International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 19 (2018) pp. 14303-14307

A New Approach to Hide Secret Message and Book in Rgb Image

[1]Alhussain AKOUM
[1]Lebanese University, Faculty of Technology, Department of CCNE, Lebanon
E-mail: [1]hussein_akoum@hotmail.com

Abstract

Modern steganography (information hiding) is widely used nowadays for ensuring the security of information transmitted through the internet, where the messages are hidden in a digital data such as images. This paper presents advanced algorithm for hiding secret message as images in an RGB colored image, and a new role for steganography which is hiding a book in an image. This paper discusses two main parts. The first one is algorithm for encoding or hiding a secret message in a cover image (RGB colored image) at the sender side, and then decoding or extracting the message from the cover image at the receiver side. The second part is algorithm for encoding or hiding the pages of a book in the cover image and then decoding or extracting the book from the cover image. Saving the quality of the extracted message is a critical point in this technique was the quality in the worst case would undergo negligible loss. Special filters for enhancing the message or book texts and figures are used after the decoding is done for getting rid of any loss in quality. Any RGB colored image can be used in this process taking into consideration the dimension of the image because it will limit the number of pages you can hide in the cover image.

Keywords: *Steganography, Cryptography, Cover Image, Security*

INTRODUCTION

The word "steganography" means hidden writing and it is of Greek origin. The term steganography combines the two Greek words "steganos" which means covered, or protected, or secret, and "graphein" which means writing [1][2]. Steganography is the process of hiding data inside another data like hiding text inside image, or image inside image or audio or video [3]. Steganography is similar to cryptography which is the process of encrypting data, so that the message you send is secured, and no one can read the secret message you send except the one who has the key for decrypting the message.

Steganography is more powerful than cryptography or encryption, since encryption just hides the meaning of the message but not the message at all [4]. In other words, anyone can detect the encrypted message but without decrypting and understanding it, while steganography hides the message completely (not just its meaning) so that the message is undetectable and no one can notice the presence of a hidden message in the cover data holding the secret message.

The steganography technique was first invented by the ancient Geeks in 440 B.C. They shave the head of a trusted slave, then tattoo a secret message and wait until the hair grow again, so that the message is unnoticeable and cannot be read or detected until the head is shaved again [5].

The most popular steganography techniques since the last decade use images as the cover data for the secret messages [6]. Hence, in this paper we work on hiding a message in an RGB image and extracting it, where the message is transformed into images of type "bitmap" (.bmp) or "tagged image format file" (.tiff) and then these images will be hidden in the least significant bits (LSB's) of the pixels that forms the cover image (RGB). The message can be formed of multiple pages (up to six) which are transformed to images, where each image must have a dimension less than or equal to that of the cover image. However, in the first algorithm the images of the message must have the same dimension as that of the cover image in order to meet the specified requirements for this algorithm.

This approach leads us to the idea of hiding larger number of images in the cover image by choosing a cover image having a dimension greater than that of the message pages. Thus instead of locating the pages of the message in the entire cover image, we can locate them in well-chosen portions to leave space for locating more images (pages), which means that we can hide an entire book in an RGB image by locating its pages which are images (.bmp or .tiff) in different portions in the image.

The number of pages of the book is not a problem as long as the chosen image has the suitable dimension [10].

Our system is made up of two subsystems. The first one is the "Encoding System" that will be with the sender of the message. The second one is the "Decoding System" that will be with the one who will receive the message.

Not only no one will notice the hidden message or book, but also no one can extract the hidden data from the cover image even if he have the decoding system until passing an authentication test.

This paper will discuss the encoding system in section two, the decoding system in section three, the experimental work and results in section four, and it will end with a conclusion and future view in section five and six respectively*Figure1: Examples of face images.*

ENCODING SYSTEM

The message texts or pages must be saved as bitmap or tiff files (respectively .bmp or .tiff). In our work we focus on the bitmap files because they use less space than TIFF files. A

bitmap image is made up of very tiny parts known as pixels. Each pixel contains a binary number corresponding to the intensity of a color. We can use any type of images (RGB, grayscale and binary...), but it is preferred to use the binary bitmap image (black and white), since when we extract the message in the decoding part, the images (pages) of the message will be binary:

HIDING SECRET MESSAGE

The first step is to choose an RGB image having a dimension larger than or equal to 800x600 to be the cover image of our secret message. If the chosen image is larger than the mentioned dimension, the image must be resized to 800x600.

The second step is reading the images (pages) of our secret message which are of type 'bitmap', and resizing them to 800x600 to ensure that their dimensions match the dimension of the cover image. No matter if the images are of type RGB or grayscale or bitmap, since we will treat every image as single plane. Thus, if the images are of type RGB for example, we will extract one plane of the three available planes, to work with them as single plane images (as if we are working with binary images).

We will define two matrices having the same dimension as the cover image and assign to each of them three pages of our message that is made up of six pages or images. Every page will be located in plane 1, 2, or 3 of one of the two matrices. Then, we alter the texts of the two defined matrices holding our message pages using the 'altertxt' function in order to obtain one resultant matrix (image) of three planes.

We take the bits of the message and replace them with the least significant bits (LSB's) of the cover image in an organized sequence using the 'hidetxt' function.

Changing the LSB's of the cover image will not make a difference that can be detected by the naked eyes [7][8]. The difference between 10000000 (128 in decimal) and 10000001 (129 in decimal) is very small (129-128=1) which means that there is very slight variation in the intensity of the color of the pixel, which is impossible to notice. Thus, storing the information of the secret message in the LSB's of the cover image is a perfect choice for applying steganography [9]. In the ST-FMM algorithm proposed by Firas A. Jassim [6] the characters of the message text are transformed into ASCII values and then hidden in the cover image using the five modulus method, where here we are hiding the pixels of the message pages which means you can include in your secret message figures, pictures, signature, logo.

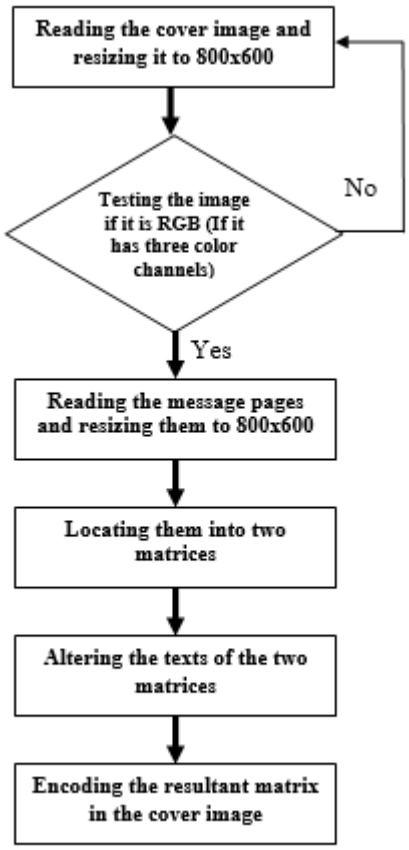

Figure1. Encoding System Block Diagram.

FACIAL MOTION CAPTURE

ENCODING SUBSYSTEM

Facial motion capture is the process of electronically converting the movements of a person's face into a digital database using cameras or laser scanners. This database may then be used to produce CG (computer graphics) computer animation for movies, games, or real-time avatars. Because the motion of CG characters is derived from the movements of real people, it results in more realistic and nuanced computer character animation than if the animation were created manually. [5]

HIDING BOOK

The concept of hiding a book in an image is quite similar to that of hiding a secret message.

In the first part we hide the pages of the message in the entire cover image (each page has the same dimension as the cover image). In this part, the cover image will be larger than each page of the book. We will keep using the 800x600 dimension for the book pages, and will choose a large cover image having dimension that is multiple of 800x600. The idea is that the cover image will be divided into equal portions; each region is of size 800x600.

Similarly, as we do in the first step, we define two matrices and locate the pages of the book in them, but with specifying the range of the rows and columns which is the region that will hold the page, not the entire cover image.

Using a cover image of dimension 1600x1200 means that it can be divided into 4 equal portions each of dimension 800x600. For locating the pages of the book in the cover image we decide in which region each one is located.

The first region if from the row number 1 till 800 and from column number 1 till 600. The second region if from the row number 1 till 800 and from column number 601 till 1200. The third region is from row number 801 till 1600 and from column number 1 till 600. The fourth region is from row number 801 till 1600 and from column number 601 till 1200. Each part is of size 800x600. Thus, we can hide 24 images (pages) in the cover image. The first matrix that we have defined will be divided similarly into four regions. In each region we locate three pages in the three planes respectively, then this matrix can hold twelve pages. Also, the second matrix will be treated by the same way and will hold another twelve (fig 2).

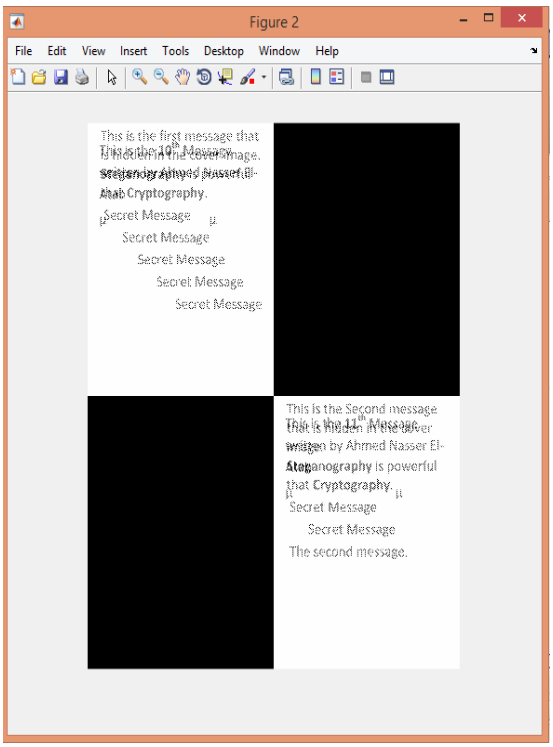

Figure 2. Locating pages in Different Regions.

We will alter the texts of the two matrices to have one resultant matrix. According to the number of pages of the book the cover image dimension is specified. The pages of the book are encoded in the cover image using the 'hidetxt' function.

DECODING SYSTEM

This system is responsible for recovering the hidden message from the cover image by extracting the text images from its LSB's using the 'extracttxt' function. After that we apply the 'seperatetxt' function on the extracted data in order to obtain the two original matrices that hold the secret message. Then, we select the pages of our secret message or book from these two matrices. This process is done according to the way of encoding. If the hidden data is a message made up of six pages, then we select from each plane of the recovered matrices (images) the page that it holds, where each page or image has the same dimension of the cover image which is also the dimension of the recovered matrices (images).

If the hidden data is a book, then we select the pages from different portions of each plane forming the two recovered matrices or images. As we assume that the cover image is divided into several equal parts (800x600) in the encoding process, in the decoding process we take into consideration the same division to ensure the correct selection of the pages from the specified regions.

Approximately half of the text image pixels are interpolated after the encoding of the secret message in the cover image, which leads to some errors in the extracted message. Thus, the recovered text image loses some quality. For retaining the quality of the decoded text images to be as the original ones, we use median filter

EXPERIMENTAL WORK AND RESULTS

In our experiment we will encode a message made up of six pages and then a small book made up of 18 pages. (Fig 3).

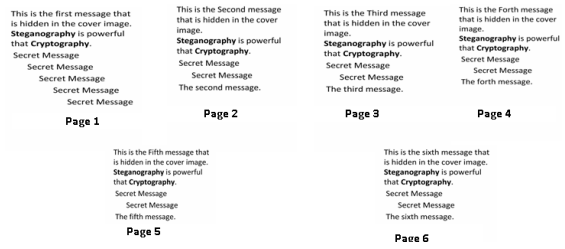

Figure 3. Message Pages.

Every page is of dimension 800x600 and will be located in one of the three planes of the two matrices im_msg_part1 and im_msg_part2.

im_msg_total is the resultant matrix after altering the text images im_msg_part1 and im_msg_part2 using the 'altertxt' function in Matlab that returns the interleaved text image of the two input text images(part1 and part2).

The pages of the message are encoded in the cover image of dimension 800x600 using the 'hidetxt' function available in Matlab.

As shown in fig4, there is no difference between the original image and the encoded one. This is because the variation in

the LSB's of the cover image cannot be detected by human vision.

Figure 4. Before and After Encoding.

After decoding the cover image at the receiver side, the recovered message after filtering will be as shown in fig5.

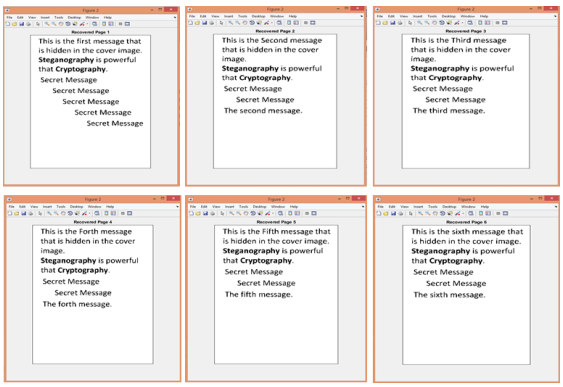

Figure 5. Recovered Message.

The recovered message retains the quality of the original message with negligible loss which is about 0.75%. It is recommended to keep the dimension of the message pages as it is and don't resize them for obtaining the 100% of the original quality.

In order to hide a book of eighteen pages, we use a cover image having a dimension of 2400x1800 which can be divided into nine equal portions each of dimension 800x600 as shown in fig6.

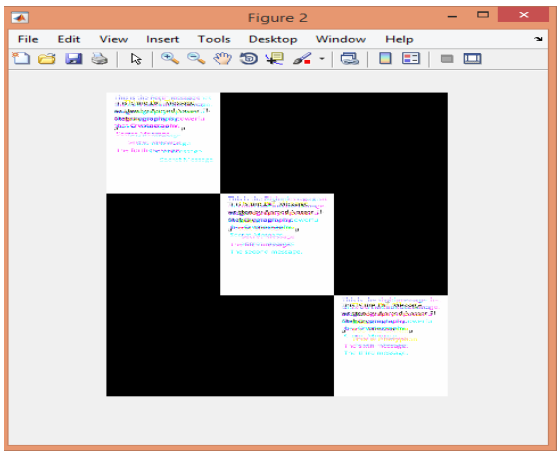

Figure 6. Recovered Message.

For simplicity, in the hiding book experiment, we used the six pages shown in fig5 and add to them twelve pages, supposing they form a real book.

We hide three pages in the upper left side where each page is located in one plane of the RGB planes. Another three pages are located in the middle of the cover image. The last three pages are located in the right down side. We define new matrix and do the same. Then, we alter the two matrices to have one resultant image holding the eighteen pages as shown in the above figure and hide it in the cover image, where no difference is noticed between the original image and the encoded one. We can locate more images in the black regions fig7.

Files of PDF format can be encoded after transforming them to bitmaps.

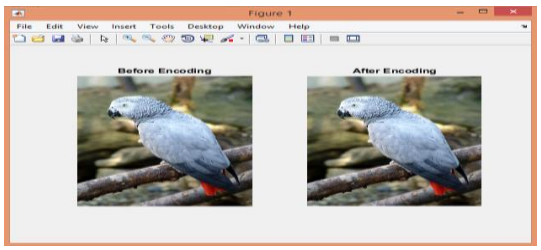

Figure 6. The Cover Image Before and After Encoding.

When we decode the cover image, we extract the pages of the book from their corresponding locations. Any mismatching selection of a page from the decoded image will result in a destroyed page. Median filtering is applied on the message pages for enhancing the contents of the pages fig8.

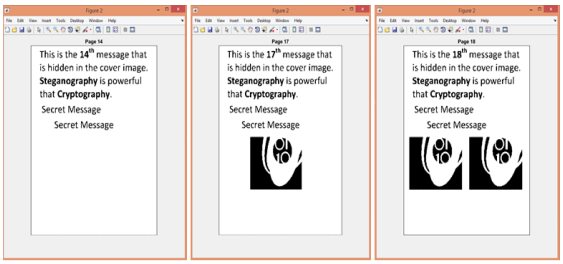

Figure 8. Sample of the Extracted Message.

CONCLUSION

Steganography is a wide science that is being studied and developed. Many techniques have been proposed concerning this science of hiding data inside another data where many of these techniques suffer from quality problems and they deal with short messages. In this paper, we developed the technique of hiding image inside another by saving the quality and allowing hiding multiple pages (book) in one single image with completely retained quality. This developed technique gives us the chance of strengthening the security of the

message, since the user has the chance of hiding the message in any region in the covered image, so that it is difficult for hackers to know where the message is located and what is its dimension, knowing that no one can extract the hidden message from the cover image without passing an authentication test linked with the sender. This is the very worst case since steganography don't let anyone detect that there is a hidden data. Hiding a book in an image can be a new way for selling books.

This system is available on windows now. Our future work is releasing an android version of this system that will be available on the app store, so that anyone can use this app for sending and receiving secret messages or books. Giving the user the option of slicing the message and hiding its parts in different region in the cover image is also a part of our future plans

REFERENCES

[1] Vipul Sharma and Sunny Kumar, "A New Approach to Hide Text in Images Using Steganography", Volume 3, Issue 4, April 2013, ISSN: 2277 128X, pp.701-708.

[2] C. Thiagarajan1, N. Aarthi2, "Novel Algorithm for RGB Image Steganography", IJCSMC, Vol. 5, Issue. 4, April 2016, pg.261 – 270.

[3] Tawfiq A. Al-asadi, Israa Hadi Ali,Abdul kadhem Abdul kareem Abdul kadhem, "A New Steganography Method for Hiding Message in Image Based on Quad Chain Code and DCT", International Journal of Digital Content Technology and its Applications, pp. 78-89, April 2015.

[4] K Thangadurai and G Sudha Devi, "Evaluation of LSB Based Image Steganography Technique for various File Formats", International Journal of Computational Intelligence and Informatics, Vol. 3: No. 3, pp.207-212, October -December 2013.

[5] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Imaging System (SIS): Hiding Secret Message inside an Image", Proceedings of the World Congress on Engineering and Computer Science 2010 Vol I WCECS 2010, October 20-22, 2010, San Francisco, USA.

[6] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", International Journal of Computer Applications, Vol.72, No.17, pp. 39-44, June 2013.

[7] Prof. D P Gaikwad, Trupti Jagdale, Swati Dhanokar, Abhijeet Moghe, Akash Pathak, " Hiding the Text and Image Message of Variable Size Using Encryption, and Compression Algorithms in Video Steganography", International Journal of Engineering Research and Applications (IJERA), Vol. 1, pp.102-108.

[8] Swati Patel, Jitendra Agrawal, "Digital Image Steganography using Particle Swarm Optimization with DCT and BPPCM", International Journal of Current Trends in Engineering & Technology, Volume: 03, Issue: 05 (SEPTEMBER –OCTOBER) 2017, pp. 306-310.

[9] Ian Davidson and Goutam Paul, "Locating Secret Messages in Images", International Conference on Knowledge Discovery and Data Mining, Seattle, Washington, USA, August 22-25, 2004.

[10] Pratap Chandra Mandal, "Steganographic technique: A survey", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345,Vol. 3 No.9 Sep 2012, pp. 444-448