide Data in Card

Noor Fahem Sahib

college of science for women , computer dept. , Babylon University

Babylon , Iraq

Tel: 07813464096 E-mail : noor.aljaiphri@yahoo.com

Zahraa Amar Hashim

College of information Technology , Software department, Babylon University

Babylon , Iraq

Tel: 07825536959 E-mail: xinzhou.song@pku.edu.com

Abstract

Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. In this paper, we describe method of Steganography based on embedding encrypted message bits using RSA Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique) of the pixel of image.

Keywords: hiding private information, protect data

1. Introduction

1.1 Introduction

We are in the middle of an exciting period of time in the field of image processing. Indeed, scarcely a week passes where we do not hear an announcement of some new technological breakthrough in the areas of digital computation and telecommunication. [3]

1.2. Image processing

Image processing is a method to perform some operations on an image, in order to get an enhanced image or to extract some useful information from it. It is a type of signal processing in which input is an image and output may be image or characteristics/features associated with that image. Nowadays, image processing is among rapidly growing technologies. It forms core research area within engineering and computer science disciplines too.

- Image processing basically includes the following three steps:
 - Importing the image via image acquisition tools.
 - Analyzing and manipulating the image.
 - Output in which result can be altered image or report that is based on image analysis.

There are two types of methods used for image processing namely, analogue and digital image processing. Analogue image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. Digital image processing techniques help in manipulation of the digital images by using computers. The three general phases that all types of data have to undergo while using digital technique are pre-processing, enhancement, and display, information extraction.[1]

1.3 Digital image

A digital image is an electronic file that forms into square picture elements (pixels) when displayed on a viewing device (e.g., a computer monitor). The displayed image is a two-dimensional matrix of thousands or millions of pixels each of which has its own address, size, and color representation. You might think of pixels as serving a role similar to the grains in a photograph.3 digitizing a photograph means converting or capturing its image electronically through a scanner or digital camera. Digital image processing software allows you to magnify an image to see the pixels, and to sometimes measure the numeric color values for each pixel – like a

sophisticated, computer generated, paint-by-number matrix.

People use digital images in many ways. The same image can be viewed on a wide variety of monitors, printed in many formats, and transmitted electronically through e-mails, cell phones, and other systems. Digital images are stored electronically on media such as computer hard drives, CDs, DVDs, or magnetic tapes.[2]

The image types we will consider are: Binary Image, Gray Scale Image, Color Image, Multispectral image.(It will be described in Chapter two)

Pixel is the smallest element of an image. Each pixel correspond to any one value. In an 8-bit gray scale image, the value of the pixel between 0 and 255. The value of a pixel at any point correspond to the intensity of the light photons striking at that point. Each pixel store a value proportional to the light intensity at that particular location.

1.4 Types of Digital image

The image types we will consider are: Binary Image, Gray Scale Image, Color Image, Multispectral image.

1.4.1 Binary image

Binary images are the simplest type of images and can take on two values, typically black and white, or '0' and '1'. A binary image is referred to as a 1 bit/pixel image because it takes only 1 binary digit to represent each pixel.

It is often created from gray-scale images via a threshold value is turned white ('1'), and those below it are turned black ('0'). Every pixel in a binary image must be one of two colors, usually black or white. This inability to represent intermediate shades of gray is what limits their usefulness in dealing with photographic images. [4]

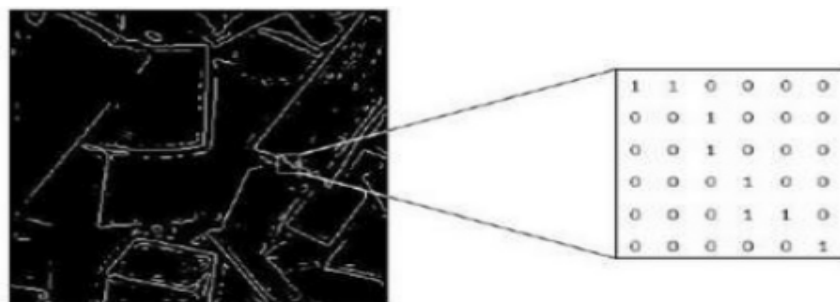


Figure 4:binary image

1.4.2 Gray Scale Image

Gray _scale images are referred to as monochrome or one-color image. They contain brightness information only brightness information only, no color information. The number of different brightness level available .The typical image contains 8 bit/ pixel (data, which allows us to have (0-255) different brightness (gray) levels. The 8 bit representation is typically due to the fact that the byte, which corresponds to 8-bit of data, is the standard small unit in the world of digital computer.[4]



Figure 5:gray image

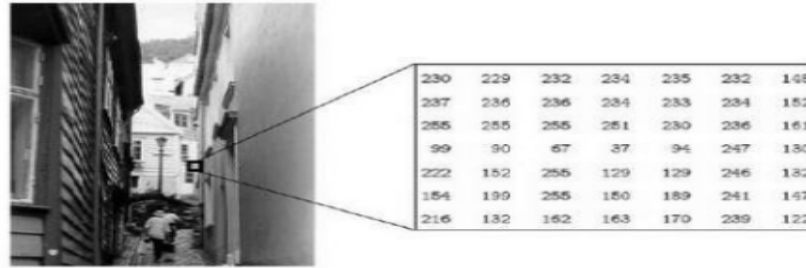


Figure 6:gray image

1.4.3 Color Image

Color image can be modeled as three band monochrome image data , where each band of the data corresponds to a different color. Typical color images are represented as red, green ,and blue or RGB images .using the 8-bit monochrome standard as a model , the corresponding color image would have 24 bit/pixel – 8 bit for each color bands (red, green and blue). The following figure we see a representation of a typical RGB color image. [4]



Figure 7:color image

1.4.4 Multispectral images

Multispectral images typically contain information outside the normal human perceptual range. This may include infrared (),ultraviolet (), X-ray, acoustic or radar data. Source of these types of image include satellite systems underwater sonar systems and medical diagnostics imaging systems.[1]

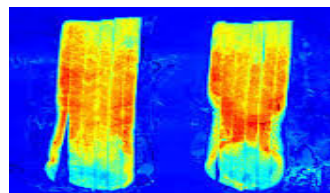


Figure 8:multispectral image

1.5 Representation of digital image

dimensional digital image can be represented as a 2-dimensional(2D) array of data $s(x, y)$, where (x, y) represent the pixel position. The pixel value corresponds to the brightness of the image at position (x, y) . Some of the most frequently used image types are binary, gray-scale and color images.

1.6 Dimension of images

An important feature of digital images, that they are multidimensional signals, meaning that they are functions of more than a single variable. The signals are usually 1D functions of time. Images, however, are functions of two and perhaps three space dimensions.

Image dimensions are the length and width of a digital image. It is usually measured in pixels, but some graphics programs allow you to view and work with your image in the equivalent inches or centimeters. Depending on what you plan to use your image for you may want to change the image size.

For example, if you are using a high-resolution digital photograph, you may want to make the image dimensions smaller for publishing to a Web page. When using a graphics or image-editing program, you will usually have two options for changing the image dimensions: resize or resample. [2]

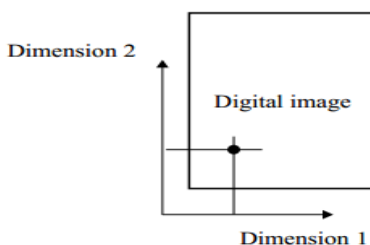


Figure 9:dimension of image

1.7 Problem Statement

- How can we send a message secretly to the destination.
- Using steganography, information can be hidden in carriers such as images ,audio files, text files, videos and data transmissions.
- In this study, I proposed a new framework of an image steganography system to hide a digital text of a secret message.

1.8. Research layout

The researches arranged as follows:

- Chapter one consists of a general introduction to all topics, which are implemented, in the project and research problem.
- Chapter Two introduces for digital image, image Steganography.
- Chapter three deals with design and implementation of the proposed system.

Chapter four deals with the result that yields from the research, concluding remarks and future works.

2 . Steganography

2.1 Introduction

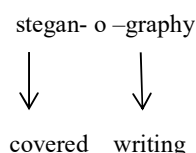
Steganography is the technique of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the hidden message. It is taken from Greek word “STEGANOS” which means “Covered” and “GRAPHIE “which mean “Writing”. So, Steganography is a method of covering important information behind an image. Steganography ancient origins can be traced back to 440 BC, from the Histories of Herodotus. Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye It is not a rule that we must hide data in image files only; we can also hide data in MP3 and Video files too. When hiding information inside images the LSB (Least Significant Byte) method is usually used. When hiding information inside Audio files the technique usually used is low bit encoding which is

somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random noises to the signal, the information is concealed inside a carrier and spread across the frequency spectrum. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video. When only a small amount of information is hidden inside of video it generally is not noticeable at all, however the more information that is hidden the more noticeable it becomes. So Steganography in Images is preferred.

2.2 What is Steganography?

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message

- Steganography comes from the Greek word ,it means covered or secret writing.



- “The goal of steganography is to hide messages in such a way that no one apart from the intended recipient even knows that a message has been sent.”

- This can be achieved by concealing the existence of information within seemingly harmless carriers or cover.

2.3 What is Image Steganography?

Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden messages or data. For example, Cover Image Data / Message Stego Image.

2.4 Steganography Technique

Pure steganography: Pure steganography is the process of embedding the data into the object without using any private keys. This type of steganography entirely depends upon the secrecy. This type of steganography uses a cover image in which data is to be embedded ,personal information to be transmitted, and encryption decryption algorithm to embed the message into image.

Example: To hide (100011) in a gray scale image:

Original: 01001101 01001110 01001110 01001111 01010000

01010000 01001111

1 0 0 0 0 1 1

Encoded: 01001101 01001110 01001110 01001110 01010000 01010001 01001111

2.5 The aim of project

This type of information concealment is very effective against discovery and can serve a variety of purposes. These can include authentication purposes, hiding messages, and transferring encryption keys. The most effective method for this type of information hiding is usually the least bit significant method. This simply means that the hidden message will change another bit of bytes in the image. By changing it slightly past, there will be relatively no change in the color of this pixel in the carrier image. This message keeps them from being easily discovered. The best type of image file to hide information inside is a 24-bit bitmap.

2.6 Applications of Image Steganography

.Secure Private Files and Documents.

.Hide Passwords and Encryption Keys.

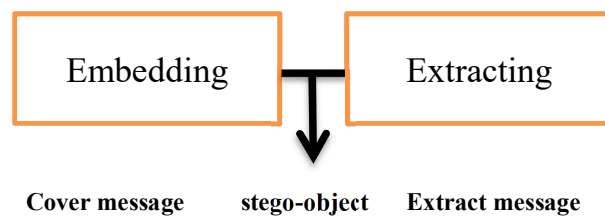
- .Transport Highly Private Documents between International Governments.
- .Transmit message/data without revealing the existence of available message .

3. The design and implementation of proposed system

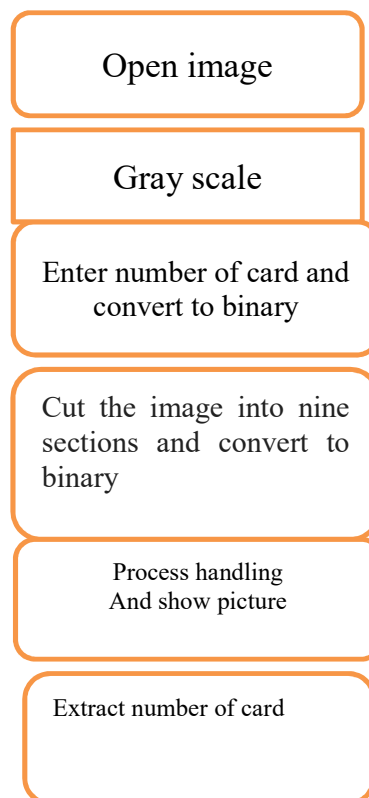
3.1. overview

In this chapter, the proposed system stages are discussed thoroughly from the pre-processing stage to final documents clustering.

3.2. Scheme of steganography



3.3 The system stages



3.2.1. Open image

The first step is to read an image; It depends on your file path.

The second step is open image.

Algorithm (3.3.1): Open image

Input path of image

Output image

1. Chose the size of the image that we want.
2. Open an image depending on the path.
3. Display pictures in the Pictures Box.

Figure 7:open image

3.3.2. Gray scale

Algorithm (3.3.2): Gray scale image

Input original image

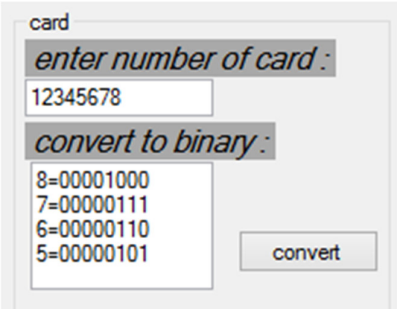
Output Grayscale image

1. **Select the image that we want to convert to grayscale.**
2. Bitmap bit.
3. For I from 0 to image width -1 .
4. {
5. For J from 0 to image height -1 .
6. {
7. **c = bit.GetPixel(I, J);**
8. **gray = 0.333 * c.Red + 0.333 * c.Green + 0.333 * c.Bule**
9. **image[I, J] = gray;**
10. }//End of the loop height.
11. }//End of the loop width
12. **Display pictures in the Pictures Box.**

Figure 8:gray image

3.3.3. Enter number of card and convert to binary

In this step you enter the card number to hide in the digital image.



card

enter number of card :

12345678

convert to binary :

8=00001000
7=00000111
6=00000110
5=00000101

convert

Figure 9: card number

Code (3.3.3): convert number of card to binary

```
e=number of card
i, k, j;
for (j = 0; j < 8; j++)
{
    if (j == 0)
    {
        k = e % 10;
        e = e / 10;
        textBox1.Text += k + "=";
        for (y = 7; y >= 0; --y)
        {
            c[y] = k % 2;
            k = k / 2;
        }
        for (y = 0; y < 8; y++)
            textBox1.Text += c[y];
        textBox1.Text += "\r\n";
    }
}
```

Figure 10:code convert binary

3.3.4 cut image and convert to binary

In this step the image is divided into nine sections with a drawing of each section of the first eight pixels with a red color value and placed in eight matrices.

code (3.3.4) cut image

```
for (i = 0; i < w / 3; i++)
{
    for (j = 0; j < h / 3; j++)
    {
        m = 0;
        cut11[i, j] = (re.GetPixel(i, j).R + re.GetPixel(i, j).G + re.GetPixel(i, j).B) / 3;
        m = cut11[i, j];
        if (m == 106)
        {
            richTextBox1.Text += cut11[i, j].ToString() + " ";}}}
}
```

Figure 11:cut image

code (3.3.4) convert binary

```
for (j = 0; j < 8; j++)  
{  
    if (j == 0)  
    {  
        k = e % 10;  
        e = e / 10;  
        textBox1.Text += k + "=";  
        for (y = 7; y >= 0; --y)  
        {  
            c[y] = k % 2;  
            k = k / 2;  
        }  
        for (y = 0; y < 8; y++)  
            textBox1.Text += c[y];  
        textBox1.Text += "\r\n";  
    }  
}
```

Figure 12: convert binary

3.3.5 process handling and show picture

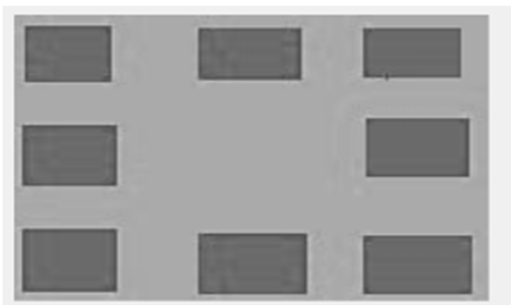


Figure 13: original image

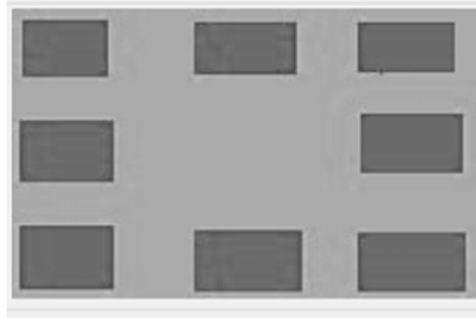


Figure 14: stego image

4. Implementation and conclusion and future work

4.1 Implementation

- In this project I mainly concentrated on embedding the data into an image. I have designed the steganography application which embedded the data into the image.
- Normally, after embedding the data into the image, the image may lose its resolution. In the proposed approach, the image remains unchanged in its resolution as well in size.
- The speed of embedding the data into the image is also high in the proposed approach such that the image is protected and the data to the destination is sent securely.

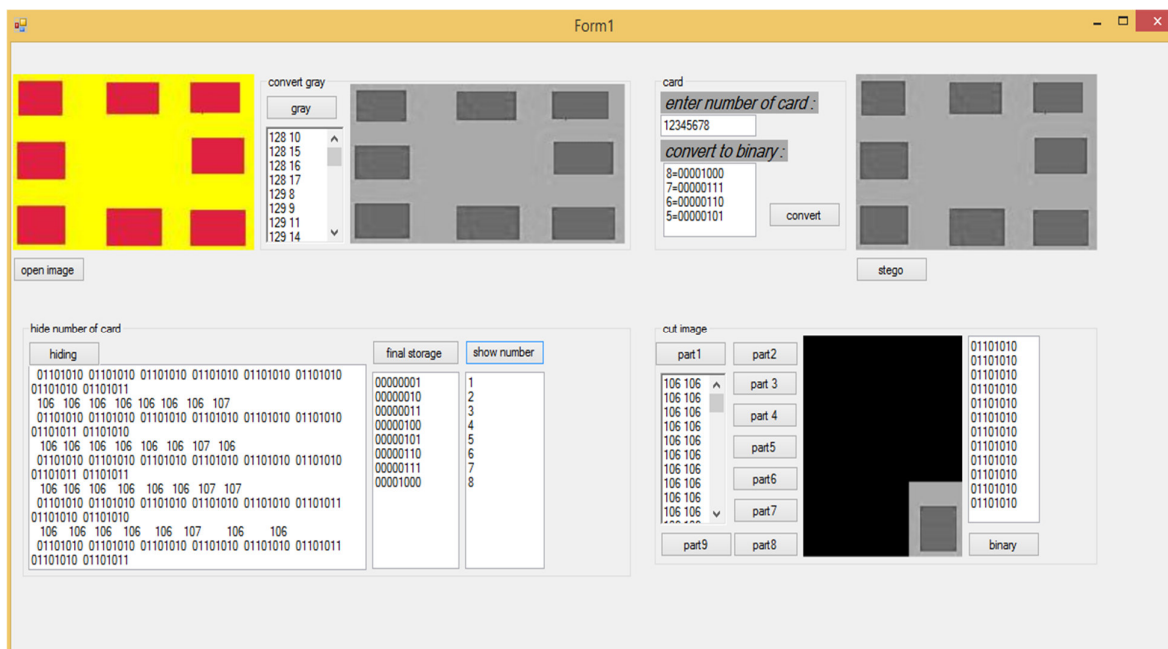


Figure 15:original image

4.2 conclusion and future work

- In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So ,many individuals and business people use to transfer business documents ,important information using internet.
- Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it use lessor obtain information un- intended to him.
- The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for the different types of image formats like .bmp, .jpeg etc., in the future. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

Reference

- [1] Beenish Mehboob and Rashid Aziz Faruqi “A Steganography Implementation” in 2008 IEEE.
- [2] Nedal M. S. Kafri1 and Hani Y. Suleiman Bit-4 of Frequency Domain-DCT Steganography Technique in 2009 IEEE.
- [3] Ismail Avcibas N.M. and B. Sankur, “Steganalysis using image quality metrics”, In IEEE Transactions on Image Processing, vol. 12, No. 2., February 2003.
- [4] M. S. Sutaone, M.V. Khandare “Image Based Steganography Using LSB Insertion Technique”
- [5] Swati Tiwari1, R. P. Mahajan2 “A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion “ in International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 1, ISSN 2249 –071X