International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 3, June 2022, pp. 2812~2817
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i3.pp2812-2817

American standard code for information interchange mapping technique for text hiding in the RGB and gray images

Ahmed Abdulrudah Abbass[1], Salam Al-augby[2], Hussein Lafta Hussein[3], Jasim Hussein Kaabi[4], Robert Tornai[4]
[1]College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq
[2]Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Kufa, Iraq
[3]Ibn Al-Haitham College for Education, University of Baghdad, Baghdad, Iraq
[4]Faculty of Informatics, University of Debrecen, Debrecen, Hungary

Article Info

Article history:

Received Mar 27, 2021
Revised Dec 31, 2021
Accepted Jan 19, 2022

Keywords:

ASCII mapping technique
Grey image
Information hiding
Information security
RGB image
Steganography

ABSTRACT

One of the significant techniques for hiding important information (such as text, image, and audio) is steganography. Steganography is used to keep this information as secret as possible, especially the sensitive ones after the massive expansion of data transmission through the Internet inside a conventional, non-secret, file, or message. This paper uses the American standard code for information interchange (ASCII) mapping technique (AMT) to hide the data in the color and grey image by converting it in a binary form, also convert the three levels of the red, green, and blue (RGB) image and grey image in the binary form, and then hide the data through hiding every two bits of the text in the two bits of one of the levels from the RGB image and grey image that means the text will be distributed throughout the images and allows hiding large amounts of data. That will send the information in a good securing way.

Corresponding Author:

Salam Al-augby
Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa
P.O Box 21, Kufa, Najaf Governorate, Iraq
Email: salam.alaugby@uokufa.edu.iq

1. INTRODUCTION

Steganography is a Greek word that means covering writing, this word consists of a two-part word "stegos" and "grafia" which means "cover" and "writing", respectively [1], [2]. Steganography mainly aims to hide secret data in embedded cover and it can be considered as a pro-security innovation [3]. The main two components of steganography are the message which represents information that ought to be covered up and the carrier that represents the media that holds the message.

At the present time using images to hide significant information is a popular technique. The internet considered as a suitable medium to transmit the used images, as appeared in Figure 1. In order to get good hiding results in steganography the appearance of the picture should not be altered and the changing in the cover source should be in "noisy" areas with color variations that will lead not to draw attention to these changes. These changes will be achieved in many ways, such as the least-significant bit or least significant bit (LSB), masking, filtering, and transformations on the cover image. These methods can give different accuracy results on various file types [4]–[7].

The factors that affected the steganography techniques which may make some difficulties of these techniques are the followings [8], [9]:

– Invisibility: gives an indication of how similar the stego-picture for the original image [10], [11].
– Payload/capacity: it gives a limited amount of data to be hidden in the spread media [12].

Which may be considered as the problem that we tried to solve in this work besides the wider distribution of the hidden data in picture the harder of detecting them, therefore, this paper uses a new technique to hide the text in the image by considering the images as keys for the hiding process, so that will keep the text not observed. The text will be sent in a form of a table where this table represents the locations of the text to hide into the image so it is not possible to know the hidden text. That's beside hiding a big amount of data in the three levels of image red, green, and blue (RGB) and gray image where the text is hidden at each level of the color image and gray image [13], [14].

2. RELATED WORKS

Literature that is related to the major interest of this work includes different studies in this field as illustrated below: in the first paper, the authors devised a novel approach to hiding messages in lossless RGB images. It presents an improved LSB image steganography method where each encoded message bit is embedded in one of the three RGB channels (indicator/selector) on the basis of the most significant bit (MSBs) of channels, with encoding being obtained based on the parity values of that selected channel. The experimental results demonstrate that our method has primarily shown significant improvements in terms of imperceptibility and robustness. Although the capacity is not very high, higher payload capacity has to be sacrificed for higher imperceptibility. The essential contribution of this study is that decent number of secret message bits is encoded into LSB positions effectively by altering comparatively a few numbers of cover image bits and without direct involvement of any stego-keys. Our scheme is straightforward in generating quality stego-image, and feasible for other steganographic fields such as audio/video steganography [15]–[17].

A new technique for adopting a set of two-letter words was presented by Kukapalli *et al.* [11]. The suggested method used zero width non-joiner (200C) and zero width joiner (200D) symbols. The proposed method suggested providing data security by hiding bit information in a text file. This paper achieved many aims such as perceptual transparency, hiding capacity and robustness. In addition to that, the hiding method will not make any changes to the original script. Unicode uses two bytes in representing each non-printing characters that lead to one of the cons of this method is the increase in file size [18], [19].

One of the new steganographic algorithm for hiding text files in images was proposed by Sharma and Kumar [20]. Maximum compression ratio of 8 bits/pixel by an underlying compression algorithm was applied. This paper concluded that there were no clear changes after conducted a proposed method on different sizes of text files to be hidden on few images in addition to its efficient work on .bmp images. Based on that they supposed that the proposed approach has good results in hiding text files in images [20].

The main goals of papers in this field is to suggest a significant steganography technique that is not easy to break or discover by other parties. One of these techniques that is presented by Hussein *et al.* [21] is an American standard code for information interchange (ASCII) mapping technique (AMT). In this technique, the cover image will be matched with some bits of the text message and that will create an encoding table. Saving the matched character parts and where it is located. This technique has increased its security by changing the related flag from zero to one for matching locations. As a conclusion from testing this system was this technique can be used for widespread applications on account of its effectivity and its low cost [21]. One of another proposed technique that depended on ASCII mapping technology (AMT) that is used for text steganography. The ability of the quantum logic technique of finding a valid embedding position led to the use of it for increasing the security level. The using of AMT was used to generate stego-text with minimum or zero degradation that was proved by using the Shannon entropy and correlation-coefficient values [22].

An improved version of the predictive mean matching (PMM) method that is originally based on a specific domain was introduced by Banerjee *et al.* [23]. Their paper consisted of some steps that is started by converting the input message into a digital character format for the purpose of dealing with bit stream. The second step was adapting a mathematical function with a 2-bit pair in order to the embedded process of pixels in selecting and separating. The selection technique was the next step in this process and it is based on the pixel intensity value and the pixel position on image. Mapping two bits from the secret message was adopted so as to increase the pixel embedding. The values of intensity and previous pixel in addition to the number of ones (in binary) present in that pixel were the basis for the embedded pixel. This work suggested besides the embedding pixel selection method the concept of previous pixel intensity value.

Another contribution of systems that uses the image to hide secret data was presented by Alsarayreh *et al.* [10]. One of the main findings of this work is that converting the image RGB decimal values and the secret message/data to ASCII will produce exact matching between them. In this system the secret data is generated randomly on the basis of matching the secret text and pixels, a key is generated to recover this secret data. That will be performed with the same image's pixel values in generating a random key-dependent data (RKDD).

The studies [24], [25] tried to present a simple and significant model for hiding a secret message in an image. One of the important stages in this system was the calculation stage wherein the LSB of each pixel was used to introduce the key and connective logical (CL) algorithm to conduct a new binary number of secret messages that resulted a new binary number of secret messages. A new secret message will be produced by calculating the LSB of each pixel by using of Negation, OR and XOR operators. The embedding in the LSB of pixels will assist the new secret message.

3. RESEARCH METHOD

This suggested algorithm consists of the following steps: firstly, each character (8-bits) of the secret message will be divided into two bits. The next step is searching for the two similar bits in each level of the image RGB image and gray image) levels where each level has 256 gray scale that means we need one byte for representing one pixel in gray image. The matching pixels that are connected to the secret messages' characters will have a higher probability of finding. The final step is that these matched pixels will be sent to the recipient in an isolated encrypted channel after saving it. The principals of the proposed algorithm is composed of two parts, the first one is a preprocessing and the second one is hiding process.

3.1. Pre-processing

This process composed of two types, the first type represents the text manipulation, each character from the message is converted into binary form, and then each 8 bit (represent one character) will be divided into four sections each one contains 2 bits. The second type represents the image manipulation, when deal with the color image (RGB), three levels (R level, G level and B level) will be taken in addition to using the gray image for the same image. The next step is converting each level and gray image into binary form where each pixel is represented in 8 bits of each level and gray image and then divide them into four sections, each section contains 2 bits as illustrated in Figure 1.

- Step 1: Input Secret Messages
- Step 2: Convert the Secret Message and each level of the RGB Image into binary form
- Step 3: Divide the Secret Message into four Section each one have 2bits
- Step 4: Repeat Step 3 for each level of the RGB image and Gray Image

Figure 1. Preprocessing algorithm

3.2. Hiding process

To hide the secret message that are converted into binary form, the first 2-bits section is taken from the message and then the same 2-bits will be searched in the R level from the image and then saving the location and position in the table for this 2-bits from R level (which represent the row and column of the R level) and ignoring this location and position from the R level. After that the second section of 2-bits from the message will be taken and the same 2-bits will be searched in the G level from the image and saved the location and position in the table for this 2-bits from G level, also ignore this location and position from the G level. The third section of 2-bits from the message will be taken then and searched the same 2-bits in the B level of the image when finding the same 2-bits will save the location and position in the table and ignore this location and position from the B level. The last section from the message last 2-bits will be searched in the gray image and then saving the location and position in the table and ignore this location and position from the gray image. Therefore, this technique will use two keys for hiding the secret message, the first key is a RGB image and the second key is the gray image, the message will be saved in the table that are represented as a location of the levels RGB for the image and the gray image, the Figure 2 illustrate this process.

4. RESULTS AND DISCUSSION

The proposed method was tested on various lengths of the text message, and the .bmp image color. In the following paragraphs we will present the results as well as the discussion. The results are shown and described in detail in the following paragraphs.

- Step 1: Input n of the sections that contain 2bits from the secret message
- Step 2: Search in the R,G,B, levels, and Gray image depends on the n
- Step 3: Save the Location and position in the Table and ignore them from the image
- Step 4: If the number of sections (n) is greater than 4, End the process, increase the number of n, and repeat all steps.

Figure 2. Hiding process algorithm

4.1. Results

The main goal of using color image is to benefit from the (RGB) levels where every level from these levels will use the location of the pixel that will give the random distributed for the secret message in all levels of the image. Table 1 illustrate how to save the locations for the secret message in the image levels, when the input message is INPUT MESSAGE: "*MATLAB program for hiding text in color image using mapping technique*". After agreement between the sender and recipient where RGB image will be used as the first key and the gray image represent the second key of the steganography system, then the Table 1 will be sent to the recipient and then extract the secret message by detect the location (row and column) for each level of RGB and gray image.

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

Char.	Red			Green			Blue			Gray		
	Row	Column	Position	Row	Column	Position	Row	Column	Position	Row	Column	Position
m	1	2	3	1	1	4	1	1	1	1	3	3
a	1	3	3	1	2	3	1	10	4	1	6	4
t	1	5	4	1	3	1	1	3	3	1	1	4
l	1	11	4	1	5	2	1	2	1	1	5	4
a	1	14	4	1	6	3	1	11	4	1	7	4
b	1	20	3	1	7	3	1	13	3	1	2	3
p	1	1	4	1	8	3	1	14	3	1	10	4
r	1	28	3	1	4	1	1	15	4	1	14	4
o	1	32	3	1	9	1	1	17	4	1	8	3
g	1	33	2	1	13	3	1	4	1	1	4	1
r	1	34	2	1	14	3	1	6	4	1	9	1
a	1	37	4	1	10	1	1	22	4	1	11	4
m	1	38	3	1	15	3	1	24	4	1	17	4
…	…	….	….	….	….	….	….	….	….	….	….	….
…	….	….	….	….	….	….	….	….	….	….	….	….
h	2	32	3	1	91	3	1	55	4	1	60	3
n	2	33	2	1	92	3	1	54	1	1	59	3
i	2	38	4	1	93	3	1	57	3	1	70	4
q	2	42	3	1	33	1	1	109	4	1	74	4
u	2	45	4	1	35	1	1	94	4	1	75	3
e	2	48	4	1	94	3	1	97	4	1	77	4

4.2. Discussion

From the practical tests of the proposed technique and using different sizes of text, the proposed system distributes the secret message and spread the bits of the secret message on the R level, G level, and B level, which represent the first key of the hiding process, also using gray image as a second key of the hiding process. The proposed system can hide a large size of a secret data, while the previous methods hide limited size of secret data where these methods depend on the size of the image. The proposed method gives a high distribution of the text and thus gives a high power of the hiding, which leads to difficulty of knowing the hidden text. The restrictions to use this method, the hiding process needs more computations to find hidden locations, and therefore it needs more time in order to hide the text.

5. CONCLUSION

Based on what have been achieved one can concludes the followings: firstly, the proposed technique does not have effects on the original image because the image will be designed as a key of steganography technique. Therefore, the image will be kept without any changes. Therefore, that can be considered as an

important point of the Steganography for both of users and developers. Secondly, the AMT technique depend on converting the secret message into a binary form and then distributing and spreading it over all levels of RGB and gray image. In the matching process where 2 bits from the secret message matching with 2 bits from the levels of the RGM image and gray image, the location of these 2bits will be saved in a table. This table will represent the locations of the secret message on the RGB image and Gray image. This technique will make the stego analysis very difficult to know the secret message. Thirdly, using two keys in the hiding process that will increase the difficulty of knowing the secret message and finally, distributing and spreading the secret message over all locations of the RGB and gray image will increase the difficulty of prediction the secret message.

REFERENCES

[1] K. Sara, A. D. Mashallah, and Y. M. Hossein, "A new steganography method based on HIOP (higher intensity of pixel) algorithm and strassen's matrix multiplication," *Journal of Global Research in Computer Science*, vol. 2, no. 1, pp. 6–12, 2011.

[2] A. R. Khekan, H. M. Wajeh Majeed, and O. F. Ahmed Adeeb, "New text steganography method using the Arabic letters dots," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, no. 3, pp. 1784–1793, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1784-1793.

[3] S. Katzenbeisser and F. Petitolas, "Information hiding techniques for steganography and digital watermaking," *Edpacs*, vol. 28, no. 6, pp. 1–2, Dec. 2000, doi: 10.1201/1079/43263.28.6.20001201/30373.5.

[4] M. Hariri, R. Karimi, and M. Nosrati, "An introduction to steganography methods," *World Applied Programming*, vol. 1, no. 13, pp. 191–195, 2011.

[5] B. T. Ahmed, "A systematic overview of secure image steganography," *International Journal of Advances in Applied Sciences (IJAAS)*, vol. 10, no. 2, pp. 178–187, Jun. 2021, doi: 10.11591/ijaas.v10.i2.pp178-187.

[6] R. A. Hamzah, M. M. Roslan, A. F. Bin Kadmin, S. F. B. A. Gani, and K. A. A. Aziz, "JPG, PNG and BMP image compression using discrete cosine transform," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 3, pp. 1010–1016, Jun. 2021, doi: 10.12928/telkomnika.v19i3.14758.

[7] M. A. A. K. Al-Dabbas, A. Alabaichi, and A. S. Abbas, "Dual method cryptography image by two force secure and steganography secret message in IoT," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, pp. 2928–2938, Dec. 2020, doi: 10.12928/telkomnika.v18i6.15847.

[8] K. Ganesh and S. Yaji, "Implementation of securing confidential data by migrating digital watermarking and steganography," *International Journal of Research in Engineering and Science (IJRES)*, vol. 2, no. 5, pp. 76–81, 2014.

[9] M. Shirali-Shahreza and M. H. Shirali-Shahreza, "Text steganography in SMS," in *2007 International Conference on Convergence Information Technology (ICCIT 2007)*, Nov. 2007, pp. 2260–2265, doi: 10.1109/ICCIT.2007.4420590.

[10] M. A. Alsarayreh, M. A. Alia, and K. A. Maria, "A novel image steganographic system based on exact matching algorithm and key-dependent data technique," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 5, pp. 1212–1224, 2017.

[11] V. R. Kukapalli, D. B. T. Rao, and M. B. S. Narayana, "Image steganography by enhanced pixel indicator method using most significant bit (MSB) compare," *International Journal of Computer Trends and Technology*, vol. 15, no. 3, pp. 97–101, Sep. 2014, doi: 10.14445/22312803/IJCTT-V15P122.

[12] A. Y. Tuama, M. A. Mohamed, A. Muhammed, and Z. M. Hanapi, "Randomized pixel selection for enhancing LSB algorithm security against brute-force attack," *Journal of Mathematics and Statistics*, vol. 13, no. 2, pp. 127–138, Feb. 2017, doi: 10.3844/jmssp.2017.127.138.

[13] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar, "A novel technique for image steganography vased on DWT and huffman encoding," *International Journal of Computer Science and Security (IJCSS)*, vol. 4, no. 6, pp. 561–570, Jun. 2010, doi: 10.5121/ijcsit.2010.2308.

[14] P. D. T. A. Abbas, "Steganography using fractal images technique," *IOSR Journal of Engineering*, vol. 4, no. 2, pp. 52–61, Feb. 2014, doi: 10.9790/3021-04225261.

[15] Z. A. Alwan, H. M. Farhan, and S. Q. Mahdi, "Color image steganography in YCbCr space," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 202–209, Feb. 2020, doi: 10.11591/ijece.v10i1.pp202-209.

[16] A. A. Mohamed, "An improved algorithm for information hiding based on features of Arabic text: a unicode approach," *Egyptian Informatics Journal*, vol. 15, no. 2, pp. 79–87, Jul. 2014, doi: 10.1016/j.eij.2014.04.002.

[17] M. Kumar and M. Yadav, "Image steganography using frequency domain," *International Journal of Scientific & Technology Research*, vol. 3, no. 9, pp. 226–230, 2014.

[18] A. K. Mandal and M. N. M. Kahar, "Variant of LSB steganography algorithm for hiding information in RGB images," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 10, no. 1, pp. 35–48, Jan. 2017, doi: 10.14257/ijsip.2017.10.1.05.

[19] S. S. Baawi, M. R. Mokhtar, and R. Sulaiman, "New text steganography technique based on a set of two-letter words," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 22, pp. 6247–6255, 2017.

[20] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 4, pp. 701–708, 2013.

[21] H. L. Hussein, A. A. Abbass, S. A. Naji, S. Al-augby, and J. H. Lafta, "Hiding text in gray image using mapping technique," *Journal of Physics: Conference Series*, vol. 1003, no. 1, May 2018, doi: 10.1088/1742-6596/1003/1/012032.

[22] S. Bhattacharyya, P. Indu, and G. Sanyal, "Hiding data in text using ASCII mapping technology (AMT)," *International Journal of Computer Applications*, vol. 70, no. 18, pp. 29–37, May 2013, doi: 10.5120/12169-8282.

[23] I. Banerjee, S. Bhattacharyya, and G. Sanyal, "Hiding & analyzing data in image using extended PMM," *Procedia Technology*, vol. 10, pp. 157–166, 2013, doi: 10.1016/j.protcy.2013.12.348.

[24] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, and M. Mamat, "A new model for hiding text in an image using logical connective," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 6, pp. 195–202, Jun. 2015, doi: 10.14257/ijmue.2015.10.6.20.

[25] M. Taleby Ahvanooey, Q. Li, H. J. Shim, and Y. Huang, "A comparative analysis of information hiding techniques for copyright protection of text documents," *Security and Communication Networks*, vol. 2018, pp. 1–22, 2018, doi: 10.1155/2018/5325040.

BIOGRAPHIES OF AUTHOR

Ahmed Abdulrudah Abbass born in Baghdad, Iraq, in 1972, holds a master's degree from the Iraqi Computer and Informatics Authority in the field of information security, and Ph.D. from the University of Babylon in the field of computer science. Research interests in the field of information and network security. He can be contacted at email: ahmed.alzamili@uoitc.edu.iq.

Salam Al-augby received his B.Sc. Degree in Electronic and Electrical Engineering from MEC in 1997 and the master's degree in computer science from the University of Technology, Iraq in 2005. He got his Ph.D. degree in IT in Management from University of Szczecin, Szczecin, Poland in 2015. The area of interests is data analysis, data mining, text mining, behavioral finance, sentiment analysis, IT in management, big data analysis, social media analysis, and natural language processing. He can be contacted at email: salam.alaugby@uokufa.edu.iq. ResearcherID: C-6851-2016.

Hussein Lafta Hussein born in Baghdad, Iraq, in 1964, B.Sc. master's degree from university of technology in the field of computer science, Iraq, and Ph.D. from the University of Babylon in the field of computer science. Research interests in the field of digital image prpcessing and information security. He can be contacted at email: hussein.l.h@ihcoedu.uobaghdad.edu.iq.

Jasim Hussein Kaabi born in Baghdad, Iraq, in 1992, B.Sc. degree from Baghdad College for Economic Sciences University master's degree from University of Debrecen in the field of computer science, Hungary, and Ph.D. student at the University of Debrecen in the field of discrete mathematics, data processing and visualization. He can be contacted at email: jasimhussein67@gmail.com.

Robert Tornai B.Sc. master's Ph.D. degree from university of Debrecen, Hungary in the field of computer science. Research interests in the field of computer graphics and image processing. He can be contacted at email: tornai.robert@inf.unideb.hu.