Hiding text in gray image using mapping technique

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012032 doi:10.1088/1742-6596/1003/1/012032

Hiding text in gray image using mapping technique

[1] Hussein L. Hussein, [2]Ahmed A. Abbass,, [3]Sinan A. Naji, [4]Salam Al-augby and [5]Jasim H. Lafta

[1] Ibn Al- Haitham College for education, Baghdad University, Baghdad, Iraq.
[2] College education for girls, Kufa University, Najaf, Iraq.
[3] College of Engineering, Univ. of Information Technology and Communications, Baghdad, Iraq.
[4]Faculty of Computer Science and Maths, Kufa University, Najaf, Iraq.
[5]Faculty of Informatics, Debrecen University, Debrecen, Hungary.

Abstract: In order to hide the significant and secret message inside a cover object, Steganography is considered as one of the most used technique because of its strength. This paper presents a new steganography technique that it is difficult to discover or break by a third party. The ASCII Mapping Technique (AMT) is used to create an encoded table by mapping the text message and matching some bits with that of the cover image. The system saves the character parts matching and the location of which part of the pixels. Then change the related flag from zero to one the for matched locations so that they cannot be used again to strength the technique and make it more secure. The proposed t**echnique** was tested and showed low computational cost with effective performance to be used for multi-purpose applications.

1-Introduction.

"Covered writing" is the literal translation of the Steganography term which consists originally from the "steganos" and "graphia" Greek words. Steganography can be considered as a way of concealed communications which is highly related to cryptography [1] [2].

In fact, the protection of messages is the main goal of cryptography and that is the vital difference between cryptography and steganography, by converting it to cipher text, meanwhile the main objective of steganography is to conceal a secret message in a cover object. As a result, the message will be hidden from the unauthorized users [3]. Steganography, Digital watermarking and other information hiding mechanisms is used to solve this problem [4].

Steganography implies embedding process and extracting process. In the embedding process, the new generated image is called stego-image or a cover image and used to carry the secret data. For hiding data, the selected pixels should be chosen secretly by using a special algorithm or secrete key as shown in Figure 1 [5] [6].

The challenges associated with steganography techniques are influenced by the following factors [7] [8]:

1. Invisibility: implies that the stego-image looks very similar to the original image [9] [10].
2. Payload/Capacity: defines the amount of secret data which can be hided in the cover media [11].

3. Robustness against statistical attacks: Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) are two most fidelity parameters which are used to measure the robustness against statistical attacks [9] [12] .
4. Computation Complexity: It is a computation of the expensiveness of the embedding and extracting process of a hidden message [2] [13].

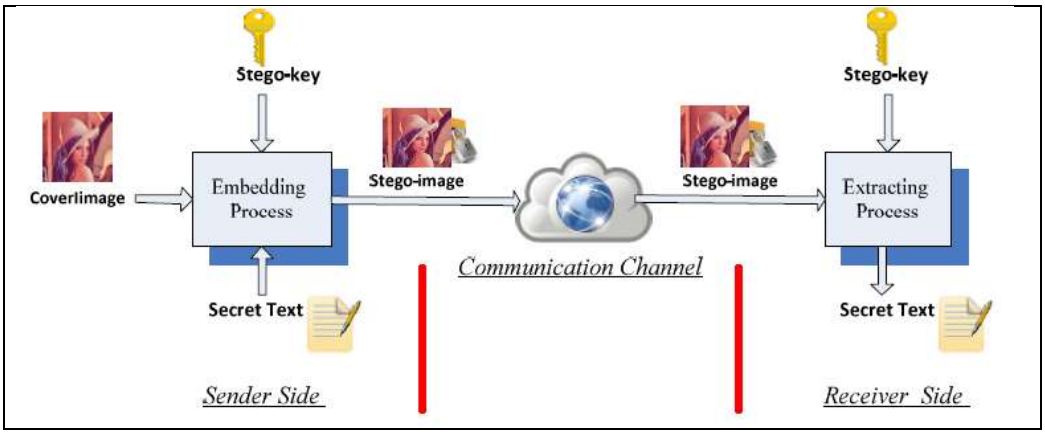

Figure 1: Steganography system

2.Related Works

Many techniques are proposed to improve the steganography techniques. Kukapalli et. al. [8] presented an enhancement method of the Pixel Indicator Method (PIM). The methodology was built on using the last three MSB of each pixel. Blowfish was used as an encrypted algorithm. Taking the advantage of the difference between colors to embed message bit was one of the strength points of this method. Depending on color differences and values of variable N the color will be selected and the authors claimed the detecting of message will be difficult. Moreover, changes in the image will be indistinguishable.

Bhattacharyya et. al. [4] proposed a text steganography method based on ASCII Mapping Technology (AMT). In order to increase the security level, the quantum logic technique was used because of its ability to find a valid embedding position. The Shannon Entropy and Correlation-coefficient values showed that Stego text was generated with minimum or zero degradation using ATM method.

For hiding secret message in an image Satar et. al. [14]designed a simple and efficient model.

In calculation stage of this model, a new binary number of secret messages was conducted by Connective Logical (CL) algorithm while the key was represented by the Most Significant Bit (MSB) of each pixel. Using Operator Negation, OR and XOR helped in the production of a new secret message by calculating the MSB of each pixel that will assist the new secret message by embedding in the LSB of pixels.

Alsarayreh et. al. [7] presented a system to hide secret data inside the image. This work finds the exact matches between the image RGB decimal values and the secret message/data after converting them to ASCII. However, the system generates a key to recover the secret data which is randomly generated based on matched pixels and the secret text. As well as, a Random Key-Dependent Data (RKDD) is generated without performing any changes on the image's pixel values.

One of the concealing information technique that hide information within the spatial domain of any gray scale image is Pixel Mapping Method (PMM) technique. It is firstly proposed by Bhattacharyya et. al. [15]. Some mathematical functions were the basis of choosing embedding pixels where the pixel intensity value of the seed pixel and its 8 neighbors are the cornerstone of this process. The selection was taken in counter clockwise direction. Each two or four bits of the secret message were mapped to data embedding.

This process was conducted in each of the neighboring pixel on the basis of some features of that pixel. In order to retrieve the original information there will be different reverse operation are executed at the receiver side.

Banerjee et. al. [16] presented an improved version of PMM method which is based on special domain. In the first step of this method, the input message is converted into a digital character format in order to deal

with bit stream. For the purpose of embedding in a separate pixel and embedding pixel selection, a 2-bit pair and a mathematical function are adapted. In the next step pixel intensity value and pixel position on image were used as the basis of selection technique. For more embedding in a pixel, a two bit from the secret message were mapped. This embedded pixel is based on the intensity value, previous pixel value and number of one's (in binary) present in that pixel. The concept of previous pixel intensity value is added in this work along with the embedding pixel selection method [16].

3.The Proposed Technique

The main idea of the proposed algorithm is to divide each character (8-Bits) of the secret message into two bits and then search the image pixels for the two similar bits in that image (Each pixel in gray image has 256 gray scale, i.e. in the representation of one pixel in gray image we need one byte). As an expected result of this method, the probability of finding matching pixels that are in relation to characters of the secret messages. The matches are saved and sent to the receiver in separate encrypted channel.

Error! Reference source not found.Error! Reference source not found. shows the structure of the proposed algorithm that can be summarized in the four steps as follows:-

3.1. Embedding algorithm the secret message:

Input : secret text , covered image.
Output : covered image , locations table.
The Technique Consists of the Following Steps
Step-1:

- Select gray scale image.
- Read the secret message.
- The gray scale pixel image and each character of secret message will be represented as binary values.
- Divide each binary value of the pixel image and binary values of each character into four parts of 2-bits long.

Step-2:

- Sequentially, two bits are selected from the data stream after that a search of a two bits similarity in the image pixels will be conducted.
- Save matches location of which part of the pixel.
- Set the flag to one for this location and that part so that cannot be used again.

Step-3: Repeat step 2 until the end of secret message.
Step-4: Output the resulting location table.

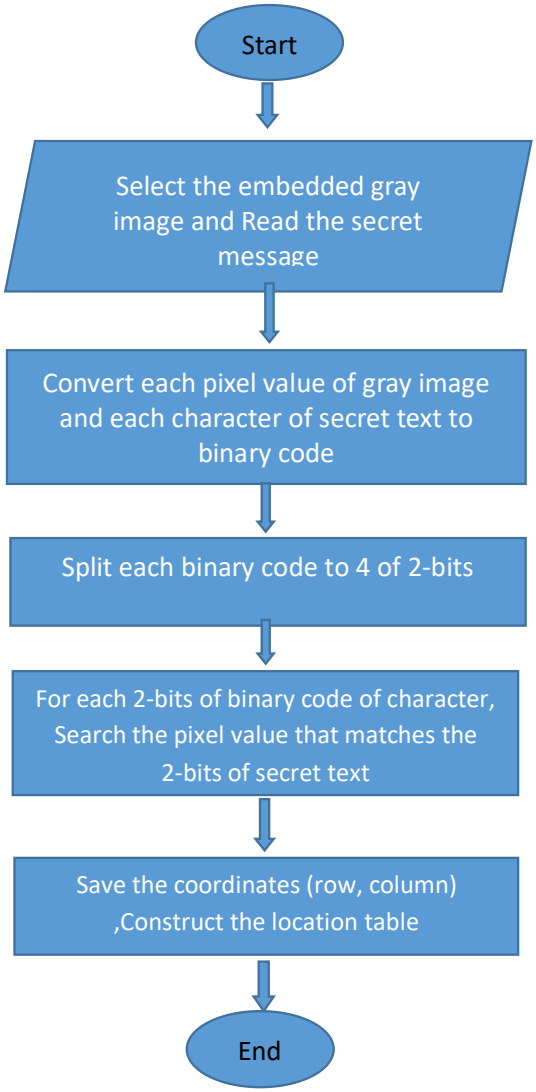

Figure-2. Flowchart of proposed system for mapping technique.

4.Experimental Results

For testing the proposed algorithm, various lengths of secret messages and different sizes of images were taken as depicted in Table-1 where:

INPUT TEXT= 'this free online service allows to … separate files ".

Table 1: The input letters along with their matches locations in the image

Letter	ASCII Code	1st 2-bits location		2nd 2-bits location		3rd 2-bits location		4th 2-bits location	
		Row	Col.	Row	Col.	Row	Col.	Row	Col.
t	01110100	1	14	1	14	1	2	1	3
h	01101000	1	15	1	479	1	3	1	7
i	01101001	1	21	1	490	1	4	1	4
s	01110011	1	22	1	15	1	1	1	1

space	00100000	29	4	1	491	1	10	1	9
f	01100110	1	23	1	492	1	8	1	2
r	01110010	1	24	1	21	1	11	1	8
e	01100101	1	25	1	495	1	9	1	5
e	01100101	1	26	1	496	1	12	1	6
space	00100000	29	9	1	497	1	13	1	12
. . . .	. . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .
f	01100110	1	315	20	58	1	75	1	56
i	01101001	1	318	20	59	1	27	1	68
l	01101100	1	319	20	60	1	46	1	75
e	01100101	1	331	20	61	1	76	1	69
s	01110011	1	338	1	83	1	87	1	79

5.Conclusion

The system achieved two important goals, which can be summarized as following:
First, we illustrate that the system keeps the cover image unchanged because the image plays the role of the key to encode the secret message.

This is an important issue for the developers and users.
Second, the proposed system uses the mapping technique.

The mapping of each character of the secret message and matching each binary two bits of the stream data to the same two bits in the image was the first step. Secondly, locking the locations in the image will lead to a distribution of every two bits the character of the same bits of the image and will give each character of the secret message a new substitution value. Increasing the probability of finding another matching that has a mapping to characters of the secret message was done by distributing the bits of the characters.

This makes the task of the steganalysis harder to reconstruct the message.

References.

[1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica ridrich, Ton Kalker, 2007 ," Digital Watermarking and Steganography" ,Second Edition, Morgan Kaufmann Publishers is an imprint of Elsevier, USA.

[2] Mehdi Hussain, 2013,A Survey of Image Steganography Techniques*, International Journal of Advanced Science and Technology*, **54**.

[3] Al-Husainy, M.A.2009, Image Steganography by mapping Pixels to letters. *Journal of Computer science,* **5**(1): p. 33.

[4] Bhattacharyya, S., P. Indu, and G. Sanyal,2013, *Hiding Data in Text using ASCII Mapping Technology (AMT). International Journal of Computer Applications*, **70**(18).

[5] Samagh, R. and S. Rani,2015, Data Hiding using Image Steganography*, International Journal of Emerging Trends in Engineering and Development,*: p. 123-129.

[6] Li;, B., et al.,2011, A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing,.*

[7] Alsarayreh, M.A., M.A. Alia, and K.A. Maria,2017, *A Novel Image Steganographic System Based on Exact Matching Algorithm and Key-Dependent Data Technique. Journal of Theoretical and Applied Information Technology*, **95**(5): p. 1212.

[8] Kukapalli, V.R., B.T. Rao, and M.B.S. Reddy,2014, Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare,*International Journal of Computer Trends and Technology (IJCTT)*, Volume-**15** Number-3.
[9] Tuama, A.Y., et al.,2017, Randomized Pixel Selection for Enhancing LSB Algorithm Security against Brute-Force Attack. *Journal of Mathematics and Statistics* , **13**((2)): p. 127-138.
[10] Nag, A., et al.,2011, A novel technique for image steganography based on DWT and Huffman encoding. *International Journal of Computer Science and Security,(IJCSS)*, **4**(6): p. 497-610.
[11] Kumar, M. and M. Yadav,2014, Image steganography using frequency domain. *International Journal of Scientific & Technology Research,* **3**(9): p. 226-230.
[12] Goyal, M., Y. Lather, and V. Lather, 2015,Analytical relation & comparison of PSNR and SSIM on babbon image and human eye perception using matlab. *International Journal of Advanced Research in Engineering and Applied Sciences*, **4**(5): p. 108-119.
[13] Chen, P.-Y. and H.-J. Lin, 2006,*A DWT* based approach for image steganography. *International Journal of Applied Science and Engineering,* **4**(3): p. 275-290.
[14] Satar, S.D.M., et al.,2015, A New Model for Hiding Text in an Image Using Logical Connective. *International Journal of Multimedia and Ubiquitous Engineering,* **10**(6): p. 195-202.
[15] Bhattacharyya, S., L. Kumar, and G. Sanyal, 2010,A novel approach of data hiding using pixel mapping method (PMM). *International Journal of Computer Science & Information Security*, p. 1.
[16] Banerjee, I., S. Bhattacharyya, and G. Sanyal, 2013,*Hiding & analyzing data in image using extended PMM.* Procedia Technology, 10: p. 157-166.