Conceal Data in Digital Image Processing by using Steganography

Mohammad Khaleel Sallam Ma’aitah* and Kamil Dimillier
*Corresponding author email id: mohammad.maaitah87@gmail.com

Date of publication (dd/mm/yyyy): 08/01/2018

Abstract – Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, such as (image, audio, and video files). It is always non visible. Steganography has various useful applications. The main objectives of steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data. These are the main factors which make it different from other techniques watermarking and cryptography. This project includes the important steganography method called LSB technique and the main focus is on the review of steganography in digital images, and apply this technique via VB application for implementation.

Keywords – Steganography, Robustness, Cryptography, Communication technologies, LSB RGB based steganography.

I. INTRODUCTION

The communication technologies around us has grown at a great pace in recent times. For exchanging of data these days everyone is depending of high speed computer networks like internet which is quite unprotected and information can get exposed. Vast amount of personal data is often collected, used and transferred to third party organizations for a variety of reasons. Hence data security is becoming a serious problems in data communication via Internet or any other media. Steganography or Cryptography can be used to protect sensitive data. Steganography is often considered better than cryptography because the intended secret message does not attract attention to itself for scrutiny.

Steganography is the art of concealing a message, image or file within another message. One of the major requirements of data hiding is that the hidden data must be imperceptible. The use of steganography has many advantages and are very useful in digital image processing which makes them suitable for a wide variety of applications. In this modern area, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. In order to solve this problem of security and safety has led to the development of steganography schemes.

Steganography is different from watermarking and cryptography. The main objective of steganography is to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is. While cryptography techniques tend to secure communications by changing the data into a form so that it cannot be understood by an eavesdropper. Steganography is the type of hidden communication that means “covered writing” from the Greek words stego or “covered” and graphos or “to write”, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user needs to write his secret message in such holes after placing the mask over a blank sheet of paper. Then remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text.

II. RELATED WORK

Steganography is the practice 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. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography comes from the Greek words Steganos (Covered) and Graptos (Writing). Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password.

Throughout history Steganography has been used to secretly communicate information between people. Some examples of use of Steganography in past times are: 1. 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 urine, 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. 2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secret message. 3. Another method used in Greece was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax.

The recipient of the message would simply remove the wax from the tablet to view the message. East significant bit (LSB) based-RGB intensity steganography technique
proposes an improved hidden data technique for images. It deals with an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. At first it encrypts the secret message, then detects edges in the cover-image by using improved edge detection filter. After that the message bits are embedded in the least significant byte of randomly selected edge area pixels and 1st, 3rd and 4th LSBs of (Red, Green, Blue) combinations respectively across randomly selected pixels across smooth area of image. Some other types of LSB steganography techniques based on least bits.

In RGB Intensity Based Variable-Bits Image Steganography describes algorithm for RGB image based steganography. This 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. Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth introduces two methods of RGB image steganography one is pixel indicator technique and other is triple-algorithm. They use the same principle of LSB, as the secret is hidden in the least significant bits of the pixels, better randomization in selection of the number of bits and color used. This randomization increase the security of the system and it also increase the capacity. These techniques can be applied to RGB images where each pixel is represented by three bytes to indicate the additive values of red, green, and blue.

### III. LSB STEGANOGRAPHY

This is the simplest of the steganography methods based in the use of LSB, and therefore the most vulnerable. Embedding process consists of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for the bit message. For its simplicity, this method can camouflage a great volume of information. The guidelines are given below:

- **Step 1:** Convert the data from decimal to binary.
- **Step 2:** Read cover image.
- **Step 3:** Convert the cover image from decimal to binary.
- **Step 4:** Break the byte to be hidden into bits.
- **Step 5:** Take first 8 byte of original data from the cover image.
- **Step 6:** Replace the least significant bit by one bit of the data to be hidden.

First byte of original information from the cover image:

E.g.: 1 1 0 1 1 0 0 0

First bit of the data to be hidden: 1

Replace the least significant bit

\[
\begin{array}{c}
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
\downarrow & & & & & & \\
1 & 1 & 0 & 1 & 1 & 0 & 1
\end{array}
\]

This process will be continued for first 8 byte of data and conceal the first byte of data.

- **Step 7:** Continue the step 6 for all pixels.

Images after embedding data using LSB-1 Steganography.

### IV. PROPOSED SYSTEM

The proposed technique in this project is RGB pixel value based steganography method. The specialty of this algorithm is that not to change the pixels like other steganography algorithms except if it is absolutely needed. To a computer an image is a collection of data/information that represents light intensities at various points (pixels) these pixels making up the image’s raster data. All Digital images are typically stored in either (24-bit) RGB or (8-bit) known as Grayscale files. A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). All color combinations are derived from three primary colors - red, green, and blue. Each of this primary color is represented by one byte. Because RGB values are all represented by numbers, we can make use of this numbers to represent text using a mod bit algorithm. A mod bit algorithm is very similar to the Luhn mod n algorithm. Traditionally a Luhn mod algorithm is widely used for generating checksum formula for validating credit card numbers, IMEI numbers etc. As part the concept used in Luhn mod N algorithm but for finding the pixels which can represent a character. Each character from the input text will be mapped to a set of numbers and this mapping will be maintained internally in the Stegano program. For example letter „a” could be represented by digit 10, letter „b” could be represented by digit 12 and so forth. During encryption process the Stegano program will scan the image and will add the RGB values, divide it and find the mod value. If mod matches the character, that location in the image could be used to represent the character.

### V. ENCRYPTION PROCESS

- **Step 1:** The application prompts for the text and image from the sender who wants to hide the message.
- **Step 2:** Steganographic program encrypts the text using DES or RSA or any other encryption algorithm.
- **Step 3:** Steganographic program analyses the image to find the pixel value of all the pixels within the image.
- **Step 4:** Steganographic program uses the unique RGB modbit method to find out whether each letter of the message can be represented in the image and records the position to a field in the image metadata itself. For calculation of modbit the program adds the RGB values of each pixel and divides it to get the mod. If the mod value matches with that represented for the character internally, the position for that character is recorded.
- **Step 5:** If the image does not have pixel values to represent a particular character, the steganographic program finds and changes a pixel that almost matches with the image pixel and which can represent the character of text.
- **Step 6:** Finally when all the pixels which can be identified on the image and its position is recorded along with the image metadata, the user is informed that the encryption part is complete.
Figures (1-8) of Encryption and Decryption.

- **Fig. 1.**
- **Fig. 2.**
- **Fig. 3.**
- **Fig. 4.**
- **Fig. 5.**
- **Fig. 6.**
- **Fig. 7.**
VI. DECRYPTION PROCESS

Step 1: The receiver opens the image.
Step 2: The steganographic software asks for key to decrypt the image file.
Step 3: Steganographic software decrypts the metadata first and finds the pixel positions.
Step 4: Using the pixel positions, get the RGB values and decodes by reverse modbit and finds the corresponding encrypted text.
Step 5: Decrypt this text and provide back the message to the user.

VII. EXPERIMENTAL ANALYSIS

To demonstrate the algorithm a small application was developed by VB. The first step is to encode the text to be hidden into the image which needs to be used. The application allows for both encoding and decoding the text to be hidden. The application screens below show each of the steps of encryption and decryption processes.

VIII. CONCLUSION

The project proposed a LSB technique for image based steganography. It presents an improved steganography method for embedding secret message bit in image metadata fields based on the RGB values and the position of the pixels. The image pixels will be changed only for characters where the algorithm cannot find a pixel which can represent it. Since only the metadata is modified, the stego image looks exactly the same as original image or at max it will be very difficult to identify the changes for the human eye. Only the size of the stego image will increase slightly however in our test cases this has been found to be comparable with other steganography methods. This research was aimed towards the development of a new and improved data hiding technique based on RGB based steganography without changing the image. Some of the possible application areas include transmitting small secret messages, using an image as a password token by encrypting and hiding password using this technique, simply adding a hidden signature to an image etc.

REFERENCES